Smart Government Resilience & Cybersecurity Risk Management

المرونة وادارة مخاطر أمن المعلومات في ظل الحكومة الذكية

by

HOOR RIADH DALI

A thesis submitted in fulfilment

of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN BUSINESS MANAGEMENT

at

The British University in Dubai

September 2020

Smart Government Resilience & Cybersecurity Risk Management

المرونة وادارة مخاطر أمن المعلومات في ظل الحكومة الذكية

by

HOOR RIADH DALI

Dissertation submitted in fulfilment

of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN

BUSINESS MANAGEMENT

at

The British University in Dubai

September, 2020

Thesis Supervisor
Name of Professor

Approved for award:

_____	_____
Name	Name
Designation	Designation
_____	_____
Name	Name
Designation	Designation
Date: _____	

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

_____

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

ABSTRACT

In smart government systems, there is a high level of local and global business interconnectedness, which increases the overall vulnerability on the cyber platform. Usually, the highest risk can be found in the smart infrastructure of smart government. Consequently, this needs to be protected and safeguarded. In order to be effectively equipped, the establishment of a sophisticated cyber resilience framework is essential. Smart governments need to be well-prepared (managerially) and well-equipped (technically); especially in times of cybersecurity crisis. For this purpose, the researcher reviewed and evaluated the existing resilience frameworks worldwide and developed a proposed framework for the smart governments in the UAE. This study determined and identified the components of the resilience framework, which addresses the above issues and results in smart government resiliency and cybersecurity risk management. This research contributed to filling the gap in the literature, particularly in Resilient Measurement in relation to cybersecurity, especially in the case of smart government systems. The suggested model matches the smart government needs/culture in the UAE according to this study survey, which measured the readiness and determined maturity level of the smart systems analysed.

The researcher adopted a quantitative research methodology for this work. Responses from 432 smart services users in the UAE were collected and analysed. It was discovered that the proposed resilience structure can be adopted successfully by the smart government enterprise. It has assessed the flexibility of the electronic platform procedures to fill the gap in sustainability materials related to smart government resilience structures and cybersecurity risk management; and found the best current resiliency framework.

ملخص الدراسة

في القرن الحادي والعشرين ، كانت التكنولوجيا تتطور بشكل لم يسبق له مثيل. أحد العناصر الرئيسية التي تؤثر على مرونة أمن المعلونات هو بيئة التكنولوجيا المعلوماتية في أي مؤسسة. في الوقت الحالي ، هناك مستوى عالٍ من الترابط العالمي للأعمال ، مما يزيد من الضعف العام لمنظمات الأعمال على منصة الإنترنت. من أجل أن تكون مجهزًا بشكل فعال لاستعادة الهدوء بعد وقوع حادث أمني ، هناك حاجة إلى إنشاء مرونة متطورة لأمن المعلومات ، يكملها نظام تكنولوجيا معلوماتي خال من الثغرات. يجب حماية جميع عناصر تكنولوجيا المعلومات بأفضل طريقة ممكنة بحيث يمكن تقليل حجم الثغرات. يعد أمن المعلومات ضرورة أساسية للمؤسسة حيث يمكن أن يساعد في الحصول على مرونة فائقة ضد الاخطار. بينما في مجال الأعمال ، أدى عامل التغيير إلى تسليط الضوء على مجال التحكم الإداري ، والذي ينبع من حقيقة أنه في هذا العالم سريع التغير والاختراعات المتطورة ، فإن الخطأ أو اللوم ليس فقط على أدوات تكنولوجيا المعلومات ، ولكن على البشر الذين يجب أن يحاسبوا في أوقات الازمات. المشكلة الرئيسية هي النظر إلى امن المعلومات كمشكلة فنية في حين أنه خطأ بشري. العالم المتغير ، عصر التقنيات الجديدة ، أنماط جديدة من الحكومة الذكية مصحوبة بمشاكل لا نهاية لها في الفضاء الإلكتروني بينما يصعب تحقيق أمن المعلومات. قوى التغيير لا يمكن تجنبها من أجل التأقلم مع السوق الحالية وإرضاء الجمهور. المصطلحات الجديدة المستمدة من هذه المشكلة يجب ان تدرس بعمق. الحل هو النظر الى امن المعلومات من الجانبين الإداري والفني من أجل تحقيق المرونة. اقترحت هذه الدراسة إطار عمل جديد يعالج القضايا المذكورة أعلاه لمشاريع الحكومة الذكية في دولة الإمارات العربية المتحدة. من أجل تحقيق المرونة ، نحتاج إلى النظر إلى أي تغيير مفاجئ أو حدث جديد (جيد أو سيئ) باعتباره خطرًا حقيقياعلى نظامنا الذكي ويجب أن نكون مستعدين جيدًا (إداريًا) ومجهزين جيدًا (تقنيًا) للتعافي والتعلم والتغلب عليها وحتى الازدهار بعد الصدمة.استخدمت هذه الدراسة المكونات الرئيسية لعملية الصمود وساهمت في توفير أداة جديدة وبسيطة ومبتكرة لكي تستخدمها الحكومات الذكية. كما أنها سدت الفجوة في الأدبيات حول قياس المرونة وفقًا للعوامل الإدارية والفنية. يتطابق النموذج المقترح مع احتياجات / ثقافة الحكومة الذكية في الإمارات العربية المتحدة وفقًا للمسح الذي استهدف 432 مستخدما لنظام الحكومة الذكية والذي قاس مدى الاستعداد وتحديد المرحلة التي هم فيها الآن من حيث مستوى نضج نظامهم ومرونته ضد الاخطار والهجمات الالكترونية المحتملة.

DEDICATIONS

I feel great gratitude, and pride to dedicate all of my research and work to the greatest mother and father of mine. Furthermore, I dedicate my work to my blessings, my seven uncles and four aunties. On this occasion I would also like to express my gratitude to my older brother who has been my companion on this journey.

ACKNOWLEDGEMENTS

I am thankful to everyone who cooperated and appreciated in this research. I am grateful to my supervisory team, Dr. Corenelius Ncube and Dr. Maria Papadaki. Furthermore, I am especially grateful to The Dean of Research Prof. Ashly Pinnington, whose kind behaviour and valuable guidance enabled me to accomplish my research objectives.

Table of Contents:

List of Figures:

List of Definitions and Abbreviations:

1. Smart government	2. Information Resilience
3. Telecommunication infrastructure	4. Network Resilience
5. Smart government project	6. Developing Organizational Resilience
7. Cyber Security	8. IBM Business Resilience Model
9. Cyber Security's Risk	10. Cybernetic Resilience
11. IT infrastructure Risk	12. European Union Agency for Network and Information Security Standards (ENISA)
13. Economic risk	14. Local Government Research Center Framework
15. Legal and Regulation Risk	16. Network Centric Warfare (NCW) Framework
17. Change Management Risk	18. National Academy of Science (NAS) Framework
19. Performance Risk	20. Internet of Things (IoT)
21. Risk Management of Cyber Security	22. Cybernetic resilience in the UAE
23. Resilience measurement	24. System's Maturity
25. Cyber Security Frameworks	26. Exclusive Cybernetic Resilience Framework
27. Operational Resilience	28. Resilience business projects
29. Supply Chain Resilience	30. IBM Business Resilience Model
31. Linkove Framework	32. Centric Warfare Framework

Chapter 1

Overview: Smart Government Resilience and Cybersecurity Risk Management

1.0 Introduction:

The system of Smart government is primarily based on both information and communication technology, which disseminate information regarding public services and the important activities of the government sectors via electronic means. Smart government services are prevailing, and in order to maintain public trust Smart government ensures that the information and privacy of customers and the government should be protected. The security of information is considered the most important element. In this ever-changing world 'cyber villains' are growing faster than the security solutions developed to counter them. Nowadays, the most worrying condition is that cyber criminals are more trained, persistent and skilled. Cybersecurity and resilience measures are thus in greater demand in recent times (Walser, Kühn, & Riedl, 2009). Due to the complex nature of Smart Government, a number of security issues have emerged. Smart Governments are in need of a sophisticated resilience framework to address these cybersecurity issues. Moreover, because of this rapidly changing world and the changing business environments as well as new styles of smart and electronic governments, understanding and adapting to the change factor has become a priority among all factors affecting resilience (Linkov, 2013).

Cybersecurity is the second dimension of this study and can be defined as the technologies, methods and procedures that are made to protect organizations and individuals from cyber criminals and villains (NASTASIU, C 2016). Cyber-attacks can harm organizational reputation no matter how resilient is this organization. The organization that suffers from the cyber-attacks holds

lot of problems like loss of reputation, assets, and business and also faces many fines and lawsuits. According to a 2017 survey conducted by the UK government on cybersecurity breaches, the cost of a cybersecurity breach for a large business is £19,600. However, the cost for a small business is £1,570. To cope with cyber-attacks cyber resilience is increasingly important (IT Governance, 2017).

A Smart Government project's main goal is to enhance the business arena in the country (Keys, Chhajer, Liu & Honer, 2016). Governments that use Smart Government systems should focus on preventing financial losses because of these cyber-crimes, as stated earlier. Countries should know how to learn from these attacks and how to be resilient to them by being flexible to any kind of change or disruptive event. Countries that have embraced these technologies and adopted the idea of Smart Government, have become international investment destinations, even in the media, commerce and economic areas (Kumari & Kumar, 2015). Thus, cyber resilience is a wider term that covers business management and cybersecurity. It not only defends an organization from cyber-attacks but it also helps in coping with the aftermath and ensures the survival of an organization from such attacks. Resilience equals the capability of the organization to succeed and prosper by preparing, anticipating and adapting to the sudden change and disruptions in the organization that result from a cyber-attack. Organizational resilience also enables a business to take risks with more confidence at a strategic level (Keys, Chhajer, Liu & Honer, 2016).

While developing a resilience strategy, three main domains of resilience should be considered, which are very necessary in every type of organization, either large or small. First, is operational resilience. The organization which is resilient has an in-depth understanding of the operations of the organizations and how it is working and running. To meet the needs of the

customers, the operational resilience is the identification of the specific operational developments or improvements in its products and processes. This shows the consistency and potential of the organization to fully achieve and grow in any circumstances (Kerr, 2016).

Second, is the supply chain resilience. To achieve resilience, the organization needs to have more focus on the identification of risks in order to minimize the disruption and to maintain its financial reputation. Third, is informational resilience or cybersecurity resilience, which is very important and critical. To maintain resiliency, an organization must protect its customer information. This requires robust information security techniques to securely gather information and process this data (Kerr, 2016). This is especially the case for Smart Government where sensitive data about a government and its public/customers are stored in its smart systems, which need to be safeguarded and protected at any cost (Annareli & Nonino, 2016).

Moreover, some authors considered resilience as a risk management technique or a more mature level of it (Linkov, 2013). The concept of risk management is considered as fundamental for any business and organization's security. Information technology departments rely on risk management techniques, strategies and education to address cyber-attacks. With the increase in cyber-attacks, the techniques of cybersecurity risk management have also increased. Cybersecurity risk management involves the realization of threats and identifying "vulnerabilities", developing strategies and applying these to minimize the potential threat (Britt, 2017). The vulnerability factor is the traditional factor that affects resilience, whereas this research emphasized the role of the change factor as the new priority in resilience frameworks.

A turning point that highlights the importance of resilience frameworks, especially for government organizations, took place earlier this decade. The USA Guardian NP (2013) released a sensational article concerning private National Security Agency (NSA) documents in the United States of America (USA). The case emerged because of a young man, who had been working as a NSA contractor for a few months and who managed to breach the NSA's private files concerning security and political matters between the USA and other countries around the world. The retrieved private files were then ultimately publicly published.

The case was defined as the turning point in the history of the cybersecurity arena. The contractor took a risk to uncover the private information of governmental documentation in the security field. Some would consider his action as heroic behaviour in the sense that it promoted transparency between the public and its government. Of course, this varies based on the existence of different understandings of secrecy and transparency among the public and the government itself (Ginsberg et al., 2012). On the other hand, some would think that it was unethical and unprofessional and could lead to a national security disaster, as all governmental documentation is considered to be sensitive, confidential and dangerous, especially when exposed to the public, let alone for the USA which has been the number one target for terrorist cyber-attacks according to a study conducted in 2013 (USA Today, 2013). The UAE government, has witnessed similar cases of cyber-attacks, however, there is limited information about these incidents. Notably, new legislations have been embedded into law by the Prime Minister of the UAE due to the repetition of theses cyber-crimes (*Dubai.ae*).

However, it is noteworthy that cyber-attacks have emerged as one of the main problems for the governments of different countries all over the world. In many cases breaches come from within the organization's staff. Unfortunately, most risks and threats are hidden within the boundaries of

the organization itself. A survey conducted in 2006 entitled with “Information Security Breaches”, conducted by the DTI and PricewaterhouseCoopers found that approximately 32% of cyber-attacks are performed by internal staff, whereas only 28% of cyber-attacks are performed by external staff, such as stakeholders and external clients or attackers (Patel, 2006). Moreover, cyber-risks appear not only from internal staff that have access but also outside the government where anyone with malicious intent can attempt to commit a breach of the system. According to Gary Hyslop (2016), risks could come from internal staff and from external stakeholders, which he called the “third party”; Hyslop argued that organizations can avoid such cyber risks by creating work processes with closed-ended cycles, meaning every process of the electronic system should start and end within the same staff group without involving any third party external to the organization. This, he argued, should minimize the risk that comes from staff who have access to information and files. In conclusion, cybersecurity problems result due to human errors before technical errors.

Nowadays, while most governments are implementing some form of Smart Government, the risk has expanded exponentially, as the internet tends to be easier to hack and the risk management is questioned for its absolution in most cases (Widmer, 2013). It has been found recently that the notion of risk management is not enough in many cases of cybersecurity risks, and the need for system security theories has arisen, especially when it comes to the resilience in the case of complexity and vulnerability of the Smart Government system (Sikula et al., 2015). This brings the debate back to the main problem of this Smart Government initiative in terms of the cybersecurity risks. Afterall, it begs the fundamental questions: Does cyberspace hold an unavoidable risk? And can this risk can be controlled or not?

The change factor led to highlighting the role of management control in resilience frameworks. Studies show that management control is more effective than strategic management,

due to the fact that leadership does not have great impact on resilience. Leadership should avoid the traditional leadership pathologies in a crisis situation (Boin and McConnell, 2007). Resilience and management controls outdo the leadership, which does not prove to be a great factor in the success of organizations over the years, whereas management control in the "Enterprise Resilience" is more measurable and manageable (Chesley & Amitrano, 2015).

The reason behind highlighting the management control role, is that human errors overcome technology errors in times of cybersecurity crisis. This means the problem must be looked at from both perspectives, managerially and technically. This research concerns the managerial perspective; are not these cyber-crimes committed by humans? Are not humans dealing with it? Therefore, humans are the ones that should be held accountable during a cybersecurity crisis (Pennathur, 2001). Cybersecurity risk, when put in a business context, reflects the reality of the similarity between the traditional "pre-automated and pre-internet" business risks (Lanz, 2016). This remarkable step towards a cyberspace communication world has its own disadvantages such as the vulnerability to risk; where burglars and hackers are not slowing down any time soon, and always looking for weak points in new systems to commit a breach. This growth in cyber-attacks highlights the huge amount of risk which those new means of communication are facing each day, which are hard to handle from a security perspective. At this point the issue of cybersecurity is raised, and it is even more important for some countries to develop Cybersecurity Risk Management.

The Internet forms a backbone of Smart Government projects, which depends entirely on cyberspace where all of associated processes take place online; but the industry has been slow to embrace this form of risk management due to the risk that lies beneath the vulnerability of the online-based processes of the system. While the Internet has become an essential communication

medium, it is a medium that demands innovative thinking and implanting cutting-edged cybersecurity strategies, and demonstrates new plans, tactics and IT instruments that cannot be ignored by Smart Government staff. Knowing which tool to use, and when, is a strategic matter, especially when it comes to cybersecurity risks. Here arises the role of the System Maturity notion, and many of its associated methods, which offers a solution to the challenges of risk resilience, variation, differentiation and measurement (Barrinha, 2016). When integrated into a strategic electronic communications effort based on solid and business-oriented objectives, the Internet can make it easier to achieve those most effective win-win scenarios (Holtz, 2002).

This research discusses resilient measurement in relation to the cybersecurity, in smart government in the UAE, concerning the two main parts of this study: smart government resilience and cybersecurity risk management. In addition, this study discusses the Smart Government maturity level in terms of using resilience and risk management strategies and plans, what they are doing and how they are doing it, besides determining the cybersecurity risks accompanied with those processes. This is done to find out how practitioners can measure the resilience in relation to cybersecurity, by using the System Resilience and cybersecurity risk management theories. In order to determine to what extent they can control the risks posed to the Smart Government system "management control", they need to realize how to be resilient to risk. The research objectives will thus be fulfilled and this study will serve the overarching goal, by suggesting the necessary components of the resilience framework that have the ability to measure the resilience in the system of Smart Government. This will be of value to the Smart Government professionals and practitioners who will be made aware of how to control cybersecurity risk and achieve and maintain resilience.

Measuring the resilience in the governmental field is not easy (Sikula et al., 2015). In this regards, this researcher attended "The Enterprises risk Management of Cyber Security 2017, which was held in Dubai, and one the most famous British hackers (Brian Kuyfyt, 2017) talked of how Cyber Security is really difficult to achieve in the age of the internet. He explained how Google itself can be a dangerous tool with its information-hungry features which can be used as tools to hack hundreds of classified files of companies in one minute, by a click of a hacker (The Enterprise RISK Management Conference, RISK & Cyber Security 2017). Finally, the study tries to show that risk can be controlled to some level, but the traditional methods of cybersecurity risk management no longer work and the need for new resilience strategies and "capabilities" is fundamental to any Smart Government project; furthermore, it has a considerable and deep impact on cyber resilience and the control of cybersecurity risks.

Gerben, Peter, Margareta and Gerard (2015) presented that beyond the IT domain, cybersecurity is considered as one of the major concerns that promotes the idea of corporate governance. In this era when the level of cybercrimes and threats has increased, the need for robust cyber management frameworks has become more critical for both government and public organizations (Onwuldike, Lock & Phillips, 2015). In the UAE, the government has taken major steps to establish awareness by educating the public with regards to the attacks, past incidents, and the present vulnerability. In the past few years, it has been seen that the government of the UAE is involved in implementing initiatives to boost the responsiveness to cybercrime by paying attention to resilience. It has been seen that the cyber resilience is one of the major domains of the cybersecurity framework, which is based on the idea of maintaining flexibility of cyberspace. This ensures the availability of IT systems and resilience to attacks. Cyber resilience aims to provide a

protected and secured system and resiliency framework that allows the secure exchange and flow of information using the advanced mechanisms to combat the threats (Brecht, 2015).

1.1 Problem Statement

The problem domain of the study is the smart infrastructure of Smart Government. The traditional risk management strategies no longer work in the constant changing governance and business worlds, the new styles of Smart Government and the new innovative business environments are accompanied with endless problems in cyberspace, whereas cybersecurity appears to be very difficult to achieve and maintain. The reason behind this difficulty is that the internet and cyberspace were created to indorse connectivity not security in the first place. Nevertheless, the change factor is unavoidable, in order to cope with the existing market and to please the public. Therefore, the researcher referred to this as the forces of change in this study. A lot of new terms are derived from this problem such as, cyber defence, cybersecurity, cyber resilience and even cyber war, which are mentioned in many cybersecurity and cyber resilience studies, and need to be addressed, studied and defined in depth.

The problem is that most of the resilience frameworks out there are theoretical but not practical. Whereas the essence of resilience plans is the exercise, meaning the framework has the ability to be exercised over and over again until the organization reaches a level of maturity and be called resilient. This is actually what distinguishes resilience from traditional risk management tools. Planners and resiliency teams should be given a greater role in the Smart Government organizations and should have the full support from the top management; considering their role in making the Smart Government resilience a reality, rather than just giving theoretical assumptions.

Smart Government projects should place more concern on management controls over strategic management in this case.

The solution is to look at cybersecurity from both managerial and technical sides in order to achieve resilience. Cyber resilience also creates up-to-date resilience plans; which is essential because villains are growing faster than cybersecurity solutions and one should be innovative in fighting these cybercrimes constantly and even learn from this experience. Suggesting a new framework that addresses the above issues to Smart Government is a solution offered by this study. In order to achieve resilience, practitioners need to look at any sudden change "change factor" or disruptive event (good or bad) as a serious risk to a smart system and there is a need to be well-prepared (managerially) and well-equipped (technically) to recover, learn, overcome and even prosper post-trauma.

In cyber-crimes, it has been seen that there are no borders for hackers. As a result, the threat and challenges to cybersecurity have become a major concern for both government and public organizations. The growing use of technology has increased the dependence on information technology to store, sort, analyse, and evaluate the data and information related to different people and things. In recent years, the researchers have identified that the threat to cybersecurity requires the attention of people. As a result, the concept of cyber defence, cyber resilience, and cyber war have gained significant attention. Information is considered as a weapon or power and its protection is essential. For this, governments and organizations need to be aware of what they are protecting and what they are protecting from. The use of security management and risk management techniques and cycles can be utilized to manage resilience (Blanchet, Nam, Ramalingam & Martin, 2017).

The usual strategies that already exist in most organizations lack the ability to assess or to evaluate the quality, while also failing to consider business continuity planning, which is really documented and well employed in times of crisis, such as a crisis of technology breakthrough. Even in most cases, traditional plans consist of required elements but lack logical action planning, which creates a significant gap and difference between the plans content and what is being submitted for review. Therefore, this thesis focuses on Smart Government resiliency and cyber security risk management, from a managerial perspective. This thesis emphasizes the role of resiliency frameworks in resolving the security issues that take place in the smart infrastructure of Smart Governments.

1.2 Theoretical lens and focus

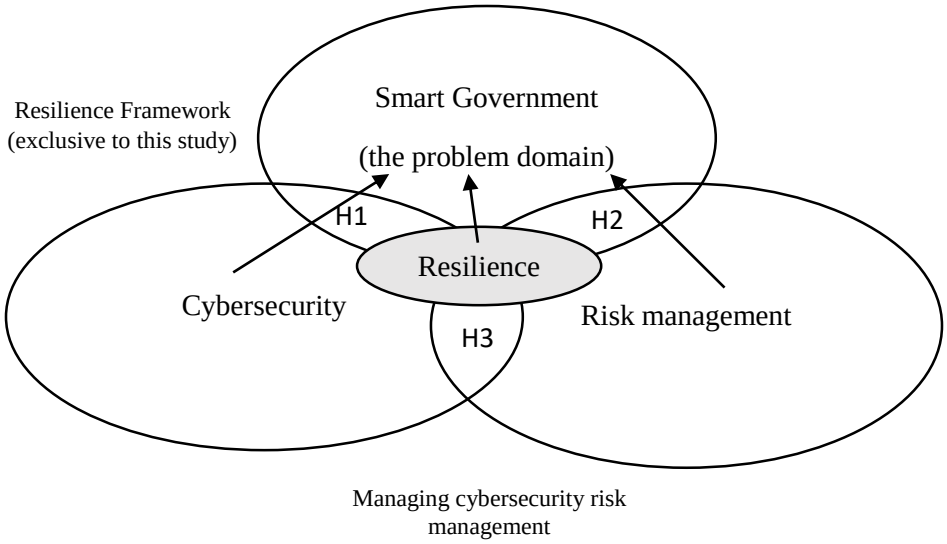

Figure 1.1: Scope of the Study

The hypothesis will be explained in detail in Chapter Three: Theoretical Framework of this thesis. The general hypotheses in short are: 1) the first hypothesis will emphasise on whether the

governmental organizations under the Smart Government umbrella are using the frameworks of resilience and cybersecurity risk management, or not; 2) the second hypothesis will concern the maturity level of several governmental organizations under the umbrella of Smart Government in terms of using cyber resilience and cybersecurity risk management, to explore whether the differences depend on the kind of an organization or on its system maturity; 3) the third hypothesis will consist of the relationship between the main two elements of this research: cyber resilience and cybersecurity risk management.

Nevertheless, cyber resilience is the ability of an organization to recover from a cyber-attack. Therefore, cyber resilience is the key element for organizational sustainability. There are several moving parts of cyber resilience that should be approached methodologically. There are five interconnected domains of the cyber resilience framework; each of those domains has a different function. The domains are: identify, protect, detect, respond, and recover. The resilience framework (figure1.2) is all about detecting, preventing and recovering from a cyber-attack. Therefore, cyber resilience is the key to the sustainability of an organization. The Smart Government resilience framework of this research is as follows:

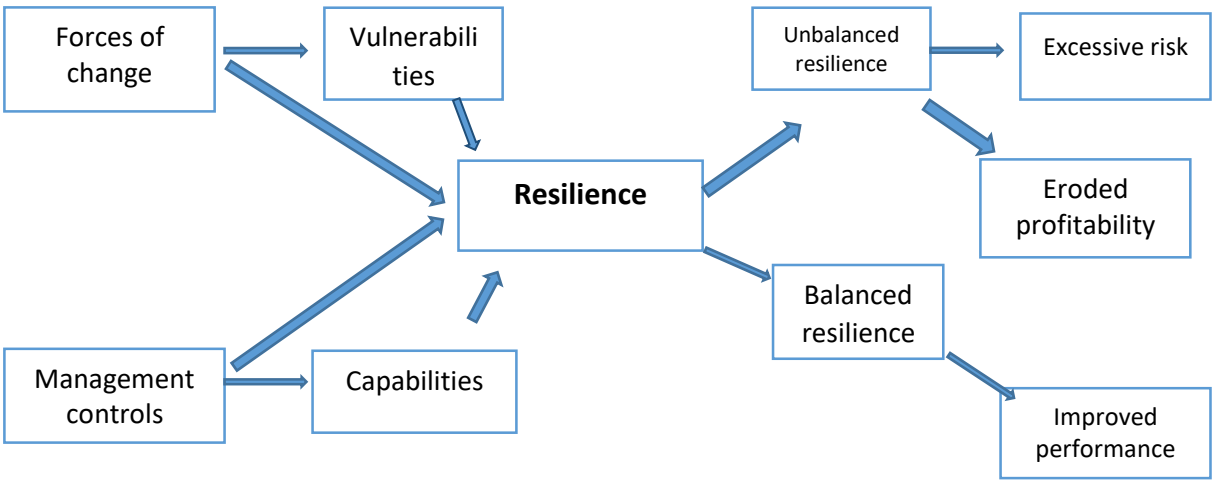

Figure 1.2: Framework of Study

Thus, resilience is affected by the important variables of vulnerabilities, forces of change, management controls, and capabilities. Finally, resilience shows output in the form of balanced resilience, improved performance, or unbalanced resilience and eroded profitability. The main factors of vulnerability, management control, capabilities, and forces of change have further factors that control them.

- ***Vulnerability Factors***

Vulnerability factors include turbulence, deliberate threats, external pressures, resource limits, sensitivity, connectivity, and disruption by supplier or buyer of the product/service.

- ***Capability Factors***

The key capability factors are flexibility in sourcing, capacity, flexibility of order fulfilment, efficiency, visibility, anticipation, adaptability, recovery, disruption, collaboration, organization, security, market position, and financial strength.

- ***Forces of Change***

Internal and external change in an organization, such as social change, political change, environmental change.

- ***Management Controls***

Management control create capabilities for proper functioning and resilience against cyber-attacks.

If the capabilities increase in the organization, there is less vulnerability. Thus, there is linkage between vulnerabilities and successfully used capabilities to face those vulnerabilities (Lambert & Knemeyer, 2004).

Therefore, the specific hypotheses of this thesis will be as follows:

H1

The capability factors affect resilience in Smart Government organizations.

H2

The change factors affect resilience in Smart Government organizations.

H3

The management control factors affect resilience in Smart Government organizations.

H4

The vulnerability factors affect resilience in Smart Government organizations.

1.3 Research aim, questions and objectives

The purpose of this thesis was to study risk-based cybersecurity frameworks which use cybersecurity developments to create a strong, protected, complete and hard to break smart system. This framework can be adopted by a Smart Government project; it can help the project to achieve Smart Government resiliency and manage the cybersecurity risk, in addition to avoiding repetition of past cybersecurity mistakes made previously by Smart Government projects. This research is aimed at measuring the resilience of the smart systems' processes to fill the gap in the literature on resilience measurement in relation to Smart Government and risk frameworks in the cybersecurity arena, to determine which framework is proven to be the most effective for this topic. The intention is to use the above techniques, to develop the right framework of Smart Government resilience and cybersecurity risk management.

This thesis investigates a Smart Government system's maturity and measures its resilience level, assessing whether it is in the very basic risk management level or in the advanced matured resiliency level. The suggested resilience model for the Smart Government project helps it meet its goals and keep its promises to the citizens by mitigating cyber risk and creating the maximum level of resilience and security to its smart systems. This is done in order to be able to achieve the best quality for online services, without playing by the rules of terrorists and hijackers and will eliminate the number of cybersecurity crimes in Smart Government systems. This kind of study also serves a greater purpose in the national security context; by creating a hard-to-breach system, sensitive government information will be highly protected and federal information will be kept safe from being exposed to the public, let alone sparing the country of the political and financial problems that come from a cybersecurity crisis and cyber-attacks.

The objectives pursued in the thesis are:

Objective 1: To determine and identify the components of the professional resilience framework to achieve Smart Government resilience and cybersecurity risk management.

Objective 2: To elaborate the risk management frameworks for cybersecurity in Smart Government.

Objective 3: To evaluate the existing resilience frameworks and identify the areas of potential improvement.

Objective 4: To develop a sound model for Smart Government organizations, on the measurement of resilience.

This Research is guided by two main questions:

RQ1: Validating the framework of Smart Government resiliency and cybersecurity risk management.

RQ2: How to evaluate previous frameworks on the measurement of resilience.

1.4 Contribution and novelty of the research

Information technology in the recent era is extremely important. With the passage of time people are getting more used to this technology by using more internet services and computers. Every single person uses some form of digital media. Smart Government is also providing many

e-services to citizens. To achieve the trust of customers governmental organizations need to maintain their customers' privacy and security. However, in spite of all the security plans there are a lot of hacking cases. The more the technology is becoming advanced the breaching of security is also getting advance. Many organizations are facing lawsuits because of breaching of security. This research will include a significant scope in terms of resilience and risk management of these organizations and the numbers of system breaches.

In the last decade, countries around the globe have been drawing significant attention to strategies and methodologies concerning Smart Government. In the same regard, a few "very" fast growing countries have taken a step ahead and succeeded previously in terms of execution, activity and delivering fancied effects. The fast movement of certain cities begins with pioneers who always encourage change to achieve advancement, can bring more the benefits of quick reactions and affects (Rahman et al., 2013). The concept of quality in any organization's culture across the globe will be defined and outlined when perfect and flawless models drive towards Smart Government that are prepared for emergent threats and risks.

This research will contribute in:

- Filling the gap in the literature particularly in resilience measurement in relation to cybersecurity, especially in the case of Smart Government systems. A model (figure 1.2) that is original to this research will be suggested concerning the two main parts of this study: resilience and risk management.
- This model (figure 1.2) will be studied in depth and revised to match with the Smart Government system's needs and to be able to be used as an essential resource for the users of the system, such as employees, citizens and officials of the Smart Government entity.

- The above model (figure 1.2) will help secure the system by employing resilience standards within it, for the system to be equipped and prepared for the unforeseen events that might threaten the functionality of large-scale projects, such as Smart Government. The focus will start by examining the existing frameworks ability to identify the maturity level of the Smart Government system. Of course, from a business management perspective, the researcher will try to manoeuvre between two main elements: 1) the latest policies and developments of cybersecurity; 2) the number of breaches; and 3) the frameworks of risk management. Without touching the computer science and programming arena.
- Moreover, the thesis contributes in focusing on the issues of cybersecurity in the prime time of Smart Government projects, which will provide the internal and external users of the system plans and evidence to be better prepared for any kind of risk or opportunity. The method should be scientific and well-planned, which brings the focus back to the resilience and resilience measurement and system maturity frameworks, which could work as proactive plans rather than being reactive.
- The notion of "change" appears frequently in the information and communication technology industry. It is considered as the most important change in the twentieth century and even before that; and in many scenarios this industry is becoming a creator and innovator for more changes in every aspect of life and other industries. This change reached out to both, public and private sectors, where new information and communication technologies have been implemented since. Meanwhile, hackers have grown bolder every day, therefore this thesis framework contributed in providing a new tool as weapon to face these burglars.

- Raising the awareness of Smart Government resiliency and the cybersecurity risk management topic. Cities that are joining the Smart Government project must be fully aware of all kinds of risks that may affect the governmental field and, in some cases, will lead to catastrophic results, or whether the Smart Government risk management practitioners are ready, aware, equipped and prepared for such huge transformation. It has been found that there are too few studies concerning the measurement of resilience.
- Furthermore, the lack of resources about models concerning system maturity in Smart Government as a means of risk management is evident. This thesis emphasizes the system's maturity issues, such as compatibility, effectiveness, and accountability, Smart Government employees must utilize effective cybersecurity strategies to achieve the overarching goals of their organizations, as well as those of their clients (Johnson, 1994). An essential question is raised here: how can resilience be measured in Smart Government organizations?

1.5 Structure of the Thesis

The introduction defined the main dimensions of the research. The first dimension is Smart Government resilience and its main issues, in addition to highlighting the change factor and a discussion of why it is a priority as a component in designing contemporary resiliency frameworks. The second dimension is cybersecurity risk management and its main areas, especially cyber resilience in the business context. Finally, on the measurement of resilience, the introduction highlighted the previous frameworks that were used to develop the framework of this research,

such as Linkov (2013), Kerr (2016) and Hyslops (2016). The remaining six chapters explain how the questions of this research are answered and how its aims are met.

Chapter 1 also consists of the problem statement, as well as the motivation to choose this topic, while pointing out the historical turning point on cyber resilience and how it is important for governmental departments as a national security matter. Moreover, the theoretical lens which consists of general and specific hypotheses along with the conceptual model and the methodological framework of this research are included. Nevertheless, research aims and objectives along with the contribution and the novelty of the thesis and the thesis structure.

Chapter two describes where the problem is exactly and explains the scarcity smart government resilience studies and the lack of smart government resilience studies. Chapter 2 is a systematic review of more than 70 quantitative research on this research topic and 30 qualitative and mixed methods more research. This chapter consists of a literature review on the first dimension, Smart Government resilience and Smart Infrastructure where the greatest risk entity exists, and where the suggested framework of this thesis can be applied for security and protection purposes. This literature review chapter also points out the strong correlation between the highly integrated infrastructure cities around the world, such as Dubai, and being highly targeted by hackers and hijackers and how this is a symbiotic relationship. In chapter 2, the second dimension of the thesis, cybersecurity risk management is explored and a description given of the different stages of the system's maturity from the reactive stage (no plans or strategies are used to address change), to the proactive stage (using risk management plans and framework), to the maturity stage (applying and exercising resiliency frameworks). This chapter discusses previous frameworks on

the measurement of resilience, and cybersecurity risk management techniques, plans, strategies and theories.

Chapter three consists of a review of quantitative theories used for measuring resilience, plus a review of the existing resiliency framework. It also justifies the evaluation of the previous frameworks based on certain criteria. The researcher developed a conclusive model that covers all the important matrices in the previous frameworks at the end of the chapter to be presented in future conferences. In addition, certain criteria for evaluating resilience in cybersecurity in relation to the business management field are detailed. Last but not least, the chapter presents a linkage of the new criteria to the literature review on how to measure resilience, to develop a methodological framework on resilience.

Chapter four consists of how the researcher investigated the hypotheses of the study quantitatively and the reason behind choosing a quantitative method to conduct this research. In addition, an introduction to the relationship between cybersecurity and resilience in Smart Government is given, tying it to the business management arena. In this chapter the researcher included a justification of using a quantitative methodology, validity and reliability of the measurement method, and theoretical validation. Reliability is tested by a pilot study as well, for the items of the survey, given to the group of 15 respondents twice to test the time reliability of the test and the results revealed the stability of the responses of the same 15 respondents over time. Chapter four includes an in-depth analysis of the literature in comparison with the current method used to validate it, along with research philosophy, deductive method, ethical consideration, methodological limitations and a chapter summary.

Chapter five presents the findings obtained from the survey. There are different sections in this chapter, that include results and findings, which are further divided. The chapter presents the demographics of the participants and then moves towards the analysis of questions asked. In addition, the summary of correlations, and ANOVA tables have also been provided along with the elaboration of reliability analysis. The chapter elaborates on how the study tests relationship between two or more variables and how hypotheses are developed which can be tested using quantitative analysis. Nevertheless, this study is empirical and quantitative and it depends on numeric data. The study showed that measuring resilience needs quantitative methods and research. The researcher tested the hypothesis in a numeric way and then prioritized the main factors that have greater impact on resilience. The chapter also clarifies in detail how the researcher designed the questionnaire according to the dependent and independent variables of the research.

Chapter six consists of a discussion on the results of the survey and the research, and a discussion on the distinguished findings of the research, along with a detailed table on the main findings, results and surprises of the research and how these can be addressed. The chapter also develops a discussion on the research questions and objectives and how the researcher answered them and tested the hypotheses of the thesis. The chapter also includes a discussion on the components of a professional resilience framework, which serve business continuity as an overarching goal of Smart Government resilience. A summary of the chapter is also given.

Chapter seven consists of the practical and theoretical Contribution of the research and longer terms goals of this research. Chapter seven also includes suggestions on new areas of investigation. Conclusions and recommendations are included as well. In this chapter the researcher included the contribution of the quantitative method to the resilience measurement

research arena, in addition to a practical example of using the evaluation method of the research. The researcher also explained how the study will function in the actual world and how Smart Government organizations worldwide and in the UAE can benefit from this research and use its framework to measure and achieve resilience.

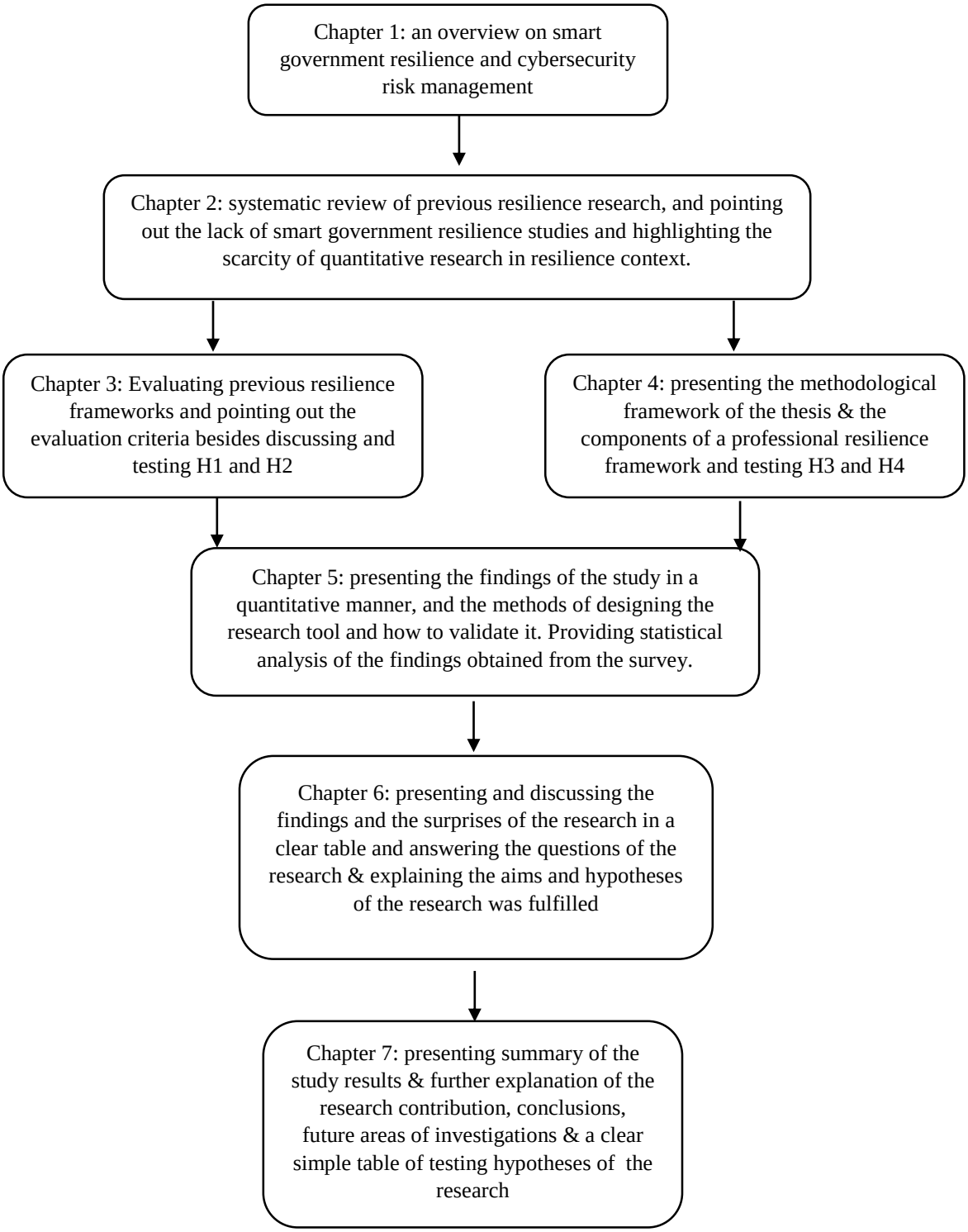

Figure 1.3: Structure of the Thesis

Chapter 2: Literature Review

2.1. Smart Government Resilience

Smart Governments emerged as the most remarkable results of the cybernetic revolution, and as a type of virtual community from the 1940s. Smart Governments were launched at the end of the twentieth century as administrational services, or what could be called, 'distance administrating' (Zamoum, 2007). Smart Governments aimed at supporting IT, businesses and investments in the country through improving its infrastructure; it also facilitates public services, which reflects democracy and transparency. It was rapidly developed to become a primary tool in the continuous and general development process, besides opening some areas, such as quality, competition, and implementing successful government systems that increase interconnectedness of businesses on local, regional and international levels (Scholl & AlAwadhi, 2016). Due to the complex nature of this smart tool and the vulnerability of cyberspace, Smart Governments focused on how to be more resilient to risk, by applying resiliency plans to deal with cyber-attacks and online attempts to breach to related systems (Bosen, 2017).

2.1.1. What is Smart Government?

According to Rahman et al. (2012), Smart Governments are organizations that employ ICT through the internet to run governmental business, activities and investments with all partners and stakeholders. These smart projects benefit from technology, cutting-edge policies and business models to be able to study and identify the changing environment. It tackles financial problems and focuses on public service in order to support its continuity and sustainability and to please the audience (Dolicanin, 2014). Smart Government is a public virtual portal that provides information, services, and helps citizens, especially in administration and business. In addition, it facilitates the

daily processes of individuals and companies, which can shift the perception of individuals towards the role of recent governments in improving their environment. Smart Government also works on developing different policies regarding the validity and the security of information, through using new technologies (Zamoum, 2007).

Oliver and Sanders (2004) prefer to use the concept "Integrated Governance" rather than Smart Government. They argued that this concept is more accurate and reflects the nature of the interactivity combination that stands between the citizen, the IT and the governmental e-services. This is especially true when the IT is middling in directing and organizing an individual's and an organization's affairs. Moreover, it directly affects a government's relationship with its citizens, and contributes to rethinking democracy in the new millennium, which consists of challenges, such as transparency, equity, and privacy.

Smart Governments have three bases: information, computerization and communication technology. In addition, they strive to achieve specific goals, such as improving the levels of cybersecurity, interactivity, qualification, and effectiveness among all the governmental and non-governmental organizations, and facilitating access to information when needed by different organizations, simplifying the accountability and transparency, as well as electronic shopping which is the new trend of global commerce (Rotchanakitumnuai, 2007)

In order to build e-services, countries need to lay down a general plan to enable the transfer from traditional services to electronic services. These include the emerging e-services and building a human cadre that is able to use and adopt various techniques of IT, and establishing communication infrastructure, such as highways in the internet business, and importantly, identifying the public needs (Rahman et al., 2012).

In general, the main criteria for any community to be able to enter the space of virtual communities and build a Smart Government is to work on these aspects: first, providing communication and information infrastructure by developing the information systems and communication nets; second, digital economies rely on computer and multimedia as media of commerce and business activities; third, the information society consists of people who are able to use the Internet with enough experience to link the traditional activities with economic, cultural and scientific changes, as products of the digital age; fourth, digital authority, which is reflected in the ability of the government to impose the extension of its digital power, through providing different kinds of services and legislations to support the digital activities in this new society (Zamoum, 2007).

This hypothetical and virtual space has cancelled all the place and time elements, and re-conceptualized the boundaries facing users, photos, information, items, and money, as well as the way of thinking. These virtual nets are expanding place and time limitations in every aspect, such as video games and entertainment, interactive cinema, virtual life, education and culture, including treasuring cultural heritage, exploring art works, virtual museums and governmental e-services (AlKuwaiti, 2017).

Technological interactivity represents real democratic success for information and communication technology, where the computer can respond to us and accomplish our desires; it only takes a tap on a button to obtain the desired information. That represents the technical base every Smart Government needs. Through technological interactivity, audiences have transformed from passive receivers to positive and interactive ones (Dolicanin, 2014).

Western governments realized the importance of this communication and information revolution in the 1980s, while eastern governments realized its importance in the 1990s, and its

significant role in interacting and communicating with its citizens in all arenas: politically, culturally, economically and socially. New communication technologies contribute to facilitating public and company services, and guarantee information security and transparency to some level (Scholl & AlAwadhi, 2016).

2.1.2. Smart Government Project

Countries around the world have embraced these technologies and adopted the idea of Smart Government, which enabled them to be attractive international investment destinations, even in the commerce, media, business and economic areas. Through their massive investments in new technologies and the launch of projects in the early 1990s, which attracted international companies in the Internet and IT space, the American Smart Government, Canadian Smart Government and UK Smart Government projects represent a remarkable move towards a new century; because these have led the experience across the world, especially when it comes to the electronic services (AlMatroushi, 2017).

Whereas, in the developing countries Smart Government projects face a socio-economic status as the number one obstacle that stands between turning such projects into reality (Holtz., 1999). Due to the relatively expensive cost and the need for internet connectivity it has been found that poor countries or developed countries with poor people cannot use Smart Government systems. This is why it is a late step for developing countries to take. They need to make sure that they have reached a certain economic level to be able to implement this kind of Smart Government in their regime, they also need to define the relationship with the public and to look at the political stability issues before taking this step (Ginsberg et al., 2012).

The Smart Government as a project which consists of different features, is turning into a reality through different stages, which include achieving a customer-centric approach with government e-services (where the customer is a priority). Moreover, employees are considered as customers of this new system and should benefit the most from its ability to save time and effort with such high levels of technological instruments and online processes, in a safe and secure cyberspace. This increases effectiveness and efficiency, and simplifying and streamlining government services using technology as a key enabler. In conclusion, a Smart Government system innovates new government systems and business processes and services (AlKuwaiti, 2017).

On a local level, the UAE smart government took place, whereas the Prime Minister of the UAE declared that Dubai city is heading towards a new smart century, which means a huge jump in telecommunication infrastructure and investments. Huge investments and ICT projects are taking place nowadays in Dubai city and across the UAE, especially for Smart Government projects and smart governance initiatives, which have already been launched in the UAE and will be completed by the end of 2020 (RISK Management and Cyber Security Conference, 2017).

The Smart Government project in the UAE has a strong impact on business management and the IT field. It also helps significantly in drawing the attention of big investors from around the world towards the UAE. This smart initiative uses the advancements of IT strategies and processes along with business management and resilience frameworks. It provides funding for important projects in the business and IT industries that are related to this field, such as: innovative projects, Internet City, a free zone and free-trade zones for e-commerce. It also funded media and political projects, which have been successful through various channels and electronic services, which have helped in facilitating business connections and networks and communication processes locally and internationally (Scholl & AlAwadhi, 2016).

By leveraging Information and Communication Technology (ICT), cities with highly integrated telecommunication infrastructure are established as knowledge-based economies. This is now playing a significant role in improving the service and cybersecurity effectiveness and beneficiary to all kinds of organizations, in both the public and private sectors. Smart Governments are aiming at consolidating their achievements by creating an organizational culture of cybersecurity and creating systems with high resilience to risk; to ensure sustainable growth in public and private industries. In the meantime, it is building a strong infrastructure and enhancing its services. Of course, that would be achievable with a highly trained cadre, along with good strategies and scientific methods to face the potential risks before they even occur and to minimize the impact of risks in the future (ALMatroushi, 2017).

The Smart Government project in the UAE has several projects which have a knowledge-based economy element using ICT as a key enabler. These include the Smart Government initiatives. The key components in this project economy are government, business, citizens and residents. Their interactions, for example, 1- Government-to-Business, 2- Business-to-Business, and 3- Government-to-Citizen, play a fundamental economic role and result in the exchange of goods and services. Recently, Smart Governments adopted the ICT as a tremendous change that is happening in their countries for the sake of these entities to become Smart Government, e-business and e-citizens. This e-transformation will contribute to positioning their countries as the competition of economy is growing worldwide coupled with high standards of living among citizens, residents, and investors (Bosen, 2017).

The Smart Government area in the UAE has been the site of significant investment by business and IT related companies over the past three decades. Especially in the business and marketing arena, the Smart Government project offers many core services, but its primary ones are

through its official public portal, which integrates the e-services of all the governmental departments. Other core economic and cultural services of Smart Government projects include e-ticketing, e-management, e-pay, e-learn, e-host, and its mobile services through the mobile portal such as Smart Government as a different version of the government (Kerr, 2016). Smart Government projects are heading towards a new era of virtual government with the implementation of smart systems which will facilitate the citizens business deals with the government (Rotchanakitumnuai, 2007).

Smart Government also has a corporate website, which details its initial and present accomplishments. All these websites are connected to each other, and consist of different kinds of processes which need resilience frameworks and cybersecurity risk management to protect data, these online processes need to address the problem, identify the potential risk, assess and prioritise the risk attached to it, then find out how to be flexible to any kind of sudden change or disruptive event. To be able to absorb change and mitigate risk they need professional frameworks in the area of measurement of resilience (Linkov, 2013).

2.1.3. Smart Government Resiliency

In the technology-driven era, the cybersecurity landscape is evolving like never before. According to the 'Cyber Threatscape Report' by Accenture, cybercrime campaigns are being designed in a sophisticated manner so that the vulnerabilities and risks of the users, such as individuals and organizations, will be increased. Currently, cybercriminals are able to adapt to the fast-paced technological setting. The ability of the cyber attackers to remain functional in spite of high-profile law enforcement actions show that the cybersecurity resilience and maturity of

organizations need to be strengthened (Hirani, Lasiuk & Hegadoren, 2016). The current criminal operations are being designed so that the chances of disruption and detection can be minimized. The changing behaviour of cybercriminals and online hackers has to be taken into account while designing the cybersecurity resilience of undertakings. This factor must be given high priority as it can impact the overall effectiveness of the resilience of the cybersecurity of a business undertaking (Hyslop, 2016).

However, this online smart tool presents many vulnerabilities and ambiguities in the smart system due to the complex and weak nature of cyberspace; this helps explain why there are so many cyber-attacks and cyber-crimes in the age of the Internet (AlKuwaiti, 2017). To establish Smart Government resilience, it is important to stand on the demands and needs of the system's security which can be catered to in an efficient and effective manner using ICT, plus non-technical solutions that are beyond the IT domain. Smart Government resiliency also involves inducing a cultural change whereby knowledge exchange is the norm and networks are at the heart of institutions (Kumari & Kumar, 2015).

The Smart Government project was turned into reality with the existence of different elements; one element is the communication infrastructure of modern cities in particular, and the developed countries in general. The USA, Canada and Great Britain have always been pioneers when it comes to adapting new policies and technologies, and they represent good examples of countries that are open to new developments, which help these countries lead in many areas. Since they have implemented and adopt Smart Government projects, they have witnessed a rapid development in telecommunication infrastructure. A strong correlation has been found between two elements: Smart Government implementation and the fast-growing and enhancement of the integrated infrastructure of any country around the world. Furthermore, it increases the potential

of being a target by terrorists and cyber-criminals around the world, therefore, such countries are under a great deal of risk due to their highly integrated infrastructure, such the USA which is classified the a number one target around the world, in relation to cyber-attacks (Ginsberg et al., 2012).

The governments of the three countries mentioned above have employed new policies and legislations to help make the environment more suitable for this new industry. Another benefit will be gained from these new legislations, which is to encourage investors from around the world to invest in these countries, which could lead to the birth of stronger leaders in the business arena.

Nowadays, the USA, Canada, and Great Britain have spent millions and millions of dollars on telecommunication infrastructure (www.wekipedia.com), therefore, internally, they have modern telecommunications infrastructure compared to other countries across the globe. Locally, Dubai has frequently been referred to as the "most wired" state in the Middle East (Dubai.ae). Local citizens have access to all modes of communication that Western nations use. ETISALAT (a famous telecommunication provider organization in the UAE) currently controls the telecommunications infrastructure industry and the majority of its related fields in the UAE. It has managed to provide and maintain a high-standards in its services which in most cases is similar to services in Western societies. According to Bosen (2017) government in the UAE is taking a proactive response for the safety of the country's digital infrastructure. The approach of the government is to safeguard the features of digital infrastructure from harm. The network helps in data exchange among government and local entities. The cybersecurity resilience initiative of the UAE government follows the introduction of the cybersecurity strategy in Dubai with the purpose of strengthening the position of the country as a global leader in safety, business, innovation, and management. The main focus of the strategy is placed on the domains of being a smart nation,

ensuring society's development, business entrepreneurship, innovation, cyberspace security, and cyber resilience (Dolicanin, 2014).

The government of the UAE is focusing on cyber resilience in order to avoid threats in the changing cyber environment. The Prime Minister of the UAE has recently launched the Dubai Cyber Security Strategy in order to strengthen the position of Dubai as a global leader in safety, innovation and security (Dubai.ae).

The changing environment brought to the UAE due to smart projects has become a problem, along with the growing demands of the enlarged population. In the light of all that, the government finds itself obligated to find sustainable, flexible, resilient and agile plans, with the right potentials and abilities to improve the emirates' infrastructure with longer-term standards of quality for its people (AlMatroushi, 2017).

According to UAE experts, by 2021, the total cost of global cybercrimes will reach $6 trillion compared to $1.2 trillion back in 2017. Smart Government websites and projects increase the global interconnectedness of business, whereas the global industry sector is most vulnerable to cyberattacks. The hybrid motive of attackers concerns their fast adaptability and dynamic movement towards technologies, which can be ahead of the industry itself. Cybercriminals are compromising the security system of smart business organizations for various reasons. Generally, the motive of an attacker is to gain financially by compromising the security posture of a firm. However, there are occasions when they have multiple motives and intensions such as ideological, financial, or political agendas. The organizations need to ensure that they devise functional resilience of cybersecurity, which can help the firm to regain their composure quickly and efficiently. The varying motives of the attackers can help to design an integrated and holistic cybersecurity resilience that will allow the business organization to be empowered against online

attackers and criminals. Nevertheless, the hacking industry is a very attractive one due to its immediate, fast and direct financial gains (Khaleej Times, 23 January 2020).

Therefore, Smart Government must invest in advanced resilient systems to establish full immunity against attacks, rather than just reacting to these cyber risks. David Young, declared that the period post-Expo 2020 will be a huge jump for the UAE in particular and the region in general. He said "The Expo 2020 will attract new businesses, talent, new industries and investments to the country." He added that the UAE will gain benefits in the short-term and long-term from the Expo 2020 this year and in years to come. This is why cyber resilience plans should be developed from now to avoid any disruptive event that might occur on the inauguration night of Expo 2020 by the country's enemies (Khaleej Times, 23 January 2020).

On the economic level, the UAE is moving very fast among the developing countries in the Gulf region (Zamoum, 2007). The UAE was established with a traditional government after the seven emirates united in December 1971. Then in the early 1990's the UAE initiated electronic government websites or the integrated governance which was completed in 1999. A year later, the UAE decided to move things to the next level by starting the Smart Government initiatives and initiating smart cities. The UAE has been able to flourish economically because of its massive oil wealth. However, even if a country has substantial oil reserves it must have a plan to diversify economically in to the non-oil sectors, the UAE has decided to go beyond its oil reserves and look into enhancing its infrastructure and supporting all kinds of commerce and business. It aimed at being a destination for entrepreneurs, investors and innovators from around the world. Supporting the business arena and economic investments was the number one goal for these smart projects, which can attract more and more business projects to the relatively newly developed country of the UAE (Scholl & AlAwadhi, 2016).

It was also a strategy to go beyond oil reserves and the petroleum industry for the country to flourish economically in every aspect. Since the UAE started to invest largely in a formulation that consists of a professional business environment supported with advanced telecommunication infrastructure, it has succeeded in changing the reality of its cities, where the city of Dubai is now called 'the most wired city'. This has resulted in leveraging awareness and enriching the culture towards the new era of the digital world. This affects the education, economic, political and cultural background of its public. In the case of the UAE, the digital hub has become a "catalyst for change" (Holtz 1999).

2.2. Cybersecurity Risk Management

Excellence in infrastructure emerges from the security fence that is built around it to keep it safe from cyber-crimes and terrorists. However, some say that if you build a fence, the hackers will build a tunnel to breach your electronic system. So, is there real cybersecurity in the contemporary world or is it just an optimistic idea to make online organizations, such as Smart Governments, feel safe, while it is far from the truth under the pressure of daily cyber-attacks. The Internet has become a fundamental medium of communication for governments, which gives us a warning to make it more and more secure for this critical environment. It is a strong, powerful, advanced and scientific tool, a network that can spread across the globe, and has international applications inside and outside organizations; here comes the role of cybersecurity which is going to be defined, analysed, and studied in depth in this section.

There is a gap in the literature about focusing on risk and opportunities at the same level, rather than just investigating the risk. Usually the higher risk lies always in the entity of smart infrastructure within the Smart Government, nevertheless researchers and authors should focus on human errors as well. Thus, the need for stronger, hard-to-breach systems is crucial, aiming for a system that is resilient to cyber-crimes and attacks. Thus, the need for managing cybersecurity risks and the role of risk management to accomplish this has been highlighted by a number of researchers and theorists.

Risk management tactics and strategies are a matter of keeping governmental data secured and protected, which helps in enhancing the defence level and making sure that the government can play its role effectively. In the past few years, it has been noticed that understanding cybersecurity and establishing an awareness of the associated risks is becoming a major concern especially in the IT domain of security, but somehow the researchers have failed in presenting an advanced framework to fully protect these systems from any threat or disruption. The need for resilience frameworks becomes crucial when risk management strategies are considered to be insufficient in many cases (Keys, Chhajer, Liu & Honer, 2016).

On the other hand, there is not enough information and research on Smart Government resiliency, which must be considered due to the complex environment of such cyber-dependent organizations. It has been noticed that governments around the world are using IT widely in their systems, and the need to integrate risk management strategies is increased nowadays (Gerben, Peter, Margareta & Gerard, 2015).

The measurement of resilience frameworks is found in the literature, but the need for evaluation criteria is a must, for the projects to be able to choose from them according to needs and

culture (Hirani, Lasiuk & Hegadoren, 2016). Recent studies show that the most vulnerable part of an organization's cybersecurity is the organizational personnel or the employees. Cybercriminals rely on the employee so that they will click on infected links or open malicious files that will release malware into the IT system of the organization. The resilience of cybersecurity has to be designed by keeping in mind that the threat actors adopt fake identities in order to engage with employees and collect sensitive and confidential information. The effectiveness of the resilience of a firm's cybersecurity largely depends on the awareness of the employees to deal with online attackers and cybercriminals (Holm & Ostergaard, 2015).

As per reports, more than ninety percent of cyber-attacks occur due to social engineering techniques that rely on human interaction to gain trust and manipulate them to break security protocols. Protection against such incidents can start, and robust cybersecurity reliance can be employed, only if the staff are educated on effective defence against security breaches (Holm & Ostergaard, 2015).

This study fills the above gap and shows how one can only achieve the above by analysing cyber resilience from both managerial and technical perspectives. Measuring Smart Government resilience and studying cybersecurity risk management can lead to an advanced level of security by intervening in all plans, frameworks and notions which will help us to deal with the emerging and changing threats and challenges. This study fills the gap on the measurement of resilience in relation to cybersecurity especially in Smart Government organizations, it addresses two of the most important dimensions that have great impact on Smart Government resiliency: change and management control.

2.2.1. What is Cybersecurity?

Cybersecurity is defined as controlling the access to information contained on networked systems. The reliability and trust in digital infrastructure of cyberspace depends on the effectiveness of cybersecurity controls. The role of cybersecurity professionals is to plan and design effective controls to ward off any potential attack on cyberspace components and effective mitigation of the consequences of such an attack. Since all the potential attacks cannot be prevented, it is therefore the key objective of security personnel to detect the attack and take control before any damage is caused (Keys, Chhajer, Liu & Honer, 2016).

In cybersecurity, the primary aim is information security and hence the concept of "respond" to an attack transforms into "recovery/correction". The critical business system is therefore completely reconstituted and recovered. Due to redundancy and diversity in the IT field, IT professionals assert that the damage caused by breaches of cyberspace are almost completely reversible. Thus, cybersecurity can be defined as maintaining availability, integrity and confidentiality of information on cyber networks by employing technology, people and processes (Bayuk et al., 2012).

Three important dimensions of cybersecurity are people, processes and technology. Continuous security improvement loops are created for better prevention of cybersecurity risks. People operate the systems by following established processes and routines thereby accomplishing missions of the system. Security cannot be achieved by technology or people (security professionals) alone. Success of security programs depends on the decisions and actions of the security professionals using them. Moreover, the overall security is based on the collective efforts of the security team which cannot be known if pre-planned processes are not in place. Thus, the

overall objective of cybersecurity is achieved when the security team integrates security programs with organizational processes strategically supporting them with technology in order to achieve the cybersecurity goals (Kumar & Kumari, 2015).

The other important aspect of cybersecurity includes a triad of three important dimensions of security, i.e., integrity, confidentiality and availability. These are information specific objectives of cybersecurity. Confidentiality is the extent to which a system prevents unauthorized access to information, while timely availability, accuracy and authenticity of the information are also equally important. However, some of these goals of cybersecurity are mutually exclusive, for example the availability of information makes the confidentiality of information harder (AlMatroushi, 2017).

2.2.2. Cybersecurity Risk

According to Lanz (2016), who held a study on a cybersecurity Risk and Audit Committee, risks should be addressed as a business issue rather than technological one; the right explanation in such cases concluded from focusing on the most significant risk faced by an organization then dealing with it; otherwise it is going to be too costly if the organization focuses on every single risk. The researcher argued that cybersecurity risks, when put in a business context, reflect the reality of the similarity between the traditional "pre-automated and pre-internet" business risks (p. 7).

Conteh and Schmic (2016) conducted a study to measure the amount of vulnerability in data infrastructure systems and focused on the "Social Engineering" attacks along with the potential risk and threats in both software and hardware assets. The study identified the risk of "Social Engineering" and designed a four steps model to address this: 1) start with gathering information; 2) then develop relationship; 3) exploitation; and 4) end with the execution step. The

hijackers or criminals usually use those four steps to commit social engineering attacks. The study suggests several motivations behind social engineering attacks such as financial, competitive and revenge purposes. The researchers added that besides all the mentioned motivations, some burglars do it just for fun! (p. 35).

Garfinkel (2012) conducted a study explaining why the problem of cybersecurity risks is getting worse every day; Garfinkel concluded that this was due to newly implemented IT systems with computer systems that are getting weaker, even more vulnerable than the traditional computer systems. He added that these new programs and systems are contributing to the rising level of vulnerability of cybersecurity. Furthermore, he went as far as suspecting that hackers are the ones creating these new security systems for cybersecurity. Even after extensive research on this topic and millions of dollars spent on cybersecurity the problem is not being solved. He added that cybersecurity risk solutions should be considered as an enabling technology not as a product; the risk will encourage up-to-date processes and will enhance the IT security system, meanwhile, a lot of business issues can be solved thanks to the cybersecurity risk which opened managers' eyes to fundamental skills and positive developments in all kinds of firms (p. 31).

Rechtman and Rashbaum (2015) conducted research on the risk of cybersecurity that lies within the CPA firms' boundaries in addition to the external threats. The two researchers argued that it is better to have a paperless environment for such firms; it could save time, effort and money of hiring more people for auditing purposes, whereas the risk of cyber-attacks will increase in this case; especially from the firm's employees who have access to the e-files. In CPA firms, critical information data comes with a high risk of breaches, where all citizens' bank and credit information are stored in their system (p. 56).

Mougan (2010) highlighted the issue of cybersecurity risk on the National Security Department of the USA; he suggested that a "Cyber security Agenda" should be used nation-wide to help solve the problem, and governmental and private institutions should work together. He added that if the USA wants to take the lead back in cyberspace, it should bring researchers and developers of systems together in one place; to be able to overcome emergent issues and come up with the best secured system for the benefit of national security. He also stated that the cybersecurity lifecycle of innovation needs continual testing and evaluating to achieve the best possible results in the cybersecurity arena. The study emphasises two kinds of partnerships the government should take part in: partnerships with educational systems and partnerships with the private sector; because sometimes the refusal of involvement from some organizations in the private sector could form a huge obstacle and slow down the development of the overarching goal of national security (p. 30).

Ruggeri (2016) wrote an article concerning the risk in financial organizations, suggesting a solution of backup systems that are not electronic and not connected to any electronic system. He offers some tips for always revising the crisis plan besides getting in alliance with key functions and/or players, for example, CISO, IT and Risk Management. After these two steps are well accomplished, one should recognize his responsibilities and become familiar with disclosure requirements (p. 13). Studies on cybersecurity risk have shown all kinds of risks but have not highlighted the issue of who depends on whom. Are cybersecurity developments dependent on Risk Management legislations, or whether Risk Management strategies are changing per the rapid growth of cyberspace. In this section the thesis shows a number of problems facing cybersecurity in every field, which could apply to Smart Government in general and the city of Dubai in particular; especially in the national security arena which forms a huge concern nowadays for the

government of Dubai, and should be taken into consideration, This is important as these new styles of government are more vulnerable to risk since the literature review above shows difficulties in handling such kinds of cyberspace, unlike traditional government styles where one can make sure that documentation and files are safe and unlikely to be hacked.

2.2.2.1. IT Infrastructure Risk

Smart Government comes from the usage of IT in providing the public services to the citizens and effective management (Guo et al., 2009). Therefore, the risk management of these information technologies is very important factor that contributes in the successful implementation of Smart Government (Woods, 2009). Due to its broader outreach and complicated structure, government agencies are faced with increased risk of IT management (Walser et al., 2009). It therefore contributes in successful Smart Government implementation processes. Some of the factors identified by researchers for a successful Smart Government implementation process are laws and regulations, user feasibility and technical capabilities (Belanger & Hiller, 2006).

IT infrastructure constitutes all those IT resources which are vital for implementation of business applications, as well as organizational communication. It comprises of communication technologies, computers, databases and technological platforms. It is the ability to make internal and external electronic communication linkages using hardware and software (Chanopas et al., 2006). IT infrastructure is integrated with front end user applications (Esteves & Joseph, 2008). It therefore directly affects the competitiveness of an organization.

2.2.2.2. Economic risk

Economic risk constitutes risks arising from changing economic circumstances, such as supply chain interruptions leading to financial and strategic issues related to competitiveness and

implementation of strategy (Matook et al., 2009). Financial operations and business management give rise to such risks and entails the potential loss of sales/money due to customer dissatisfaction from the product (Rotchanakitumnuai, 2007). If the quality of services is poor or not reliable, it can lead to economic losses and transaction failures (Ruizhong et al., 2010).

2.2.2.3. Legal and Regulation Risk

Since Smart Government structure differs from traditional government structure, this entails a change in relationships and hence the communication process among the stakeholders of the government. This means the laws and regulations as well as policies governing the activities of the government also change (Montagna, 2005). New laws and policies need to be developed which enable adoption of newer technologies while ensuring compliance with the constitution (Gil-Garcia & Pardo, 2005). Legal risk is the risk involved in breach of rights of citizens due to Smart Government thereby incurring loss (Bandyopadhyay et al., 1999). Potential lawsuits due to information leaks and other legal actions by citizen are also an important challenge for Smart government implementation success (Schneider, 2010). The regulations can also limit the ability of the government to initiate and complete Smart Government projects (Belanger & Hiller, 2006).

2.2.2.4. Change Management Risk

Change management risk is the risk inherent in changes in governance mechanisms through use of IT and the resistance to the change. It pertains to the technical aspect of process change as well as the behaviour aspect of the resistance and change management entails balancing the forces of change including its cultural impact (Montagna, 2005). Organization plans and attempts to reduce resistance and facilitate the adoption of new technologies (Iribarren et al., 2008).

2.2.2.5. Performance Risk

Performance risk is the risk inherent in the failure in the performance of the Smart Government services to meet the expectations of citizens and government alike, and chances of its malfunctioning due to design failure, amongst others (Featherman & Pavlou, 2003). It is therefore a risk related to failure to meet the performance objectives (Ratnasingham, 1999). The performance of Smart Government is its ability to deliver in terms of operational efficiency, flexibility and responsiveness. With high environmental uncertainty (characterized by adverse government regulations, stakeholder incompetence or market volatility), however, managers will perceive the performance risk as high, which could otherwise be monitored by output controls (Langfield-Smith, 2008).

2.9 Risk Management of Cybersecurity

Potential threats to successful Smart Government implementation are called risk factors (Bradley & Pratt, 2011). Risk management is the systematic process by which the risk is identified, analysed, measured and mitigated to protect the organization. Risk management in Smart Government is essential to weigh potential opportunities with potential inherent risks and adopt strategies to minimize losses. The primary purpose of risk management is risk prevention by taking a proactive instead of reactive approach to risk. Five potential risk areas have been identified below which need to be managed to overcome the risk that could occur the services of Smart Government.

Implementation of Smart Government faces several potential risk factors threatening successful implementation, such as IT infrastructure risk, change management risk economic risk, financial risk and performance risk (Kim et al., 2007).

Jeff Drew (2012) wrote an article about both threats and opportunity of virtual mobility systems, he argued that these systems have a profound impact on cyber-attacks and the non-stop development of computer and mobile systems. The problem he stated, is the danger that hides behind the desire of some employees to use their personal mobiles and PCs for work purposes; they download secret files or documentation of clients on their personal devices and if that device is stolen, lost or even hacked, all personal information of the client will be in danger of exposure. Drew suggested a risk management agreement between the company and its employees including high executive managers; to enhance cybersecurity levels by stopping that act. In fact, in most companies, employees are asked to connect their personal devices to the work IT system which can expand the risk crucially; breaches, cyber-attacks and viruses will threaten the company's system. Despite the convenience of brining your own device to work, one should always prioritise risk (p. 44).

According to Battersby (2015), more than 72% of cyber-attacks take place in small to medium sized businesses; he wrote a sensational article in 2015 about risk management in cybersecurity. He argued, every employee should manage the risk, meaning if one starts with himself diminishing the amount of cybersecurity danger becomes more likely. The writer noted the 'password' as the number one step towards a good risk management plan for cybersecurity, followed with implementing a "data security plan", which consists of a notification for all the affected parties that is released automatically when the attack occurs.

Collier, Linkov and Lambert (2013) conducted a research to define the four domains that control the cybersecurity process. They established a risk-based plan which contains four domains: physical, information, cognitive and social domains. The study explained why cybersecurity is in need of more than a risk management plan or strategy. In addition to IT development and

information infrastructure security systems, ethics (social domain) and decision-making (cognitive domain) are two challenges for the employee when faced by the dilemma of cyber-attacks. The study emphasises critical infrastructure as a target; where hijackers always constantly develop new ways to breach systems in all kinds of organizations, such as military and industrial entities (p. 469).

In a study conducted by Holisy Ougut (2011) and his group highlighting the topic of cybersecurity risk management, they developed a model for that purpose to benefit from the correlation between the risk management cost and the vulnerability of information infrastructure systems to risk. This was done to encourage organizations to decrease the budget assigned to risk management plans, and never ignore the fact that cyber-attacks will happen anyway and such risk plans can never prevent such attacks completely. The study shows a strong correlation between systems and decision-making for the organization to feel the urge to buy cyber insurance for its firms. Determining which kind of cyber assurance is suitable for an organization is relatively hard, whereas estimating probabilities associated with certain kinds of security breaches could lead to the right decision in choosing the appropriate cyber assurance premiums.

Simon Marvell (2015) suggested the measurement of "cybersecurity status" to determine the kind of risk management strategy that should be used, he argued that any cyber-attack can take place only with the absence of some risk management components, such as staff, technology or processes. The study put a table of changes that might influence the "cybersecurity status"; the table consists of skills that will switch or push cybersecurity status into a different direction. He added that there is an urgent need for the market to have a real-time cybersecurity risk management otherwise it could be subject to cyber-attacks in no time.

An article titled with “AGILIANCE Transforms Cyber security Risk Management” conducted in 2014 shows that the breaches reached a maximum limit in 2014. The study talked about the “RiskVision” product and that the number of institutions buying this product is increasing each year, to achieve cyber assurance, no matter at which cost. “The Agiliance” is a big establishment of data security risk products. Their models, programs and products could be the solution for all large-scale and small-scale organizations. The market needs more firms concerning cybersecurity risk management products; while millions of US dollars are in danger of being lost and actual theft exists in all kinds of political, financial, military and computer institutions, with no exception (p. 8).

The literature on cybersecurity risk management and cyber insurance plans, products and developments is rather limited. As the study of Ougut (2011) stated, this shows the lack of cybersecurity risk management literature, which needs to be addressed and studied in-depth to create stronger data security systems with more resilience to breaches.

2.2.3. Cyber Security Frameworks

Victoria Pellittari (2014) discussed the NIST cybersecurity framework, she pointed out that this framework can apply to different kinds of organizations and corporations, each organization has its own risk challenges and its unique critical infrastructure. The NIST plan will include workshops to develop the framework by obtaining feedback from its current users. The NIST framework is explained in the theoretical framework. The study emphasises two notions of IT and industrial control systems (ICS) where the needs of both could differ by organization type and by time (p. 20).

Michael Chertoff (2014), talked about “managing risk in today’s security landscape”. Chertoff suggested a framework key which is to recognize multiple layers of protection from potential threats. This means that in order to exit the target zone one needs to create a number of solutions, through a continual assessment of risk and measurement of vulnerabilities, to be able to deal with them. The researcher explores the vulnerability of humans rather than the weakness in systems; given the fact that only “human beings” commit cyber-attacks and human beings also have to address these attacks. He divided the dynamic risks into two main parts of one framework: 1) risk management section that consists of recognizing vulnerabilities, anticipating threats and understanding consequences; 2) planning and prevention, where operating and executing phase can began depending on risk management factors to prevent cyber-attacks from occurring (p. 38).

Again, Hoffman (2014) wrote an article criticizing the NIST framework, wherein he argued that the framework lacks details and needs to be investigated in order for governmental organizations to benefit from it. He added, the framework forms a brilliant start but ends up disappointing its customers. As the issue of cybersecurity expanded in the USA, he argued the need for a stronger, up-to-date framework is a must. The good news in this relatively new cybersecurity is that it is a risk-based solution which could achieve maximum security for the USA’s security system as well as the UAE’s with some developments in its structure, from this research point of view (p. 24).

Eva and Barry (2006) conducted a study about evaluating risk through a macro-economic framework to protect intellectual properties. The study focuses on the effects of cyber-attacks that last long. The framework for IP theft is cyber-based, it concerns the long-lasting consequences of such attacks, which matters most from an economic perspective. The International Consequence Analysis Framework (ICAF) sub-models and variables is explained in detail in their study; it is

used to estimate the loss of intellectual properties due to foreign theft. The study measures the piracy level and loss in all kinds of intellectual properties, such as books, pictures, records, music and so on. The study deploys the equity model and country-specific input-output models to estimate the level of IP piracy in different countries (p. 914).

A study conducted by Newman (2007) asked a fundamental question about potential cybersecurity attacks: “Are you prepared?”. He talked about cybersecurity skills and frameworks that should be used nowadays to be prepared for such crimes. He argued that educating students in the school period will result in extensive experience of IT and will give them enough time to develop a sophisticated and high level of skills in IT. On the other hand, giving them the chance to explore the world of IT to decide whether they would like to specialize in it or not could be detrimental to cybersecurity; given the fact that this career needs certain kinds of values and ethics where most high skilled students already have a criminal record because they know their ways around IT systems. The only way to be prepared is to make sure that your information infrastructure and your IT staff are ready, which can only be pursued through a scientific cybersecurity framework and special cybersecurity skills (p. 24).

Greenaway et al. (2015) conducted a study in the USA about a conceptual framework that could be implemented for cybersecurity. It also negotiates the privacy ethics and the control agency theory, the study highlighted the literature gap in privacy and cybersecurity for that matter; where the relationship between the citizen and the organization should be defined and organizational responses are rather limited. These issues could lead to non-trust relationships between the two parties due to the endless problems that could be caused to the citizen because of cyber-attacks or the new notion of privacy in the new era of the internet. They added, the agency should have control over the potential risk, or else it will face trust issues from its stakeholders and clients (p. 595).

The literature review of cybersecurity frameworks shows a shortage in the number of models addressing cybersecurity; there are only two or three frameworks and articles due to lack in research on the relatively new topic. The following framework by Hyslop (2016) will be adopted by this research to manage cybersecurity risks.

As is known, cybersecurity is difficult to achieve. Nowadays, resources are not enough to protect all at the same level. Despite all the most innovative IT instruments and applications, there is always a chance of being breached. The risk management approach is one of the most useful strategies in this kind of environment. Many organizations have already conducted solutions for the protection of privacy and civil liberties. The following theoretical framework is intended to supplement these processes and provide guidance for ease of risk management privacy in compliance with the organization's approach to risk management in cybersecurity. The integration of privacy and cybersecurity could benefit organizations by improving customer trust, which allows a more standardized exchange of information and simplified operations for legal regimes.

According to Business Dictionary, "the risk management identified as analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks" (BD, 2012)[i]. To be able to manage risk, organizations need to understand that when events occur, they will be affected somehow. Some organizations define this process as risk tolerance; by accepting risk and continuing to provide services without being interrupted.

"Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on." (Amoroso, 2006)[ii]. Organizations should prioritize risks and activities by understanding risk tolerance in terms of cybersecurity, which can also help organizations to establish a full idea and to make the right

decisions about the financial and managerial costs of cybersecurity. When applying and executing programs of risk management the organizations are provided with a chance to estimate quantitatively and offer their programs of adjustment in the cybersecurity arena.

Nevertheless, cyber-crimes and online hacking are becoming a huge business, which results in the electronic suffering of companies from cybersecurity breaches.

A recent study by the U.S. Secret Service and Verizon Communications, Inc., showed that more than 72% of data breaches take place in small- or medium-sized businesses. (Cybersecurity Risk Management 101, 2015)[iii].

A recent example of cyber-attack is the hacked emails of the USA presidential campaign's chairman, during the election period in the USA. This resonance case had an enormous impact on the mentioned election campaign, consequently the competent party has won the election and the United States presidential period of four-years.

To set up the approach for managing cybersecurity risk, the research of Hyslop (2016). (Chief Information Security Officer (CISO) for the City of San Diego) will be used in the current framework. The framework provides a common language for understanding, managing and expressing the life-cycle concept of cybersecurity risk, both inside and outside. It can be used to manage cybersecurity risk throughout the organization, or it can be focused on delivering critical services within the organization. Different types of organizations - including coordination structures sector, associations and organizations - can use a framework for a variety of purposes, including the creation of common profiles. At the same time Hyslop (2016) used the very common National Institute of Standards and Technology (NIST) Risk Management Framework. As he mentioned: "to demonstrate a mature risk management methodology that would enhance an

organization's cyber-security program if implemented properly" (Cyber-Security & Risk Management: an evolving ecosystem, 2016)[iv].

According to CISO there are six steps to implement a risk management process into strategic operations:

- Categorize information systems and data
- Select security controls
- Implement security controls
- Continually assess security controls
- Authorize (verify risk baseline)
- Continually monitor security controls

Therefore, following this process, each step will be reviewed as follows:

- Categorize (Information Systems & Data)

For this essential step NITS has its own tips and techniques for systems guideline. Every information system has its threats, but not all threats are the same or equal. Furthermore, every threat has an impact to an organization's IT assets. Therefore, this describes best how to categorize them and how to prioritize data protection.

NITS recommend the following steps for categorization:

- preparing for security categorizations
- identifying and matching data elements to information types
- defining and documenting information type categorizations

- defining and documenting information system categorization
- defining and documenting system overall impact level
- approval for system security category and overall impact level
- maintaining the system security category and impact level

Meanwhile the author recommends using a more specific and simple method.

- Document organizations data flows
- Generated by applications and hardware
- Network maps
- Application/Hardware portfolio's
- Understand how organizations data is used
- Understand how assets process data
- Understand where data is stored
- Know what data is transmitted out of organization and to whom

However, the official Tips and Techniques for systems guideline from NIST even more detailed action plan with exact drafts and examples.

- Select (Security Controls)

"Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information" (Recommended Security Controls for Federal Information Systems and Organizations, 2009)[v].

Security controls are established by categorization as in the previous step. Therefore, the accuracy and attentive collection of information in the first place is an important process to start step #2. Choosing an appropriate set of safety measures to adequately reduce the risks by satisfying certain and sometimes specific requirements for the safety of an organization is an important task as well. This task demonstrates the organization's adherence to safety and the due diligence exercised to its privacy policy, integrity and availability of organizational information and information systems.

- Implement (Security Controls)

For the recognized regular controls acquired by the data framework, information system security engineers with the support from information system security officers arrange with the normal control supplier to decide the most suitable approach to apply the basic controls to the hierarchical data frameworks. In fact, this does not keep them from utilizing open source devices; to utilize open source arrangements there are a couple of focuses to check:

• The chosen arrangement has a group that supports the tool and the FAQs/Support pages are current.

• Staff have the skillsets to legitimately execute and maintain it (no applications/arrangements permitted).

Since the endeavour plan and information security configuration developed by the affiliation in a general sense affect the approach used to complete security controls, giving documentation of this strategy ensures traceability concerning meeting the affiliation's information security necessities.

In shutting this progression, report controls and new settings. It is not recommended to just record settings, rather in addition it is better incorporate new scan/test results about documentation

so an organization's staff have illustrations of any new yields. It is better to keep it in mind and record now in order to not regret it later.

- Continually Assess (Security Controls)

"The security assessment plan provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures" (Recommended Security Controls for Federal Information Systems and Organizations, 2009).

In evaluation, it is required to survey the most recent review discoveries, new specialized prerequisites and every single reported metric for an organization's cybersecurity suite. Organizations consider both the specialized ability and level of autonomy required in selecting security control assessors. Organizations likewise guarantee that security control assessors have the required aptitudes and specialized ability to effectively complete evaluations of particular framework, hybrid, and usual controls. This incorporates learning of and involvement with the particular equipment, programming, and firmware segments utilized by the organization.

Compliance frameworks (PCI, HIPAA, GLBA, SOX and so on) are fundamentally the same as the security systems (NIST, COBIT or ISO), however, consistence systems have generous penalties and fines connected with them if an organization comes up short in a review by not meeting their required security controls. It is better to have some sort of information archive/entrance to track your consistence documentation and as a feature of this progression, occasionally survey any controls that have remarkable discoveries, deal with the remediation of these discoveries and track them to determination. Keeping in mind this progression is about constantly evaluating an organization's security program, risk management program and making inquiries.

- Authorize (Risk Baseline)

Set up the arrangement of activity and breakthroughs in view of the discoveries and proposals of the security evaluation report barring any remediation actions taken.

In this step, Gary Hyslop mentioned one very important issue, he found during this process that its extremely difficult to produce accurate monetary values for an organization's risk exposure. He also suggests the use of CyVar and FireDrill to test and approve the suspiciousness about security posture.

- Continually Monitor (Security Controls)

Find the security effect of proposed or genuine changes to the data framework and its environment of operation. Essentially, the current step identifies if the controls for reducing risk are effective or not.

Risk Monitoring consists of five techniques:

• Risk Response Audits: Examine the effectiveness of an organization's response to remediating risk. Typically examines the organizations responses to avoiding, transferring or mitigating specific risk exposures.

• Risk Process Reviews: This is where your organization will examine risk throughout the lifecycle of a system, workflow or process. If the identified risks change the selected risk management team will make recommendations for remediation.

• Risk Value Analysis: Assessing risk impact through:

 Qualitative Analysis – assess impact and likelihood of identified risk. Prioritize the risk, based on impact to business operations. Evaluate the probability and consequences, measuring the results with high, moderate or low ratings.

 Quantitative Analysis – numerically analyse the probability of each identified risk and its consequences on business operations. Will use tools such as interviewing, sensitivity analysis, decision tree analysis or simulations to provide data on the potential impact to an organization.

• Risk Performance Measurement: Here accomplishments are compared during operations to track for trends and reduce risk exposure to the organization.

• Risk Response Planning: Employ monitoring techniques to detect and respond to risk enhanced events.

Develop options for an organization with actions assigned to specific teams/individuals to provide a response to a specific risk event.

2.3. The Measurement of Resilience

The Resilience Studies

In this section the studies on the measurement of resilience will be presented systematically to fulfil the research aim and objectives.

2.3.1. Resilience Notion

Resilience can be defined as the characteristics of the organizational system to tolerate stress and overcome external or internal threats or attacks; it pertains to the system as a whole rather than its individual parts (Adger, 2000). To assess the resilience of an organizational system, the capacities and interaction of different parts of an organization after a disruptive event are studied to identify how they interact and communicate among themselves. Resilient organizations encourage consultative and participative decision-making whereby rules are not simply dictated but employees are encouraged to behave in a manner that is aligned with customer expectations. Thus, a resilient organization strives to articulate, recognize and exhibit its values (Kerr, 2016).

Resilience is also defined as the ability of an organization to predict and recover from the change by evolving and surviving any unforeseen events (Longstaff, 2005). It is considered to be more than just risk management and does not entail a crisis-proof organization or supply chain. Rather it is a broad phenomenon that entails every change that organization faces and not just a crisis. It includes managing unanticipated disruptions from suppliers as well as any shift in customer buying habits as well. A resilient organization both anticipates and adapts itself to be able to serve its customers with products and services that they prefer while taking care of supply shocks at the same time. It is a valuable characteristic because change is a continuous global phenomenon.

Researches show that the average company age on the S&P 500 was 61 years in 1958 while it was just 18 years in 2012. That indicates how rapid the change is and the inability of companies to survive this economic dynamism. Resilience of a business organization is its ability to detect and grab opportunities before competitors have done so while taking risks (Newnham & Crask, 2015). Resilience of an organization depends on resilience of its various component parts. It is a multidimensional concept which covers the business aspects of the organization.

The two researchers (Chesley & Amitrano, 2015) defined resilience as a capability of an organization to anticipate and face changes not only to overcome them, but to evolve by their existence. Whereas, Olson and Anderson (2016) defined resilience in the business context as overcoming the challenges depending heavily on the planners that are distributed smartly across the organization to create executive strategies besides a great deal of involvement from the leadership (p. 33).

2.3.2. Resilience Business Projects

In the late 1990's researchers talked a lot about developing the leadership notion in business firms and large-scale programs, whilst in recent years risk management has become increasingly important for the survival of organizations in the fast-growing business arena and the emergence of hundreds of competitors. After getting to know how to survive, the recovery and the ability to prosper after any disruptive event through a standard set of documented plans become critical. These kinds of plans are called "resiliency plans" which enable an organization to mitigate the potential risk by giving them the choice to exercise this kind of plan in a systematic way to increase the readiness to the all business disruptions.

Chesley and Amitrano (2015) conducted a study on the emerging capability needed by business initiatives; they argued that not every organization is ready for the change that is happening around it, unless it has a good emerging resiliency plan to be able to not only survive but to evolve while facing new changes or interruptive events. The researchers talked about six traits that every organization need to apply to be able not only to overcome the change but to be resilient to it by knowing what happened and what is happening and what is yet to come, in order to be well-prepared using scientific standards and specific steps of the resilience plan (p. 2).

Usually, the plans and programs in most organizations have basic "text book" standards elements but few are innovative and go in detail, which creates a big gap between what is happening in reality and what is stated in these plans. The usual plans that are being used in any organization are lacking scientific ways to assess its quality for being a continuity plan or just a "text book" plan that is disconnected from the actual business of such an organization. The main criteria here is to be able to choose the most distinguished information in a business continuity plan, then document it, benefit from it, employ it in a correct way, develop it and share it with the members of the organization.

Olson & Anderson (2016) conducted a study on business continuity's resiliency scoring. The researchers explored the methodology of scoring specifically as a resilience score, which helps businesses plan to continue to evaluate processes; this will help any organization to customize their system and make it more adaptable to their needs. The study argued that a resilience team is different to a risk management team, because of the scoring; wherein the resiliency scoring depends on assessing how the resilient team would execute or perform their critical plans if they face any risk or any undesired event during the plan implementation phase of their business continuity. They argued that the scoring in this case is dependent on the document analysis of the plan content, along

with the exercises that took place to prove that the plan continuity will still be effective even when faced with interruptive events. Furthermore, the difference between risk management and resilience is that the first will prevent or mitigate the risk but the second will continue to function and evolve even after an interruptive event has occurred to make sure that the plan is continuously ongoing to achieve the main goals of an organization.

2.3.2.1. Operational Resilience

Operational resilience indicates that the organization is not complacent with the present state of affairs, rather it is continuously changing and improving its business operations as well as supply chain. It is aware of its operations and business environment. It identifies operational improvements in terms of businesses processes, as well as the products and services of the organization and also people and governance mechanism (Kerr, 2016).

2.3.2.2. Supply Chain Resilience

With increased complexity of supply chains due to the globalization of organizations, it is of paramount importance for an organization to have the ability to assess and manage supply chain risks throughout the process of procurement, manufacturing, shipping and sales lifecycle. Any supply chain disruption can cause reputational risks along with operational financial risks. Supply chain resilience is an important factor in the modern business environment because supply chains are considered the backbone of the modern economy. Any disruptions in supply chain, and the ability of businesses to withstand such disruptions, determines the supply chain resilience of the system. However, resilience means availability of alternatives to withstand disruptions thereby leading to redundancies and slack hence it has a cost associated with it. Thus, the challenge for supply chain resilience is to maintain resilience along with efficiency (Editorial, 2015).

2.3.2.3. Information Resilience

Organizations deal with sensitive information and this information can be critical to business success as well. It is therefore necessary that this information be safeguarded. It is essential for a resilient organization that it manages its information security and protects its intellectual property rights. This requires that an organization adopts practices that allow stakeholders to collect, process, store and use the information in a secure manner (Kerr, 2016).

2.3.2.4. Network Resilience

Networks are linked to each other via communication nodes and network resilience determines the extent to which a malfunctioning communications system affects the overall network structure and disrupts the inter- and intra-organizational communication flow and how adaptively the network responds to it. In most cases the removal of network communication links or nodes can result in information communication taking alternate nodes or routes for information communication. However, certain network structures are more sensitive than others to node link removal while the network breaks into sub-groups that are not connected with each other (Barab´asi, 2003). The most resilient network structures are the “scale free” networks because they are not sensitive to random node removal. However, even these networks can be disrupted when critical nodes are removed simultaneously (Kahn, Barton & Fellows, 2013). Network hierarchy, network diameter and network clustering are some of the determinants of the resilience of a network (editorial, 2015).

2.3.2.5. Developing Organizational Resilience

While traditional strategies for crisis management might be helpful, it is possible to enhance administrative and social capabilities to cope with crisis management situations by developing

resilience. Research on natural disasters has suggested that immediate response to these catastrophes depends on resilience of citizens, operational commanders and first line responders such as fire fighters or emergency medical professionals while strategic leaders can make a difference in the long-run only (Drabek, 1986). Thus, efforts should be directed towards development of resilience which is perceived as an emerging quality for a professional system (Longstaff, 2005). It is suggested that better institutional quality, experience and resources can increase the pace of recovery from a crisis, yet resilience still remains an incremental quality of the system which can be gradually acquired and can only be improved by trial and error of its response in the face of future disasters and system failures. Building resilience has two preconditions: first is the awareness that a system failure, disruption or catastrophe can strike while the second condition is that building resilience does not replace basic elements of emergency response operations.

The first step in developing resilience is preparing the first responders who are well trained to take independent decisions and operate effectively in critical system failure situations. They should be aware and convinced with core organizational values, ethics and clearly defined priorities for responding to the crisis in the best interest of the organization. The next step is business continuity planning, which includes setting up a backup operations centre in an offsite location that mirrors the present business operations in offsite IT backup, for example in case of a natural disaster. This can be used to continue business operations from the remote site. The third step is joint planning involving all stakeholders whereby all possible threats are identified and possible solutions are considered on a regular basis to cope with the continuously evolving nature of change.

The fourth step is joint training of all stakeholders by exposing the contingency plan to simulations and testing its ability to respond to threats. The final step is preparing leadership to facilitate resilience in the face of crisis. Leadership should avoid the traditional leadership pathologies in a crisis situation, such as blaming others, waiting for facts and figures before decision-making, waiting for external help, sticking to the original plan or spreading rumours without verification. They need a realistic approach towards what can be done and they should take necessary steps that can be helpful to make a difference (Boin & McConnell, 2007).

According to Chesley and Amitrano (2015), change is the key of every organizational resilience plan. They raised the question of how does an organization responds to the change in its business plan? They argued that strategy is important for any organization type but after it has been initiated it becomes vulnerable to change; when faced with interruptive events the strategy cannot be completed on time. Moreover, they talked about adaptability and how it is relevant to culture, which affects the strategy as well. They found that organizational resilience outdoes the leadership which does not prove to be a great factor in the success of a business over the years. They added that "enterprise resilience" is the most important factor of success in any business; furthermore, they note that resilience is becoming more measurable and manageable (p. 3).

In terms of organizational resilience, planners are the key. Olson and Anderson (2016) argued that planners are the key in every business or program continuity plan; the more they are engaged the more the plan is ready to be implemented at any time under any interruptive circumstances. Furthermore, resiliency scoring helps in motivating the planners towards the target; by being more involved and engaged in all of the activities of their continuity programs. Moreover, this can be achieved with the support of the senior board. Additionally, this level of high

engagement and involvement will enhance the commitment level among planners, which will help them to strive to achieve the best in their performance and will improve their confidence while managing their plans standing on firmer ground than before the resilience notion was adopted. The two researchers added that the feedback of planners is a significant tool of this methodology in the organizational resilience arena, which highlights the role of the resiliency scoring in adding more value to them (p. 43).

Chesley and Amitrano (2015) argued that enterprise resilience is measurable and manageable unlike the traditional risk management frameworks that have typically been applied over the last few decades. They added that if we desire to make any firm resilient we have to know the key elements of the enterprise resilience in the organizational context. Chesley and Amitrano (2015), suggested traits that are more likely to be developed to suit any business initiative to be able to not only survive in the face of the change but also to benefit from it and set a great example in the market. That can be done by benefiting more from the young and their new ways of thinking which will create more resilience in such firms (p. 9).

2.3.2.6. Critics of the Measurement of Resilience

By reviewing critics of organizational resiliency in the literature, it has been found that resilience studies are focused on increasing the level of engagement of planners, especially in the continuity plans of programs or projects. The focus was more on a program's life-cycle, which must consist of an assessment phase, then planning phase followed by an exercising phase to reach the maturity level and aid in the fast recovery to ensure the continuation of such a program (Kott & Linkov, 2016).

To help make the recovery process reach the maturity level, planners should be more engaged, plus making sure to identify and assess the risk besides documenting the resilience plans while exercising it over and over again to guarantee the resiliency level for the potential obstacles or even disasters (Keys, Chhajer, Liu & Honer, 2016).

Resiliency scoring helps in evaluating the content of such continuity plans, it aims at directing the planning process to the maturity phase. This kind of scoring will support engagement and visibility besides enhancing compliance through the continuity programs of an organization.

However, Chesley and Amitrano (2015) argued that engaging planners and leaders is not an easy task; it is challenging as long as the culture of the firm is not ready for this kind of scope or change. As has been stated in most of the studies, strategy is affected by culture, whereas in some cases the leaders isolate themselves from the employees and find it difficult to be more engaged or even connect with the planners. After all, good leaders should work for the best interest of their business not according to their culture or personal needs.

Furthermore, Olson and Anderson (2016) argued that the resilience scoring has a huge impact on the "Target" company, wherein a successful organization tends to measure its notion of achievement by hiring the right advanced resilience team and adopting the right organizational resilience plan for its business continuity. Moreover, the resiliency scoring will raise the level of the engagement from the executive board of any organization, and will create a direct contact between them and the planners; planners that are more equipped and more aware of how to handle an interruptive event and have a specific resiliency plan with details (p. 40).

On the other hand, Chesley and Amitrano (2015) explored how the enterprise resilience notion, which the two researchers claim consists of six traits divided in two categories. The first

set consists of: Adaptive Capacity, Coherence and Agility; while the second consists of: Trust, Relevance and Reliability. They argued that if the firm follows this framework it will be able to face both opportunities and threats at the same level of benefit and will be able to prosper in responding to risks and opportunities which transpires in the strategy implementation process (p. 6).

Moreover, to make sure that the organization maintains its resilience status, it must make sure that the planners and leaders are distributed across the organization's planning process and documents best practices, while also having simple predefined standards of resiliency criteria for business continuity. Although continuity plans tend to cross the normal job tasks and go above and beyond standard requirements, planners and leaders have some difficulties finding the time to prioritize between their standard job tasks and preparing for the unforeseen disruptions that 'might' take in place in the future (Kerr, 2016).

It is noteworthy that the persons whom we called planners in this research are not professionals in business continuity programs; rather, they are experts in their own field, which is part of the continuity program (Pennauther, 2010). These important planners will help in documenting important activities and distinguish information in their field to aid in the continuity program and its owners, however, this goes above and beyond their priority job tasks and duties, the challenges of which have been explained earlier.

2.3.2.7. IBM Business Resilience Model

IBM has provided and originated a business resilience framework which is meant to identify the level of organizational resilience. It comprises a set of objects termed as layers which

underline the resilience capacity of any business. A detailed discussion of various layers of this model is listed below.

The first object is *strategy* which includes the financial, operational, manufacturing, disaster recovery strategy and so on, which govern the day-to-day business of the firms. The second layer includes the objects related to *organizational structure*, such as communication, skill level and responsibilities of employees, which is underscored by human resource and communication processes. The next layer constitutes *applications and software* used to operate business and the databases, such as Customer Relationship Management and ERP applications used for transaction processing in business operations. *Processes* are the next object layer, which include critical business processes and IT systems, for example accounts receivable and payable and problem management. *Technology* and *Facilities* include networks, systems and technologies that are used for data processing and running business applications while facilities are the factories, buildings and warehouses used to house the organization and its technologies. These layers conceptualize the components of the business resilience of an organization and help an organization to identify the key areas which should be focused on for building a resilient model. However, this model also classifies attributes of the business according to traits that determine its ability to respond quickly to any disruption.

The IBM Business Resilience framework proposes the following five attribute classes that are part and parcel of a resilient business organization. The first key attribute is “control and comply”, which describes the ability to identify, anticipate, evaluate and control the risk associated with compliance of social, economic, technical, environmental and regulatory factors. The second attribute is the ability to “predict and detect” any events that pose potential security or privacy

threat to business operations. The ability to estimate and measure such events can save the business from jeopardy of operations. The third attribute is “deflect and solidify”, which as the name implies indicates the ability to deflect the risk and ensure business continuity. “Adapt and optimize” is the fourth attribute of an organization which reflects its ability to ensure flexible, adaptable and integrated risk mitigation strategies. The fifth attribute is “protect and preserve” and indicates the ability of an organization to protect itself against damage whether accidental or intentional damage and preserve its data and resources (Cocchiara, 2005). By focusing on the core objects of resilience, organizations can build a resilient structure by adopting and acquiring the right attributes needed for resilience.

2.3.2.8. Barriers to Enhancing Resilience

Developing organizational resilience has some barriers which are primarily rooted in the degree of organizational readiness (Pauchant & Mitroff, 1992) of governance and society. There are various societal constraints to a resilient approach towards disasters and disruptions. People usually respond to threat potentials in a dysfunctional manner, including denial or downgrading the importance of a threat or its probability and it is just a mental barrier which poses resistance to resilience development. The third most important barrier is organizational beliefs and values which get in the way of resilience development because an organization focuses more on customer service, profit margins and so on, rather than on critical events and potential threats to systems. When such events are observed elsewhere, organizations rationalize the occurrence of the event and justify the improbability of the event taking place to itself. The fourth barrier to resilience is institutional design. Most organizations are designed in a manner that is not resilient to critical

system failures and breakdowns. Any emergency response requires flexible decision-making while typically organizations have authority converging upward (Boin & McConnell, 2007).

Developing resilience incurs costs concerning time and resources for an unforeseen event that may or may not take place. It also costs to train people and take them through simulations to prepare them for the unforeseen events. It also requires cooperating with various stakeholders and adjusting to their own agendas, values and cultures. All these costs pose a major barrier to the development of organizational resilience. The sixth barrier to resilience is the governance framework that typically emphasizes a centralized control and command structure and it is incompatible with the concept of resilience, which emphasizes self-reliance and preparedness for coping. The seventh barrier to resilience is most relevant to the resilience of e-governance systems, which is the socio-economic framework. Since modern cities house communities that are in disarray themselves, the poor, homeless and immigrants are the least resilient communities. It is thus increasingly difficult to develop and implement a resilient e-governance mechanism for such socio-economic classes (Chesley & Amitrano, 2015).

2.3.2.9. Resilience & System Maturity Frameworks

Applying resilience scoring has a tremendous effect on evaluation of continuity business plans, it is able to achieve that by analysing the business alignment against a pre-set criterion of definitions which can be adaptable and customized to suit all kinds of programs. This “patent pending” tool has proven to be a success in many cases; it has an impact on three main elements: enhancing the reporting process, identifying risk and helping in the measurement of the organizational resilience (Kott & Linkov, 2016).

Olson and Anderson (2016) note that resiliency scoring is measured by comparing predefined standards and outlines against the business continuity plan using the scoring guide to be able to assign the most appropriate approach based on its similarity with theses sets of outlines. Furthermore, some factors will have an impact on the score, such as 1) whether all the requirements are met in the stage of completing the compliance plan; 2) whether the recovery actions are detailed and doable; 3) whether the risk has been accepted within their plan; 4) whether the plan is being exercised throughout the planning process; and 5) whether they are performing additional activities of the resiliency scoring (p. 35).

Chesley and Amitrano (2015) have outlined a framework concerning measuring organizational resilience. The framework consists of six strong traits to make any type of organization more resilient to risk and other kinds of sudden change or interruptive events such as a technological breakthrough. The two researchers talked about how all kinds of organizations face both opportunities and threats at the same time, so they raised an important question here: do we have to predict which kind of interruptive event we will face, good or bad? The answer is "NO". The right question here is whether we are as a company or organization 'resilient' enough to face or predict these unforeseen threats and opportunities and 'resilient' enough to know how to react to them. They argued that if we intend to make the organization resilient enough, we should understand the main elements that make the practices more likely to compromise the resilience process.

This framework helps any organization to build resilience by demonstrating their six distinguishing 'traits' that reflect how an organization is able to predict and react to risk or any interruptive event. In terms of internal capabilities Chesley and Amitrano (2015) have presented

three main traits to help the organization measure its ability to respond or react to change. These first three traits are:

1- Coherence: which is all about the ability to make good beneficiary decisions that have mutual benefits.
2- Adaptive Capacity: which means the ability to adapt and reorganize when interruptive events or changes occur.
3- Agility: or the ability to make fast decisions or to implement them at a required time.

These first three traits are considered basic according to the two researchers when responding to risks that work against the decision-makers own good. These traits work to serve their ability to benefit more from risks or make the most of all kinds of change.

Chesley and Amitrano (2015) talked about a notion called start-ups. This notion consists of the three traits as follows: 1) How to respond to the feedback, meaning adaptive; 2) When to move fast right after sensing the correct signal, meaning agile; and 3) Then trying to keep their focus, meaning coherence. They argued that large organizations, such as the Smart Government in this case study, learn from 'lean' start-up processes, especially when they talk about developing their products, and in the Smart Government (developing their services). The notion of lean start-up could apply to Smart Government services in terms of launching new e-services to see if people will embrace it generally and particularly in the meantime, to see if any big opportunity arises. There is also another notion suggested in the same arena which is called Fast-Works based on the same start-up elements and principles.

This culture of resilience should be implemented across the organization not just when developing a product; but rather on the market level, organizations should be creative in how to

serve the youth that are talented and to anticipate both opportunities and risks, besides building a powerful network.

In the framework of Chesley and Amitrano (2015), which consists of six traits, the last three sets are concerning the outside relationships of the organization and its public or external stakeholders. The last three traits are as follows:

1- Relevance: this trait is about always serving or meeting the stakeholders' requirements.
2- Reliability: this trait concerns the ability to serve at the expected time and quality in terms of products or services.
3- Trust: this trait consists of the creative mentality to have a business or an investment-worthy relationship with the customers and different kinds of stakeholders.

These three traits are important to an organization's relationship with its stakeholders, customers, as well as its business partners. This conceptual framework summarizes the three traits as follows: 1) Relevance is the ability to meet stakeholders' needs; 2) Reliability is the ability to meet the required quality and time; and 3) Trust, which lies within a business relationship or in other words an investment-worthy relationship.

The three second set of traits might sound easy to achieve but in fact they are quite hard to maintain. The study of Chesley and his partner shows that most CEOs in our current century are convinced that the trust element is the most important element in the relationship between organizations and their stakeholders or business partners. The perception of trust as a threat to the growth of any business can create a bottleneck that prevents it from prospering and carrying on with such business relationship. The two researchers claim that a positive relationship between an

organization and its customers, stakeholders, partners and business leaders is an essential base to achieve business growth, which redirects back to the strategy and the best way to develop a strategy that meets organizational goals.

Moreover, the relevance trait is basic at the current time with more CEOs convinced that our current world is filled with industry disruptions. Whereas disruptions make the best opportunity for non-traditional organizations and the same disruptions could create risk for incumbent organizations. Nevertheless, the challenge lies within not knowing when the risk turns into a disaster and becoming part of this big disruption is no longer a decision that can be made. In the resilient notion, organizations should respond to such disruption as an opportunity and should perceive major disruptions creatively to be able to benefit, learn and recover from them, and then of course to find a way to prosper after the disaster, to reach the highest maturity level.

Kerr (2016) conducted a study concerning organizational resilience. The researcher talked about a phenomenal framework to maintain organizational resilience and how both criteria of risk management and business improvement have to be equally focused on in this framework. Kerr's model (2016) emphasizes the qualities that form organizational resilience, such as:

1- Strategic adaptability: This concerns the ability of how an organization handles any kind of change along with change circumstances in a successful way. In some cases, even if that means that the organization must move from its core business.
2- Agile Leadership: having the ability to handle measured risk and learn how to react in a fast and appropriate way to both risks and opportunities.

3- Robust Governance: applying accountability within the structure of an organization, which consists of three elements: 1) transparency; 2) trust; and 3) innovation in order to be loyal to their values and most importantly committed to their vision (p. 42).

According to Ward (2015) there are several strategies for a supply chain to be able to manage and control risk, which also help in boosting resiliency by minimizing costs and enhancing agility. The faster the response to the supply chain the more money, production, business deals, sales and brand damage will be saved. Even in the most complex case of a supply chain, the organization should be able to handle the situation with a wider lens on its business system, especially the changes that will occur in the 'organization's network', and should be able to adapt quickly to such circumstantial changes.

Ward's (2015) strategies for the supply chain consist of the following:

1- Having a deep understanding and a full idea of the risk
2- Using the Centric Network notion
3- The foundation should consist of a strong business continuity plan
4- Consuming all the data available
5- Collaborate inside and outside an organization
6- Resilience must be strongly built
7- Culture must be rightly created (p. 26)

Moreover, Gordon and Larry (2005) conducted a study concerning a scientific framework for business resilience. The researchers focused on five maturity levels which help the system to identify its ability and potentiality for enhancement and improvement. The five elements are:

1- Basic: this level concerns the policies of the organization and its emergency procedures along with three more elements such as: governance and privacy programs of compliance. In some cases, this level could include continuity plans.
2- Managed: is concerned with policies compliance and processes that form the key automation tool to handle both risks and opportunities. At this level, the CEOs and the executive board play a significant role in ensuring the level of awareness among the employees regarding their responsibilities and to be more committed to the organization policies.
3- Predictive: is concerned with how the organization can take pre-emptive actions to mitigate the risk by using its warning system which should be advanced and able to monitor the current performance of this organization. In this case the organization is still in the stage of mitigating identified risks manually.
4- Adaptive: by using contingency strategies and on-demand business resources the organization is able to maintain its operations by sensing and responding to future disruptions. The response has to occur prior to the risk and the system must be programmed to adapt to any change in order to avoid losing any essential element of the business (p. 16).

In this thesis the researcher will measure the resilience of the Smart Government system by testing its maturity level to determine if it is in the very basic level of maturity or in the risk

management level or even beyond that. The system will be analysed to identify if it has reached the resilience level of maturity which is the most advanced stage of a professional system's maturity. This will be explained in detail in the next chapter of this thesis.

2.3.3. The Role of Management Control vs. Strategic Management

There are various theories and concepts about both strategic management and management control that researchers have developed over the years. The theory of strategic management involves leadership skills. As Dess et al. (2013) discussed, the theory of leadership plays an important role in strategic management and is the key factor in successful risk management and resilience in organizations. He added that it has been developed with three core elements of strategic resilience: problem formulation, future orientation, and an organization's legacy. The problem formulation requires a business to reflect on the challenges faced, rather than only looking at solutions to risks. On the other hand, the theory of management control and security control appears to have a great impact on resilience, because leadership does not prove to benefit organizations in times of crisis, whereas leaders or the top management need to have flexible thinking and engage middle ranked managers in times like these (Anthpoulos, 2015).

Möller, Schäffer and Verbeeten (2020) explored management control and the need for it, especially in digital organizations, in this case Smart Government. They emphasized the role of management control on the economic status of an organization. The controllers or the planners should address the long-term development of an organization's viability and its digital plan. Their strategy will benefit from digital instrumentations and technologies. Control management gives

direct management and encourages executive managers to be pioneers in their industries, meaning, if this applied to the UAE government, then the UAE Smart Government will lead by example among other countries that have established Smart Government systems.

According to Ross et al. (2017) management control differs from strategic management, especially in digital organizations, because it calculates the areas of improvement and progress. Furthermore, it has the ability to direct them exactly where needed. Planners and controllers play a significant role in exploring changes and identifying opportunities, and they can employ that experience in business models, organizational resiliency and key strategies.

The difference between strategic management and control management, is that the second has the ability to mix traditional business model components with new digital ones, whereas the first one will work only on a traditional business model for traditional types of organizations. Management control will control the investments and budgeting and save Smart Government from significant financial losses and eroded profitability, it can also control the budget of smart devices and products. Smart Government projects can cost a huge amount of money, when it comes to buying hardware and cybersecurity programs and installing cutting-edge equipment, which needs management control to counter it (Möller, Schäffer & Verbeeten, 2020).

The strategic management field of study deals with the primary emergent and intended steps taken by managers on behalf of executives that involve resource utilization to enhance the organizational performance in internal and external environments (Nag et al., 2007). Although strategic management has been found to be crucially important by many researchers, it has emerged previously and is considered old fashioned, unlike management control that has emerged recently

and found to be very effective when changes occur; this is because it can control such developments before they even take place by anticipating, preparing and providing continuous post-trauma control. As stated by Harrington and Ottenbacher (2011), the importance of strategic management in the hospitality sector has not been realized in the past. However, the recent fluctuations in the global economy have provoked the need to assess and provide strategic management approaches that can address future opportunities and challenges. When it comes to Smart Government originations and governmental departments in general, management control and organizational resilience are the new solution for many recent problems faced by these organizations. This is important as the traditional roles that once applied to smart systems and business models no longer work due to the fast-growing industry of hackers and cybercrimes (Anthpoulos, 2015).

Guth (1981) argued in his book that organizations with complex natures, in our case Smart Government, tend to experience unpredictable events and crisis in their business environment, which can take an organization a very long time to react to. Thus, the role of strategic management is clear when it comes to overcoming a crisis or a sudden event, which is called the ability to recover and absorb disruptive events by organizational resilience. One can see the strong correlation between the strategic management practices and the organizational resilience dimensions.

Schroeder (2014) talked about the close relationship between the resilience and risk management and the differences between management control and strategic management. In his study of "An art and science approach of strategic risk management", the researcher argued that the resilience and risk management approach needs sophisticated tools and frameworks to be established in an organization; this is due to the continuous change of business environments and

the unexplained growth of cybercrimes and technological developments every single day (Dess, et al., 2013). Furthermore, the author also emphasizes the relationship between strategic management and enhancing the different dimensions of organizational resilience. The team argued that top management should have management control and change management backgrounds to be able to ensure their organizations survive under the current circumstances of continuous change in the business world.

As stated by different research studies, management control is important for organizations as it lays the foundations for using opportunities effectively and building capabilities. Management control itself involves different styles that have different effects on different types of styles that affect different capabilities. The directions from top management can have long lasting impacts on the types of choices made by an organization. After analysing the relevant literature in human resource and organizational behaviour, the researchers highlighted the impact of different styles of leadership, such as transformational, transactional, and the servant-leader style of leadership. Essentially, it is clear that leadership styles can impact organizational behaviour significantly (Anthpoulos, 2015).

2.3.4. Smart Government Case

Smart Government intends to use technology to support and facilitate better decision-making and planning. It involves the improvement of democratic processes and transformation of the methods that are used to deliver public services. Smart Government includes the efficiency agenda, Smart Government, and mobile working (Scholl & AlAwadhi, 2016). The concept of smart cities emerged during late 1990s in literature. A number of approaches to the idea have been

developed. However, it is important to understand that a smart city does not mean a city with particular attributes, but it is about different cases in urban spaces, such as web portals that virtualize city guides, agglomerations with communication technology infrastructure, knowledge bases that fulfil local needs, information and communication technology infrastructure that is used for delivering services to people, and information and communication technology for ecological use (Anthpoulos, 2015).

The Smart Government related academic literature has produced a vast body of knowledge that suggests that smart governance means a future ready, progressive, transformation, innovation, sustainability oriented approach to governance, and improved quality of life by using modern information and communication technology. As stated by Hollands (2008) 'electronic government' was the term used in academic studies in the 1990s. Therefore, Smart Government has its predecessor name 'electronic government'. Some researchers, such as Leydesdorff and Deakin (2011) argue that the term Smart Government or smart city is the term generated as a marketing tool by vendors. They considered it as a programmatic vehicle for renovation and reconstruction of public administration.

Currently the idea of Smart Government is gaining particular attention by decision-makers, researchers, and urban planners. Although, there is a lack of shared definition of a smart city and resilient city, they are becoming significantly widespread labels. The common ground of a smart city and resilient city is the use of ICT as an empowering tool to deal with external pressures. Thus, the smart government idea seems to include a multi-objective strategy of information and communication technology development that can tackle related issues (Papa et al., 2015).

2.3.5. Organizational Resilience and Risk Management

Kantur and Iseri-Say (2012) informed that the unpredictable environment of today has highlighted the importance of resilience for organizations, individuals, communities, groups, and societies. The concept of resilience is an incredibly important concept in crises management. The restless and complex business environment of today has characteristics of increased competition, complex business operations, demanding customers, and unexpected cyber threats that have made organizations more vulnerable to business risks. The complex environment requires organizations to be more adaptable, flexible, and creative in responding to risks and changing conditions. This implies the need for resilience for organizations. That is the reason why several scholars have highlighted the importance of resilience as a concept for survival of the organizations in unpredictable, chaotic and turbulent environment (Rahman, 2016).

Although, a number of research studies have focused on resilience, only a few have presented a complete framework to practical application in an organization. For instance, Ishak and Williams (2018) in their study of a dynamic model of organizational resilience have argued that the need to have organizational resilience is as important as for any other organization. However, the model to implement resilience is not the same in all organizations. There are several aspects that strengthen the process of resilience of making it weaker and slower. Thus, the researcher presented a dynamic model that is expected to be appropriate for most of organizations that strive to achieve and maintain organizational resilience. There are two phases of the model: the preparation phase and the recovery phase.

Vucina and Fabac (2017) presented simulation scenarios by exploring the possibilities of using Monte Carlo methods to find some characteristics to design parameters of working units in an organization. Particular attention was paid to the protection of information systems and their vulnerabilities. The researchers explained that resilience is the ability of an organization's system to depreciate, effectively recover, and foresee disruptions or stress related events, and is related to its risk management process. However, the researchers have argued that resilience from the perspective of an organization means continued security attention and departure from traditional ways of organizational risk management. Overall, the study is valuable as it has offered a valuable option of simulation to enhance the readiness of an organization against any risks and threats, such as fire and accidents. Therefore, it will be easier for an organization to practice resilience with efficiency as it has practiced risk management using simulations.

Leautier and Rochet (2014) examined how organizations face volatility in market power, input prices, production, risk management, and pricing strategies. The issue of volatility is common among a number of industries, such as manufacturing, retailing, and energy where the companies that are risk averse in terms of financial frictions develop their risk averse strategies before their marketing strategies. This strategy is implemented through the risk adjusted cost, such as marginal cost under the probability measure due to risk aversion by stakeholders.

2.3.6. Management Control and Organizational Resilience

Organizational resilience has been analysed by Kerr (2016) with a finding that an organization must become resilient in order to ensure long-lasting success. The researcher stated that there are several business activities that gain success after an organization focuses on

resilience. However, there are three domains that have critical importance for achieving organizational resilience: operational resilience, supply chain resilience and information resilience. While highlighting the importance of management control for organizational resilience, the researcher has argued that resilience should be part of the strategy. In other words, the researcher is of the view that resilience should not only be the defensive strategy of an organization, but it should be a part of strategic management to establish a more holistic view of the activities, success and health of the business.

The operational management of organizational resilience has been explored by Annarelli and Nonino (2016) in their research. The researchers highlighted the current state of management control relationship with organizational resilience and provided future directions. According to the researchers, organizational resilience is the ability of an organization to go back to its previous state after it is hit by an unexpected event. This means, resilience is the ability of an organization to recover fast after a disruptive event. The researchers highlighted the importance and role of management control in this process. In fact, the process of organizational resilience is more efficient if it is described as a systematic framework for the organization to follow and achieve this goal. The risk of unexpected events is high in Smart Government as there are some specific issues related to the use of technology, such as cyber-attacks. Therefore, the role of management control is vital for resilience in smart governance. No matter how many plans an organization has developed related to risk management and resilience, it needs to make them part of organizational strategy.

According to a debate by Morais-Storz et al. (2018) in their research, organizations around the world are facing cyber threats. Although, there are laws and restrictions to prevent cyber-

crimes, hackers are creating new ways to continue their criminal activities. Therefore, it is crucial for organizations to prepare for an unexpected event by maintaining their capability of resilience. The researchers have suggested that application of the rules of management control and change management on organizational resilience will enable organizations to adopt resilience as a dynamic concept. Therefore, the valuable insight that can be found in this research is that organizations need to identify the change basis of their business to achieve resilience efficiently. An important aspect of incorporating resilience in management control is that it can be achieved successfully with the right team and top management with a resiliency and flexibility background.

In research conducted by Wilson (2010) seven organizational resilience principles were developed as a conceptual model of resilience for companies facing bankruptcy. The model has been evaluated using a qualitative approach. The results of the study support organizational resilience as a management strategy. Six of the seven organizational resilience principles were observed in the case study. The researchers also pointed to the use of de-centralized decision-making, ensuring external resource adequacy, expanded communication channels, and engagement of external stakeholders with the organizational environment. Thus, there is an increasing role of resilience in risk reduction for organizations.

There are different dimensions of strategic management that have been highlighted in research studies. Bouaziz and Hachicha (2018) argued that the business environment is changing significantly, so there is increased focus on resilience by organizations around the world. The researchers suggested that this can be achieved by employing strategic human resource management in organizational resilience practices. They justify the usage of strategic human resource practices in organizational resilience by showing the significant role of top management

in this process. Leadership awareness and how the top management perceive the operating environment affect their ability to deal with vulnerabilities and to face changes and disruptive events and recover very fast from such events. In the case of Smart Government, the need for such top management and leadership is growing every day to cope with the rapid changing environment in cyberspace around the world. This kind of human resource practice in choosing the right leaders for a Smart Government initiative that will take place in 2020 will take Dubai to new places among first class countries around the world with a minimum amount of risk and high ability to rebound after any crisis that could disrupt this new project. The above research shows how human resource practices affect organizational resilience and how strategizing the human resource practice, organizational resilience can serve its purpose. The 'agility' factor was found to be more effective in resilience dimensions throughout human resource practices than the 'robustness' factor.

A way to enhance resilience has been described in strategic resilience research undertaken by Anon (2018). It has been argued in the study that in highly complex business environments, companies need to examine their own challenges that they are likely to be confronted in the future; and how they grow to become successful. The research highlighted three basic elements of achieving resilience: problem development, future orientation of the organization and legacy of the organization. The research by Moraise-Storz et al. (2018) has been highlighted in the study as the researchers put forward the case of resilience and debated that more is needed by organizations. They introduced a more dynamic concept of resilience and argued that the business environment is changing constantly. Re-invention is important for such organizations, with the focus on how such organizations function in a highly volatile world and how they adapt to unique challenges. Getting back to a pre-crises state may not be an ideal position for an organization which seeks to

evolve. The role of top management is very important in this regard. The researchers have mentioned three core elements of strategic resilience: problem formulation, future orientation and organizational legacy. The problem formulation requires a business to reflect on the challenges faced, rather than only looking at solutions to risks. This refection initiates innovation and leads to paying more attention to the nature of the organization. The second element highlights the need for future oriented attitudes by top management that envisions how the future may look and how the organization needs to grow in order to develop in this environment. The future orientation is more than a set of actions, but it is more important and central for the managerial identity of those involved. Finally, the history of an organization plays an important role in how it faces challenges and achieves resilience.

While recommending the enhanced resilience of organizations, some scholars have developed frameworks to achieve this purpose. Resilience has been described by Buliga et al. (2016) as giving two major parts or characteristics: adaptability and robustness. Robustness is a system that returns to its actual state. In an organizational context, robustness is the ability of an organization to avoid loss by withstanding stress. Resilient organizations can absorb adversity and complexity by reducing vulnerabilities to risk environments, coping with the unexpected complexities, and recovering from these risk situations. The second important part is adaptability that gained attention in organizational theory in the 1980s. Resilience was considered as reinforcement and adaptation emerging from a traumatic, stressful, and challenging event. However, adaptability is the fast action taken during crises.

2.3.7. Managing Risk and Lower Vulnerability of an Organization

As described by Trim and Lee (2007), organizations face different kinds of risks related to policy, macro-economics, resources, competition amongst others. Risk management is a complex process that requires different types of management expertise and knowledge. By developing a proactive approach to risk management, it is possible for managers to instil resilience in the value system of an organization. The organizational resilience value system supports the establishment of beneficial working relationships. If managers focus on reducing the vulnerability of an organization's value, its ability to withstand attacks from competitors will increase. The incorporation of risk assessments into strategy can reduce an organization's vulnerability. The researchers have focused on strategic marketing intelligence and multi-organizational a resilience framework by paying attention to competitive intelligence, and the relevance of strategic purchasing. The researcher paid particular attention to risks faced by an organization and the need for counter intelligence.

As stated by Kantur and Iseri-Say (2015) organizations are increasingly facing the challenges of a changing business context. Economic downturns, terrorist attacks, uncertain competitive markets, political and social conditions, and global financial crises are the main challenges that organizations need to pay attention to and build their capacity of resilience. Organizational resilience also focuses on resistance capacity to face stressful conditions. The researchers stated that resilience can be managed and developed by using a set of organizational capabilities, practices and processes that help an organization to set diverse and adjustable integration. This is found in solutions and options offered by the researchers, including the need for development of cognitive contextual and behavioural capabilities that contribute to resilience. Thus, resilience capacity can be enhanced by developing strong leadership and increasing awareness of the organizational

environment. Human resource plays an important role in this regard. While discussing the factors that are crucial for resilience, several studies have highlighted the importance of human resource management. According to Mienipre et al. (2016) there is correlation between talent management in an organization and its ability to respond to and monitor risks. Thus, 'organizational' is a multidimensional concept that includes the highly important concept of human resource management.

According to Yaich (2016) there are changes in business ecosystems that include changes in customers, suppliers, administration, citizens, banks and new stakeholders. However, incomplete democratic transition, demands by internal and external stakeholders, and terrorist acts have increased pressure on organizations. In order to be successful, companies need to be more competitive at the national and international levels. The companies need to practice resilience in order to be successful in challenging business environments. They need to be more resilient as they face internal and external risks.

The literature related to resilience has proposed solutions that are practical for organizations. Most of the scholars have highlighted the importance of the role of human resources in the process of resilience. As explained by Sonnet (2016), the development of organizational resilience capacity is the strong base approach to considering and managing unexpected and continuous change as organizational strategic capability. The researcher has explained resilience as the capacity of an organization to get ready to face risks. This readiness is developed by the behaviours and beliefs of employees of the organization. Therefore, the researcher has suggested to consider human resource management interventions to strengthen resilience capacity. The study

concluded that specific beliefs and behaviours contribute to the development of readiness capability. The starting point can be the resilience capacity risk analysis.

In order to manage resilience and prevent risks affecting the organization again, some researchers have suggested some solutions based on analysis of literature. A useful study by Annareli and Nonino (2016) used this strategy and used a systematic literature review to find the research domain of resilience and its operational and strategic organization to understand the current and future research directions. The researchers found evidence that literature has consensus on the explanation of resilience, characteristics and foundation. The researchers also found that a significant number of research studies focus on supply chain resilience. However, there is a lack of consensus in the literature about resilience implementation, such as operational resilience and creating and maintaining resilience processes. This study by Annareli and Nonino (2016) and other research studies discussed in this chapter suggest that there is a need to focus on designing, implementation and improvement processes for enhanced resilience, measurement of operational and organizational resilience, resilience in small and medium enterprises, impact of information systems on resilience, innovation to enhance resilience, and dynamic capabilities and the strategic approach for resilience in an organization.

2.4. Chapter Summary

The relationship between resilience and cybersecurity risk management can be summarized in this section from the literature. Resilience can be defined as a risk management methodology. Mitchell and Harris have stated that the concept of resilience has been introduced so that a community, system or individual can deal with any change or disturbance which can give

rise to risks and uncertainties (Annareli & Nonino, 2016). As per the research, resilience is an integrating concept that takes into consideration multiple shocks, risks and stresses, and their implications. Risk and risk management have a strong connection with each other. Since cybersecurity resilience is a risk management approach, it shares a strong relationship with cybersecurity risks.

A wide range of authors, including Hirani, Lasiuk and Hegadoren (2016), have identified the association that exists between risk and resilience. They have suggested how, by improving the resilience of a system, it becomes easier to manage risks and uncertainties. The resulting risk can be measured in terms of composite cost and/or recovering time. As per Haimes, the resilience metric of any system could be measured as a complement of a risk estimate or a probability.

According to Campbell et al. (2019), resilience has become an extremely common concept in the current parlance of risk analysis. The cyber setting is considered to be highly unpredictable in nature, which gives rise to various kinds of risks and uncertainties. The risk associated with a cybersecurity incident has a direct implication on the cybersecurity infrastructure. The impact of the risk is highly influenced by the resilience of the cybersecurity system. In addition to this, it is also influenced by the type and sophisticated nature of the cyberattack. The consequence of cyber risk is impacted by the trajectory of the employed resilience of the cybersecurity. A cyber-resilient business undertaking is one that is able to effectively respond and recover from a cyberattack, continue to operate through it, gradually get back on track and strengthen its capability to withstand future risks and disruptions. The objective of cybersecurity resilience is to help entities be equipped to handle various kinds of risks and uncertainties that can arise in their path (Kwasinski, 2016). Haimes has stated that resilience is a system capability which is able to create foresight, to

identify, to predict and to defend against the evolving shape of the risk before negative repercussions arise.

Cybersecurity resilience ensures that risks and opportunities are effectively managed, which has the potential to cripple the IT ecosystem of an organization. The cybersecurity capabilities and resilience of an enterprise are designed and upgraded on a regular basis so that sophisticated risks and threats can be effectively tackled. The objective of cybersecurity resilience is to help an organization get back on track after a risk has disrupted the business activities or processes (Holm & Ostergaard, 2015). Cybersecurity resilience is designed to implement enterprise-level risk management so that both the technical factors and human factors can effectively function for the end-to-end business continuity. Resilience is linked with cybersecurity risk as the process helps in identifying critical processes and functional implications and helps in implementing proper measures so that the firm will be able to recover after a security incident and be capable of withstanding future risks and uncertainties.

The resilience of cybersecurity is a long-term view that must be designed in a durable manner so that it will play a critical role in avoiding disastrous failure, which could arise for a business due to IT risks and vulnerabilities. Thus, a comprehensive resilience plan has to be designed, which includes the actions and results before, during and after the emergence of a cybersecurity threat. The long-term approach on the part of the leaders and decision-makers is of paramount importance while devising effective and functional cybersecurity resilience.

Thus, the literature review was done systematically according to key themes and elements of resilience processes as follows, this table explains the key themes identified from the

cybersecurity resilience literature review and led to developing the methodological Smart Government resilience framework of this thesis:

Table 2.1: Key themes in resilience processes

Forces of change	Vulnerabilities	Management controls	Capabilities	Resilience Balanced /unbalanced	Business profitability	Risk	Performance
Orlikowski and Robey, 1991	Sikula et al., 2015	Ridley and Channing,1999	Devadoss, Pan, and Huang in 2002	Guth,1981/ Drabek, 1986/ Orlikowski and Robey, 1991/Pauchant and Mitroff, 1992	Fritz, 1999	Ridley and Channing,1999	Chesley, D., and Amitrano, M., 2015
Aicholzer and Schmutzer, 2000	Schell, 2016	Leck,2015	Pan, 2006	Klein., 1998/Fritz, 1999/Ridley & Channing,1999	Aicholzer and Schmutzer, 2000	Jarrow, 2011	Olson A., and Anderson J., 2016
Chesley, D., and Amitrano, M., 2015	Jenab and Moslehpour, 2016	Olson A., and Anderson J., 2016	Jarrow, 2011	Aicholzer and Schmutzer, 2000/ Adger, 2000	Olson A., and Anderson J., 2016	Schell, 2016	Chandler, 2014
Zaklina Spalevic, 2014	Arlitsch and Edelman, 2014	Zaklina Spalevic, 2014	Nastasiu, 2016	Cardenas, et al (n d)/ Devadoss, Pan, and Huang in 2002/ Leveson., 2002		Ackerman & Rushe, 2014	
Jenab and Moslehpour, 2016		Arlitsch and Edelman, 2014	Christou, 2016	Barab´asi, 2003/ Lambert, & Knemeyer, 2004		Nastasiu, 2016	
		Bagheri, & Ridely, 2017				Cardenas, et al (n d)	

North, et al, 2016	Stolfo et al, 2008	ENISA, 2011	CISCO, 2011	Gordon., & Larry., 2005/Longstaff, 2005/ Cocchiara, 2005/ Pan, 2006	Stolfo et al, 2008	Linkov, et al, 2013	ENISA, 2011
NIST, 2014	North, et al, 2016	Bagheri, & Ridely, 2017	Keys, et a, 2016	Boin and McConnell, 2007/ Nag, et al, 2007	Cavelty, et al, 2015	Annareli, & Nonino, 2016	Bagheri, & Ridely, 2017
Blowers, et al, 2016	Blowers, et al, 2016	Linkove et al, 2013	Linkov, et al, 2013	Trim, & Lee, 2007/Stolfo et al, 2008/ Wilson, 2010	Cardenas, et al (n d)	Barab´asi, 2003	Bodeau & R. Graubart., 2011
Bodeau & Graubart., 2011	Gartner, n. d	Bosen, 2017	Gartner, (n. d)	Jarrow, 2011/ ENISA, 2011	Keys, et a, 2016	Ward., J. 2015	
Sonnet, 2016		Annareli, & Nonino, 2016		CISCO, 2011/ Harrington, & Ottenbacher, 2011	NIST, 2014		
				Bodeau & R. Graubart., 2011	Bagheri, & Ridely, 2017		
Leveson., 2002	Hyslip, G., 2016	Hyslip, G., 2016	Kerr, H., 2016	Bodeau & R. Graubart., 2011	Klein., 1998	Kerr, H., 2016	Hyslip, G., 2016
Sonnet, 2016	Lambert, & Knemeyer, 2004	Trim, & Lee, 2007	Lambert, & Knemeyer, 2004	Leydesdorff, & Deakin, 2011	Leveson., 2002	Mienipre, et al, 2016	Kantur & Iseri-Say, 2015
Yaich, 2016	Trim, & Lee, 2007	Drabek, 1986	Annareli, & Nonino, 2016	Linkov, et al, 2013/ Kahn, Barton, & Fellows, 2013	Yaich, 2016	Kahn, Barton, & Fellows, 2013	Adger, 2000
Kantur & Iseri-Say, 2015	Barab´asi, 2003	Boin and McConnell, 2007	Sonnet, 2016	Dess, et al, 2013/ Schroeder,	Kantur & Iseri-Say, 2015	Cocchiara, 2005	Longstaff, 2005

				2014/ Zaklina Spalevic, 2014			
Newnham and Crask, 2015	Kahn, Barton, & Fellows, 2013		Adger, 2000	Leautier & Rochet, 2014/ Chandler, 2014/ Arlitsch and Edelman, 2014	Newnham and Crask, 2015		Drabek, 1986
Boin and McConnell, 2007	Pauchant and Mitroff, 1992		Longstaff, 2005	Ackerman & Rushe, 2014/ NIST, 2014	Cocchiara, 2005		
Leydesdorff, & Deakin, 2011	Vucina, & Fabac, 2017	Vucina, & Fabac, 2017	Papa, et al, 2015	Annareli, & Nonino, 2016/ North, et al, 2016/	Wilson, 2010	Papa, et al, 2015	Bouaziz, & Hachicha, 2018
Vucina, & Fabac, 2017	Morais-Storz, et al, 2018	Bouaziz, & Hachicha, 2018	Wilson, 2010	Schell, 2016/ Jenab and Moslehpour, 2016/	Bouaziz, & Hachicha, 2018	Leautier & Rochet, 2014	Moraise-Storz et al, 2018
Morais-Storz, et al, 2018	Buliga, et al, 2016	Anon, 2018	Moraise-Storz et al, 2018	Mienipre, et al, 2016/ Kerr, H., 2016/ Yaich, 2016/		Morais-Storz, et al, 2018	Mienipre, et al, 2016
Bouaziz, & Hachicha, 2018	Trim, & Lee, 2007	Trim, & Lee, 2007	Buliga, et al, 2016	Buliga, et al, 2016/ Scholl, & AlAwadhi, 2016/ Bosen, 2017/ Gartner, (n. d)		Anon, 2018	
Anon, 2018		Mienipre, et al, 2016		Bagheri, & Ridely, 2017/ Vucina, & Fabac, 2017/		Trim, & Lee, 2007	

				Bouaziz, & Hachicha, 2018			
Moraise-Storz et al, 2018				Morais-Storz, et al, 2018/ Anon, 2018			
Pauchant and Mitroff, 1992	Sonnet, 2016	Dess, et al, 2013	Boin and McConnell, 2007	Sikula et al., 2015/	Boin and McConnell, 2007	Guth,1981	Nag, et al, 2007
Anthpoulos, 2015	Lambert, & Knemeyer, 2004	Nag, et al, 2007	Gordon., & Larry., 2005	Newnham and Crask, 2015/	Ward., J. 2015	Mienipre, et al, 2016	
Harrington, & Ottenbacher, 2011	Trim, & Lee, 2007	Harrington, & Ottenbacher, 2011	Anthpoulos, 2015	Cavelty, et al, 2015/	Gordon., & Larry., 2005	Kahn, Barton, & Fellows, 2013	
Guth,1981		Schroeder, 2014		Chesley, D., and Amitrano, M., 2015/ Anthpoulos, 2015/ Ward., J. 2015/	Dess, et al, 2013		
Schroeder, 2014		Dess, et al, 2013		Kantur & Iseri-Say, 2015/ Leck,2015/ Papa, et al, 2015/Sonnet, 2016	Dess, et al, 2013		
Scholl, & AlAwadhi, 2016				Hyslip, G., 2016/ Nastasiu, 2016/ Christou, 2016/ Keys, et a, 2016/ Blowers, et al, 2016	Leydesdorff, & Deakin, 2011		
Leydesdorff, & Deakin, 2011	Vucina, & Fabac, 2017	Vucina, & Fabac, 2017	Papa, et al, 2015	Annareli, & Nonino, 2016/	Wilson, 2010	Papa, et al, 2015	Bouaziz, & Hachicha, 2018

				North, et al, 2016/			
Vucina, & Fabac, 2017	Morais-Storz, et al, 2018	Bouaziz, & Hachicha, 2018	Wilson, 2010	Schell, 2016/ Jenab and Moslehpour, 2016/	Bouaziz, & Hachicha, 2018	Leautier & Rochet, 2014	Moraise-Storz et al, 2018
Morais-Storz, et al, 2018	Buliga, et al, 2016	Anon, 2018	Moraise-Storz et al, 2018	Mienipre, et al, 2016/ Kerr, H., 2016/ Yaich, 2016/		Morais-Storz, et al, 2018	Mienipre, et al, 2016
Bouaziz, & Hachicha, 2018	Trim, & Lee, 2007	Trim, & Lee, 2007	Buliga, et al, 2016	Buliga, et al, 2016/ Scholl, & AlAwadhi, 2016/ Bosen, 2017/ Gartner, (n. d)		Anon, 2018	
Anon, 2018		Mienipre, et al, 2016		Bagheri, & Ridely, 2017/ Vucina, & Fabac, 2017/ Bouaziz, & Hachicha, 2018		Trim, & Lee, 2007	
Moraise-Storz et al, 2018				Morais-Storz, et al, 2018/ Anon, 2018			

The above (table 2.1) shows that resilience is better studied as a quantitative variable. It also shows how previous studies measured resilience according to seven elements/components, as is the case in this research, whereas each study consists of two or three elements of the framework

suggested in this research, along with resilience, the main factor that gather these studies under one context.

Nevertheless, when tracking theories of resilience from 1981 until 2018, the focus became more on the change factors than the vulnerability factors. The priority switched between the elements throughout time, whereas in the 1990s the focus was more about vulnerabilities and capabilities factors, while in the twenty-first century the focus shifted to emphasize more on change factors and management control. Of course, after realizing that the problem was not just about computers and cybernetic errors, researchers acknowledged that human errors have greater impact, especially in the constant changing cyber and business world. The role of management control shows significant implication on resilience to overcome the new crises experienced in the cyberspace arena.

The framework suggested in this study consists of the main components of the resilience process or framework, applying them to business management arena. The framework covers business continuity, business profitability and performance of an organization. The reason is that the overarching goal of Smart Government is usually to enhance the business arena in the country, e-commerce, e-billing and, e-banking.

In conclusion, three areas were focused on when reviewing the literature: the components of the resilience framework, the methods of measuring cybersecurity resilience, and the evaluation criteria of the existing resilience frameworks according to a business management scale. This was done to fulfil the study aims and objectives.

CHAPTER THREE: THEORETICAL FRAMEWORK

3.1. Smart Government Resilience and Risk Management

In terms of evaluation criteria of the previous resilience frameworks, according to Mbanaso and Abrahams, the Cybersecurity Resilience Maturity Measurement (CRMM) framework can be introduced in the organizational context as a key component of the cyber risk management model (Schipper & Langston, 2015). It can primarily provide a suitable basis for managing and handling the various kinds of cyber risks in a proportionate and consistent manner. As per the U.S. Department of Homeland Security, a robust cyber resilience review (CRR) must be in place so that organizations will be equipped to manage the cyber risks that they might face in the most efficient and professional manner. The fundamental objective of CRR is to enable business entities to assess the performance of the principal cybersecurity practices effectively. The NIST Cybersecurity Framework has captured the common taxonomy and mechanism that entities need to follow in order to establish a robust resilience model. They should be able to describe the current cybersecurity posture, including all the characteristics, the proper identification and prioritization of the opportunities for improvement must be in place, and the thorough assessment of the process towards the target state must be in place. Such an integrated approach is necessary so that the effectiveness of the cybersecurity resilience can be measured.

In the highly unpredictable cyber setting, business leaders need to make sure that they measure the resilience of cybersecurity on a consistent and regular basis. Such an approach will enable them to locate existing gaps and overcome them in the most effective manner. Some of the common elements that can be measured to obtain a detailed insight into the resilience of cybersecurity include the evaluation of the effectiveness of cybersecurity training in the organizational setting, the assessment of the implementation of the updated cybersecurity policies

throughout the organization and the supervision of the existing processes. Such a holistic and integrated measurement of resilience is essential, and it can help business organizations to be properly equipped to carry out the day-to-day business processes without being affected by the threats and risks that arise in the cyber setting (Yoon, Kang & Brody, 2016). Thus, the accurate measurement of cybersecurity resilience is a vital part of the cyber risk management model that can help firms to sustain and survive in the unpredictable online setting. All the metrics must be thoroughly examined to obtain a detailed insight into the effectiveness of cybersecurity resilience.

As per Kwasinski, the evaluation of systems and resilience modelling has become quite challenging in nature due to various factors, such as operational interaction among mechanical and electrical subsystems and complex kinds of dependency (Kwasinski, 2016). The study basically captures how cybersecurity resilience can be modelled and quantified in various systems, such as cybersecurity systems, complex engineering systems, and others by using various techniques. The quantitative approaches that have been highlighted by the author include optimization, game theory, control theory, data-driven analytics, network complexity, and a Bayesian network.

Quantitative concepts relating to system or mission performance are considered to be highly critical in nature when it comes to cyber resilience. Thus, they must be specific to the exact mission of an enterprise. The quantitative theories to study cyber resilience must include objective measures, such as the total number of successful 'received and responded' web server requests to per time unit, and the total number of packets traveling through a network link without any error per time unit (Holm & Ostergaard, 2015).

After justifying the evaluation method of this research, the researcher will provide the following table to clarify how the previous resilience frameworks were reviewed and evaluated to set a focus for this study. However, in order to set a focus, this study has outlined the limitations

and benefits of the existing models in order to highlight their efficiency for collecting data for the key theme of cybersecurity and resilience (Kothari, 2004).

Table 3.2: Frameworks and Evaluation Criteria

The framework details & focus areas	Benefits	Limitations
European Union Agency for Network and Information Security Standards (ENISA)	• The (ENISA) has developed a framework based on appropriate metrics. • It has identified different principles that are important during the process of creation and implementation of a program that is created with the purpose of cyber resilience. • These metrics are required to have some technical aspects, such as quantifiable, comparable, and repeatable. Good metrics are also required to have some non-technical aspects; and should be relevant, to organizational mission, easily obtainable, and work for improvement of resilience (ENISA, 2011).	• Good metrics are also required to have some non-technical aspects; and should be relevant, to organizational mission, easily obtainable, and work for improvement of resilience.
Local Government Research Center Framework	• The Bloustein Local Government Research Center at Rutgers University published a paper in 2015 with title of 'Managing Technology Risks through Technological Proficiency'. • The research explained risks that initiate from the actions taken by people, failure of a technical system,	• The framework did not cover the managerial aspect, it looked at cybersecurity as technical issue only which is far from truth. The framework missed that cyber

	an operational process, or management, as well as disruptions caused by outside events. • These risks are explained with six interrelated concepts: operational, cybersecurity, legal, reputational, financial, and societal. • The research has presented a framework that offers organizations to tackle risk with their technical proficiency. • The main focus of the framework is on achievement of technological proficiency by creating and implementing four basic practices: planning, governance, cyber hygiene, and technical competence (Keys et al., 2016).	problems are not all IT errors, but human errors as well.
National Institute of Standards and Technology's Framework (NIST)	• The (NIST) published a framework in 2014, with the purpose of improving critical infrastructure cybersecurity. • The main focus of the framework is on utilizing the business processes of an organization to guide the activities related to cybersecurity; and to make cybersecurity internal with risk management process of the organization. • The main goal of NIST framework is to protect civil liberties. • However, as it was prepared, while taking critical infrastructure into consideration, one can use them in different scenarios (National Institute of Standards and Technology, 2017).	• A study by Hoffman Jooffman (2014) in the form of an article criticizing the structure of NIST, found that this structure contains no details and requires research so that a government organization can use it, where risk is very important. He added that the frameworks form a brilliant start, but ultimately, they disappointed their customers.

Network Centric Warfare (NCW) Framework	• The warfare and disaster resilience have the characteristics of complexity, surprise, necessity of adoption, and urgency. • The military scholars have developed a Network Centric Warfare framework that creates awareness and creates decentralized decision making as it distributes information across various networks that operate in different domains of information, cognitive, physical, and social. • These domains are as follows: • **Information –** manipulation, creation, and storage of data • **Physical –** facilities, sensors, system states, equipment, and capabilities • **Cognitive** – mental models, understanding, biases, preconceptions, and values • **Social** – collaboration, interaction, and self-synchronization among entities and individuals	• This framework was developed by military scholars, so it might not suit other kinds of organizations.
National Academy of Science (NAS) Framework	• The framework emphasizes that cyber resilience is not only the concern of IT departments, but it has become highly important in today's hyper connected world. • It also pointed out that Cyber resilience is not only about cybersecurity, but it includes the business practices and has ability to absorb cyber-attacks, recover from those attacks, and restore operations of an organization quickly	• Although it talks about cyber resilience from both perspectives, managerial and technical, however it lacks details of how an organization will peruse this vision.
Linkov Framework	• Linkove et al. (2013) has combined the definition of disaster resilience by National Academy of Sciences (NAS)	• This framework has the same problems of the frameworks that

	with Network-Centric Warfare (NCW) framework that explains operational domains of information, cognitive, physical, and social to develop resilience metrics. • There are four categories of resilience as explained by NAS: prepare, absorb, recover, and adapt. The NCW framework explains four operational domains as physical, information, cognitive, and social. • Linkove created a matrix by combining NAS and NCW frameworks. The framework estimates a system's ability to handle cyber-attacks, and provides metrics for resilience assessment. All metrics in the framework are interrelated and has implications on other metrics. • Linkov framework for cyber resilience has been used by several researchers to find solution to the issue. As businesses and federal government depend on cyber infrastructure for their functions, their vulnerability is extremely high to cyber-attacks.	its consists of. Linkov et al 2013 have tried to fill in the gaps in the previous frameworks by combining them in one framework and end up with less limitations than other resiliency frameworks.
Internet of Things (IoT)	• This highlights the maintenance and security challenges too. The increased automation and networking of power plants has created challenges as well for system security and safety in the event of updating the software (Blowers et al., 2016). • The frameworks discussed above have not mention the IoT that can enable technologies to sense and communicate with their external	• This framework is technical only, it does not cover the managerial or business perspectives.

	environment or internal states. However, most of the components of NIST and Linkove frameworks address most of security issues related to operational security. • The vulnerability of technologies revolves around the interaction among different systems. Data protection and coordination with external environment are the main focus of operational security. • There is little research on operational security; however, there is need to view best practices for internet technology through a different lens with the purpose of applying it to the Internet of Things	
Keys et al., framework	• Adapted a framework that can measure cyber resilience in different sectors and industries. The framework is mainly based on Linkov et al., and NIST framework for Improving Critical Infrastructure Cyber Security because the Linkov framework addressed that concern that most of risk-based assessments combine resilience and risk. • The framework introduced by Keys et al., (2016) has the following categories: • **Plan and Prepare.** • **Detect.** • **Absorb.** • **Recover.** • **Adapt.**	• Keys et al., decided to choose the Linkov framework as it addresses the needed components of resilience. • However, as the Linkov framework does not address the actions related to threat detection to the degree as NIST framework, there was need to combine both frameworks and to create a unique framework.
Cybernetic resilience in the UAE	• According to Bosen (2017), the government in the UAE is taking a	• However, after studying resilience and cyber security risk

(Dubai Smart Government)	pro-active response for the safety of country's digital infrastructure. • The approach of the government is to safeguard the features of digital infrastructure from harm. • The network helps in data exchange among government and local entities. The cybersecurity initiative of the UAE government follows the introduction of cybersecurity strategy in Dubai with the purpose of strengthening the position of the country as global leader in safety, innovation, and management of cyber security risks. • The main focus of the strategy is on the domains of being a cyber smart nation, ensuring society's development, innovation, cyber space security, and cyber resilience. • The government of the UAE is focusing on cyber resilience in order to avoid threats in changing cyber environment. His Highness Sheikh Mohammed bin Rashid Al Maktoum has recently launched the Dubai Cyber Security Strategy in order to strengthen the position of Dubai as global leader in safety, innovation and security. • The Dubai Cyber Security Strategy includes following domains: • **Cyber Smart Nation:** The domain has the purpose to increase awareness among people about cybersecurity to ensure building the society that understands the threats related to cybercrime, and learn the skills that	management in Dubai in-depth, it has been found that they are still in the proactive risk management stage when it comes to the maturity of their system. • However, the environment and culture in the UAE and especially in Dubai encourages innovation and its readiness to implement resilience plans is high according to the survey and this research investigation. • The Dubai smart Government is welling to adopt new ways of thinking and new strategies concerning cybersecurity because it is trying to protect the upcoming event of expo 2020 which cannot be vulnerable to the risk of shutting down its system in the night of inauguration. • Dubai has received a lot of threats and has been number two in targeting its systems

	are important to manage risks related to cybersecurity among private and government institutions. • **Innovation:** The domain of innovation is about scientific research and innovation in the field of electronic security and development of cyber space to encourage innovation in the country. • **Cyber Resilience:** The domain of resilience focuses on flexibility in cyberspace, and ensuring the availability of information technology systems if there is cyber-attack. It also aims to build a platform to exchange information and support in managing incidents of breach of cyber security. • **Cyber security:** The purpose of cybersecurity domain is building control for making cyberspace secure (Emirates 24/7 News, 2017). • The Dubai also launched an experimental small smart district, which a complete city that uses only smart system, which is a great step towards resilience. Whereas resilience depends on resilience scoring, repeating plans, repeating training, mocking cyber-attacks and the number of time resilience plans are being tested and	after Israel, due to its highly integrated infrastructure. • Sheikh Mohammad bin Rashid, the ruler of Dubai, assigned a million dirham price of the best cyber security plan to be adopted by the system of smart Dubai. • Its moving really fast, from e-government to Smart Government to smart Dubai. • More and more issues are deriving from this fast moving and changing business environment. • put under trial until they reach the level of agility and rapid detect, adapt, recover, and prosper from the attack. • It is noteworthy that the agility is an important factor in the process of resilience, otherwise the organization will not be considered resilient but rather unprepared.
Gary Hyslop's framework	• To set up the approach for managing cybersecurity risk, the research of Gary Hyslop (Chief Information Security Officer (CISO) for the City	• At the same time Mr. Hayslip used very common NIST (National Institute of

	of San Diego) will be used in the current framework. • The framework provides a common language for understanding, managing and expressing the life-cycle concept of cyber security risk, both inside and outside. It can be used to manage cybersecurity risk throughout the organization, or it can be focused on delivering critical services within the organization. • Different types of organizations - including coordination structures sector, associations and organizations - can use a framework for a variety of purposes, including the creation of common profiles. • According to CISO there are six steps to implement risk management process into strategic operations: • Categorize information systems and data • Select security controls • Implement security controls • Continually assess security controls • Authorize (verify risk baseline) • Continually monitor security controls	Standards and Technology) Risk Management Framework. As he mentioned: "to demonstrate a mature risk management methodology that would enhance an organization's cyber security program if implemented properly." (Cyber-Security & Risk Management, an evolving ecosystem, 2016)[vi]
IBM Business Resilience Model	• It is has been defined that the IBM has given and begun a business flexibility system. • The system is intended to recognize the dimension of hierarchical versatility. • It contains many items named as layers which underline the flexibility limit of any business (Zamoum, 2007).	• However, this framework concerns business resilience and missed technical and resilience assessments measures for achieving political and business goals.

	• In the late 1990s scientists jabbered about building up the authority thought in the business firms and expansive scale programs. • While as of late risk management rose to the top for the association to have the capacity to make due in the quickly developing business field and the emerged of several rivalries (Bayuk et al., 2012).	
This Thesis framework	• Cyber resilience is the ability of an organization to recover from cyber-attack. • Therefore, cyber resilience is the key element for organizational sustainability. • There are several moving parts of cyber resilience that should be approached methodologically. • There are five interconnected domains of cyber resilience framework; and each of those domains has different function. • The domains are identified, protect, detect, respond, and recover. • **Architecture of Cyber Resilience Framework** • Asset management • Configuration and change management • Controls management • Incident management • Vulnerability management • Service continuity management • Risk management • External dependency management • Situational management	• Although this suggested framework tried to cover all the important matrix and elements to a balanced resilience system, besides emphasizing the main factors that have a great impact on resilience status, it's subject to criticism by scholars and researchers. • There is no framework that is best, but this thesis has tried to do its best to create a simple tool that can be used in all kinds of organizations, governmental, private, big small scaled. • Technically not in depth, managerial and business in depth

Electronic government provides online services through IT instruments and the internet, where most of its processes and functions take place in cyberspace. Smart Government also builds business initiatives between a government and its public along with private sectors and especially with regulated entities. The Smart Government represents the domain of the problem in this research due to its nature and environment and the vulnerability that is attached to the internet and online services which can be summed-up with one word 'cyberspace'. Financial transactions, sensitive documentation, confidential files and high security information that cannot be exposed to the public are inside the system of the Smart Government, thus, the need for a suitable cybersecurity risk strategy has arisen and with the current technological breakthroughs risk management is not enough and the importance of cybernetic resilience has arisen.

Research on the implementation of Smart Government cybernetic resilience is rather limited, because of the wrong view of the public sector as rigid and risk averse. The increase of the number of Smart Government initiatives around the world makes this cybernetic resilience a special research arena, due to the lack of studies and theories in this domain.

Prior studies and theories of the Smart Government focused on E-democracy and E-Legislature by Coleman, Taylor and Van de Donk (1999) along with the E-citizenship issues explored by Bucy and Gregson (2001). Furthermore, in the previous studies the focus was on governance issues and theories in the current period of IT information breakthroughs (Tapscott, Lowy & Ticoll, 1989).

In addition to the prior research arenas, research that was conducted by Devadoss, Pan, and Huang (2002), explored the Tele-cooperation and other research about electronic commerce that was conducted by Fritz (1999).

The reason behind the creation of Smart Government is the crucial need to cooperate with the rapid development around the world and to satisfy the hard to please audience of the public; this need has found a powerful tool in IT, which is able to fulfil this need for both governments and publics (Orlikowski & Robey, 1991). Aicholzer and Schmutzer conducted a study (2000) claiming that Smart Government has changed the notion of governance in many ways: business transformation of governance – services improve in delivery and quality, cost reduce, and the administrative processes rejuvenate; the business transformation of governance can re-examine the performance and the function of the democracy in both its processes and practices. The complexity of Smart Government projects comes from the absence of three elements: fundamental structures, human and technical resources, along with the vast size of the government. Moreover, the nature of government as bureaucratic also contributes to this complexity (Pan, 2006).

Nowadays, it is crucial to have the ability to leverage the standards of the cyberspace, telecommunication and electronic infrastructure industry to cope with rapid technological development and artificial intelligence across the globe, whereas the hackers are not slowing down any time soon. The need to raise the bar in this industry is critical. Organizations around the world should employ tools that are innovative and effective and they must document successful practices, then use these tools and practices to outline their continuity plans. This summarizes the need and the notion of resilience in Smart Government projects.

Every organization needs professionals and experts in business continuity, as hey help in two essential processes. The first one is ‘planning’ and the second is ‘readiness’. These two elements will help such organizations to mitigate risk or the impact of unforeseen disruptive events. These two elements also aid in the functionality of the critical business continuity, such as Smart Government, even with the existence of potentially disruptive events such as breakthroughs. The

critical environment of Smart Government which takes place online and has a high exposure to risk, which is a result of its nature of vulnerability despite all the IT instruments that are employed to protect it and make it more secure. As discussed earlier, Smart Government documents tend to be more confidential and sensitive and protecting these data is a crucial need or else it will lead to a disaster or even national security catastrophe.

The risk management is not enough in this case. According to a study conducted by Sikula et al. (2015) risk management is not enough and the need for resilient scientific frameworks has arisen, especially in the existence of vulnerabilities in the virtual means of communication. The team set a conceptual framework of resiliency for the practitioners to adapt and to adjust according to the needs of their organization to help recover after cyber-attacks and then learn how to evolve and prosper post trauma (p. 222).

3.2. Risk Management vs. Resilience: H1 "Capabilities"

After a systematic review of the literature, and analysing the factors that affect resilience and risk management plans, besides studying the websites and online gates of Smart Governments, the researcher identified that the key capability factors are: flexibility in sourcing, capacity, flexibility of order fulfilment, efficiency, visibility, anticipation, adaptability, recovery, disruption, collaboration, organization, security, market position, and financial strength (Jarrow, 2011). Some of the above factors can be related to traditional risk management strategies and some can be related to resiliency plans (Christou, 2016). The capability factors depend on the organization's legacy, the financial status and its business resources, and how much they are willing to invest in resiliency plans and cybersecurity risk management to achieve sustainability and business continuity

(Pennauther, 2001). This will let them embrace opportunities in a safe way and employ their legacy to be more resilient than any other organization in the market.

Ridley and Channing (1999) divided risk into negative and positive; they argued that if the risk does not exist, the need for the antidote would not exist in the first place. In local authorities, they refer to the pro-active approach of providing certain kinds of services to certain public entities as positive risk which is encouraged by risk and disability. These pro-active programs will define, prioritize and mitigate risk before it happens, they can work as capability factors to achieve and maintain resilience (p. 81). They argued that the decision on how to manage the risk only occurred after listing and assessing capabilities and risks, and building a table of priorities among these factors; this is done for the researcher to be more familiar with both capabilities and risks and to choose a rational, reasonable and suitable strategy for the sake of risk management. (p. 78)

While testing the hypothesis of the research which suggested that the capability factors affect resilience in Smart Government organizations, the researcher identified a lot of evidence in the literature that suggested significant impact of capability factors on resilience and risk management plans (Anthpoulos, 2015; Papa et al., 2015; Wilson, 2010; Moraise-Storz et al., 2018); the capability factors of an organization support its resiliency status, especially when it comes to the maturity level of their system. Resiliency plans and cybersecurity risk management strategies do not come with a low cost, on the financial, technical and managerial levels. They demand all kinds of available resources, including experienced cadre, resilience teams and managers along with IT programs and programmers (Kerr, 2016).

By reviewing the literature on risk management, one can notice that there is a gap of insufficient research addressing political and national security issues; huge amounts of literature

exist regarding financial, medical and technical risk management, while few studies exist that discuss managerial risk management, such as data security (Keys et al., 2016).

However, testing hypothesis needs further investigation (see Chapter 7, Hypotheses testing table), especially when it comes to quantitative variables, such as resilience (Buliga et al., 2016). This explains the quantitative study and the statistical instrumentations of this thesis to investigate this hypothesis. In this regard, Annareli and Nonino (2016) found that the capabilities have the highest impact on resilience, such as Coca-Cola company and their legacy strength. This study by Annareli and Nonino (2016), and other research studies suggested that there is a need to focus on capabilities in terms of designing, implementation, and improvement processes for enhanced resilience, measurement of operational and organizational resilience, resilience in small and medium enterprises, impact of information systems on resilience, innovation to enhance resilience, and 'dynamic capabilities' and strategic approach for resilience in an organization (Sonnet, 2016).

Leck (2014) conducted a study investigating the managerial risks in the work arena, wherein he discussed the basic models of accidents in the work environment. The researcher focuses on the old hypothesis that says: nothing happens coincidently; rather, he suggested that every accident or risk takes place because of a malfunction in the corporation's risk management system and/or safety plan, including major accidents. All such incidents according to Leck are considered the manager's fault. He added, if managers applied a strong safety system and a pro-active risk plan and their organizations have sufficient capabilities, these kinds of threats could be diminished or even prevented entirely (p. 120).

Jarrow (2011) conducted a study entitled "Risk Management Models: Constructing, Testing and Usage". The study highlighted the importance of 'capabilities' in risk management models in all kinds of organizations. The study focuses on prescription drugs which have a beneficial value to patients when used correctly; on the other hand, they could have an unhealthy impact when used wrongly. However, he argued that these prescriptions, as with any other risk, may lead to death (number one priority in risk management). He argued that this risk does not mean that one should stop using such drugs, or in this case the projects should not be stopped but planned in a scientific, educated and strategic way. Meaning, that organizations with less capabilities should not lose hope in terms of how much their capabilities' lacking will affect their resiliency plans, they must not stop their projects but rather implemented them in a professional way. They must understand that the need for risk management models which emphasize resilience is even more urgent, especially in the financial markets which are more complex and difficult to navigate. According to Pennauther (2001) organizations can harness their experience and use their legacy.

Olson and Anderson (2016) added that the story of resilience makes more sense and has a lot of specific information inside of it, compared to Risk Management, but it always goes back to the capabilities of an organization. On the other hand, the organizational resilience will form a complete picture or vision right after the implementation of the resiliency scoring plan, the planners will set specific goals and strategies of what an organizational resilience should look like after performing the resiliency scoring in the business continuity plan. Their suggested methodology of resiliency scoring will help improve the ability to evaluate the quality of an organization business plan, whereas this method could help in removing any undesirable ambiguity besides offering multiple suggestions to enhance the quality of the plan which has not been noticed by the planners earlier (p. 41).

According to Chesley and Amitrano (2015) the difference between risk management and resilience is that the first one deals with potential risk or the disaster change, whereas the second notion of resilience has the ability to deal with the good and bad, meaning all kinds of change not only negative or catastrophic developments. They added that the change is everywhere nowadays and in our case we are talking about a Smart Government project which can be a catalyst for change especially in the business, communication and infrastructure areas. This highlights the importance of enterprise resilience, which can be more effective in these cases of technological breakthroughs than risk management (p. 4). This emphasizes the forces of change hypothesis (H2) which will be explained in the next section.

3.3. Managing Cybersecurity Risk to Achieve Resilience: H2 "Forces of change"

Internal and external change in an organization, such as social change, political change, and environmental change can affect its resiliency level. Many authors (Morais-Storz et al., 2018, Bouaziz & Hachicha; 2018; Anon, 2018; Moraise-Storz et al., 2018) have explored the change as a fundamental factor. In 2014 the Educational Journal in the UK posted an article about a new special education the government had planned for the young generation – 'educational change' – in a very early age (10-14yrs old), to make the UK more resilient to change and cyber-attacks. This special education could improve the cybersecurity skills among the new generation which will prepare them for future change and potential risk and reduce the crime level occurring in the UK electronic systems in both large-scale and small-scale business organizations. According to the article, cyber-breaches cause extensive financial issues, and cost approximately £850,000 in some cases. Moreover, Schell (2016) conducted a study about the importance of cybersecurity in today's systems, where organizations are in-need of a new security-based system; he argued that the

problem will remain the same if we continue using the current system architecture which does not have a firm requirement for maintaining the right level of flexibility and security for 'environmental change'. He added, the flexibility and security of systems could be achieved effectively in a "non-computable way, by applying up-to-date methods that could cope with the new systems" and their demands in the change and risk arenas. He pointed out that the known workflow remains unprotected even after fixing it; when the un-countable flaws remain, the risk still exists (p. 20).

Zaklina Spalevic (2014) conducted a study highlighting the issue of cybersecurity, as a global challenge of "technological and organizational change", which could be solved by advanced IT technical instruments along with an excellent "information infrastructure" (p.687). It is noteworthy that this thesis focuses on the second part of the above theory, as the researcher will focus on the information processes and infrastructure, meaning the managerial side of the topic. While the IT arena has been addressed in many computer science and computer engineering research studies conducted previously, the non-stop changing environment and continuous cyber-attacks led to an innovative strategy that suggests the exploitation of information infrastructure; which might contribute in enhancing the flexibility and security of the new systems (Anthpoulos, 2015; Scholl & AlAwadhi, 2016; Vucina & Fabac, 2017).

Spalevic also discovered that the cybersecurity developments resulted in a number of phenomena, such as "Cyber Warfare" (p. 691). She argued that such kinds of phenomena require a complex and multidisciplinary approach; to be able to implement new cybersecurity strategies, specific technics and legislations are required. She added that new regulations and strategy should be applied worldwide, with an agreement on one international law, to be able to build a unified strategy to establish democratic policies of cybersecurity "legal change".

Kouroush Jenab and Saeid Moslehpour (2016) conducted a study on cybersecurity management, the two researchers defined cyber-attacks as "…deliberate exploitation of computer systems, technology-dependent enterprises and networks" (p. 16). They suggested that cybersecurity is hard to achieve in this constant changing cyberspace of "environmental change"; because the internet infrastructure was built to serve indorse connectivity not security in the first place. Their study focused on the literature review about cyber-attacks and identified the existence of gap in the literature. They agreed with the notion of internet vulnerability to risk and the crucial need for up-to-date programs to secure the virtual space and to absorb the constant change. The two researchers divided attacks into four cases: 1- Man-in-the-browser attacks; 2- Man-in-the-Middle attacks in wireless LAN; 3- MitM attacks in wireless LAN; and 4- Fake-states attacks (p. 30).

A study conducted in the USA by Kenning Arlitsch and Adam Edelman (2014), suggested solutions of how to stay safe from cyber-attacks and how to have the ability to adapt to change. The researchers wrote an article for both public and private organizations, providing them with the right cybersecurity techniques to prevent attacks from happening and to be more flexible to change. The study pointed out the new issue of cloud-based purchase systems, which could expose credit card information to a greater amount of potential risk. The researchers added that many problems of cybersecurity came from this fundamental change in e-purchase and e-payment security and could be solved simply by passwords, or many of them with unique digits, individuals can make it harder for burglars to reach their personal information. In addition, the responsibility of organizations lies beneath knowing where to keep and store information, besides designing a secured work flow to protect their data from thieves and criminal acts (Yaich, 2016; Kantur & Iseri-Say, 2015; Newnham & Crask, 2015).

This thesis raised the issue of forces of change in the national security in the UAE which is being violated by cyber-attackers for 'political change'. The UAE is concerned about its national security, especially after the latest terrorist attacks in 2010, Sheikh Saif bin Zayed Al Nahyan the Prime Minister of Interior declared in 2013 that the UAE will never stop punishing anyone who attempts to harm the national security of the UAE. The gap in the literature appears in the shortage of studies and cases concerning cybersecurity in the Middle East governments. Furthermore, in most cases the issue of cyber-attacks is highlighted without establishing a scientific, strategic and appropriate method for information infrastructure to solve it; where most studies talk more about technical IT techniques which have proven insufficient for such cases over the last few decades. Moreover, when addressing the issue of cybersecurity, strategies have been developed theoretically but not practically, meaning, how organizations and employees can benefit from the above strategies in the work arena, and why there are not enough frameworks on this topic. Of course, the subject of cybersecurity is relatively new but more studies should be conducted with practical frameworks (North et al., 2016).

As mentioned in the introduction the notion of privacy and transparency is understood differently among public and governments around the world. The NSA had an agreement with Google to reveal part (if not all) of an individual's information to the NSA staff as the above article suggested (p. 54). Thousands and thousands of accounts dealing with customers send their data every six months to the US government (Ackerman & Rushe, 2014). This action by the US government could be considered an invasion of privacy. As such, why the privacy definition could conflict with the notion of cybersecurity and can be perceived differently by both public and government entities (Bodeau & Graubart, 2011; Sonnet, 2016; Leveson, 2002).

Again in 2016, Nastasiu conducted research on cybersecurity strategies, and suggested a new definition of cyber-warfare as 'social and political change', where the government should be in a status of war, meaning to employ all its human and material resources just like in classic war to help accept the change and to protect its electronic systems from hijackers. The researcher discussed two strategies for cybersecurity: the NATO strategy and Romania's strategy. Cybersecurity forms an enormous threat when political intensions or national security matters are involved. As mentioned earlier, the federal and governmental documentation tends to classify confidentiality sensitivity unlike other information (read more in the introduction section).

In the case of cybersecurity, Chesley and Amitrano (2015) analysed changes that came from 'technological breakthroughs' and argued that no business is safe or immune against them. The best way to look at the change is to anticipate the opportunities and risks out there, but not only to predict the potential risk, but to also be flexible in detecting both opportunities and risks and reacting to them (p. 6).

The growing online business and the emerging infrastructure in the 'business environmental change' context mean that Smart Government projects should have the passion to innovate not only for the sake of trendy government styles around the world, but also to leverage the experience of users, employees and publics at the same level. That cannot be achieved with the technology disruptions and cyber-attacks which compromise the safety of the private information of both users and clients (Blowers et al., 2016).

Organizations should be much more susceptible to the risk arena and the disruptions and unexcepted change that come from technological systems inside a firm. Continuity planners should share information with teams within the organization to make sure that the executive plans and

actionable programs are functioning correctly and heading towards achieving the overarching goal of their organization and fulfilling the needs of its system users (Jenab & Moslehpour, 2016).

In the case of cybersecurity, continuity plans focus on the impact of these forces of change factors on resilience. Olson and Anderson (2016) gave an example of that: the storage of team members, the outage of the facility, the outage of the application and outage of the vendor. The approach of the two researchers aids in ensuring the appropriate response is in place, no matter what the disruption cause was. Furthermore, this approach is important especially in the case of cybersecurity, to enable the critical functionality of online processes to continue working and flowing even with the existence of a cyber-attack without being stopped or disrupted or affected by sudden change (Chesley & Amitrano, 2015).

Olson and Anderson (2016) argued that in the case of technology disruptions such as cybersecurity in our research case, the organization should be increasingly prepared for this risk or interruptive events, such as disruptive events and cyber-attacks. They added that the resiliency scoring has proven to serve successfully the 'Target' team and to create much more educated managers and increasingly more engaged planners and "revitalized business continuity plans" (p. 43).

When analysing the impact of change on any business, the organization should identify the right teams for documenting the continuity plans, especially for the processes that are most critical in their organization, such as online processes. Nevertheless, each plan for their critical processes should have a planner and a person who wrote down this plan in the first place, both cannot be replaceable because the owner of the plan will know better and the planner will know how to plan in a scientific and systematic way. Both the planner and the owner of the plan should be part of an annual process which consists of a lifecycle that will aid in documenting the plan content,

validating its viability by exercising and helping mature the plan depending on the identified gaps that have been found during this process (Spalevic, 2014). According to Brecht (2015), change is unavoidable which is why the researcher called it forces of change; it is unavoidable in the existing market and the public or organizations will suffer sustainability and business continuity crisis.

3.4. Cybernetic Resilience

Cyber resilience is a newly developed discipline that helps organizations manage their cybersecurity problems that are not easily managed by traditional methods of cybersecurity. Organizations need to develop and implement a resilience approach of cybersecurity rather than only depending on cybersecurity controls (Christou, 2016). Resilience can be defined by the system's ability to adapt, to cope with, and to recover from issues and disturbances. There is a difference between the concepts of resilience and cybersecurity. The purpose of the cybersecurity is to keep computer systems and information safe by restricting access to data and managing the risk. On the other hand, resilience is the capacity of the system to continue performing effectively despite issues in the cyber environment (Chandler, 2014).

Within different policy topics, resilience has been described as the solution to rapid change, unexpected events, and complexity. Resilience has been a major policy topic that has focused on different issues. Resilience has developed across different disciplines as a universal mode of considering the relationship between some unexpected subjects and their highly complex environment, such as Smart Government. Due to the close relationship between resilience and uncertainty, its familiarity is shown in both the security and the international relations fields of research. A longstanding issue in security practices is the complex environment that makes it unable to identify, foresee and resolve the issues and threats in real time. Resilience gives answer

to all these problems and provides the basis for dealing with uncertainty. Resilience offers help in understanding the society as a whole system with its changing relations and changing environment. Thus, the rise of resilience shows a significant change from predictable to highly contingent.

As compared to risk analytics that focus on prevention risks and prepare for disruptive future, resilience combines present with future, and deals with insecurity and risks. The fast development of the resilience concept in different disciplines requires an in-depth analysis of the outcomes that its practices have offered for secure governance. The majority of the studies conducted in the area of cyber resilience consider technical aspects as important; however, some of the research studies focus on cyber resilience with perspectives of organizational setting. In fact, cyber resilience includes both organizational and technical aspects (Bagheri & Ridely, 2017). According to Stolfo et al. (2008), most cyber problems arise due to human error rather than any technical issues. Thus, the main reason of risks in information security is human error in cyber resilience. Thus, the organizational aspects of resilience can cause issues in business environment if businesses are not aware that organizational factors can impact their cyber resiliency (Cavelty et al., 2015).

The process of facing the cyber-attack involves different steps that have been highlighted in research studies. According to Cardenas et al. (n. d) there are three key challenges for cybersecurity of physical systems. First, understanding the threats and the outcomes of cyber-attacks. Second, identification of the properties of cyber systems and their traditional security systems. Third, discussion of the security mechanisms that can be applied to cyber systems. The researchers particularly focused on the detection, prevention, resilience, recovery and deterrence of the attacks.

In today's cyber environment, keeping pace is a necessity, but there are increased intrusions as attackers find new ways to breach cybersecurity systems. Once attackers breach the cybersecurity, the cybersecurity system must respond quickly in order to lower the scales of the threat to the organization, to minimize the effect on operations, and to make the organization learn from the security breach. In other words, organizations need to build resilience in order to face the issue of cybersecurity. The organizations must assess their ability across three major areas:

- Positive network control
- Reducing the consequences of attack, scale of threat, and breach
- Compiling relevant data to know the methods that effect the system, and the ways to avoid security breaches in future (CISCO, 2011).

There are a number of factors that contribute to the issue of cybersecurity:

- Increased internet usage
- Increased vulnerability of intangible assets of corporations, and
- Extensive use of cloud services, mobile and social media that has increased exposure of corporations to outside systems. Thus, the risks of cybersecurity have increased significantly

Attackers are aware of these factors. Businesses and government systems are more vulnerable. Moreover, as there is improvement in cyber defence, attackers find new softer targets. There are a number of actions that governments take to resolve the issues. Governments now see cybersecurity and resilience as an important part of their national security, particularly the security of critical infrastructure. There have been a number of regulations introduced to impose standards in order to ensure resilience (North et al., 2016).

3.4.1. European Union Agency for Network and Information Security Standards (ENISA)

The ENISA has developed a framework based on appropriate metrics. It has identified different principles that are important during the process of creation and implementation of a program that is created with the purpose of cyber resilience. These metrics are required to have some technical aspects, such as being quantifiable, comparable, and repeatable. Good metrics are also required to have some non-technical aspects and should be relevant to the organizational mission, easily obtainable, and work for the improvement of resilience (ENISA, 2011).

3.4.2. Local Government Research Center Framework

The Bloustein Local Government Research Center at Rutgers University published a paper in 2015 with title "Managing Technology Risks through Technological Proficiency". The research explained risks that initiate from the actions taken by people, failure of a technical system, an operational process, or management, as well as, disruptions caused by outside events. These risks are explained with six interrelated concepts: operational, cybersecurity, legal, reputational, financial, and societal. The research presented a framework that offers organizations to tackle risk with their technical proficiency. The main focus of the framework is on achievement of technological proficiency by creating and implementing four basic practices: planning, governance, cyber hygiene, and technical competence (Keys et al., 2016).

3.4.3. National Institute of Standards and Technology's (NIST) Framework

The NIST published a framework in 2014 with the purpose of improving critical infrastructure cybersecurity. The main focus of the framework is on utilizing business process of an organization to guide the activities related to cybersecurity, and to make cybersecurity internal to the risk management process of an organization. The main goal of the NIST framework is to

protect civil liberties. However, the framework is not a 'one size fit all' answer to security issues. As it was prepared, while taking critical infrastructure into consideration, one can use them in different scenarios (National Institute of Standards and Technology, 2017).

3.4.4. Network Centric Warfare (NCW) Framework

Warfare and disaster resilience have the characteristics of complexity, surprise, necessity of adoption, and urgency. Military scholars have developed a Network Centric Warfare framework that creates awareness and creates decentralized decision-making as it distributes information across various networks that operate in different domains of information, cognitive, physical, and social. These domains are as follows:

- **Information –** manipulation, creation, and storage of data
- **Physical –** facilities, sensors, system states, equipment, and capabilities
- **Cognitive** – mental models, understanding, biases, preconceptions, and values
- **Social** – collaboration, interaction, and self-synchronization among entities and individuals (Linkov et al., 2013).

3.4.5. National Academy of Science (NAS) Framework

Cyber resilience is not only the concern of IT departments, but it has become highly important in today's hyper connected world. Cyber resilience is not only about cybersecurity, but it includes business practices and has the ability to absorb cyber-attacks, recover from those attacks, and restore the operations of an organization quickly (Bagheri & Ridely, 2017).

3.4.6. Linkov Framework

Linkov et al. (2013) combined the definition of disaster resilience by the National Academy of Sciences (NAS) with the Network-Centric Warfare (NCW) framework that explains operational domains of information, cognitive, physical, and social to develop resilience metrics. There are four categories of resilience as explained by NAS: prepare, absorb, recover, and adapt. The NCW framework explains four operational domains as physical, information, cognitive, and social. Linkov created a matrix by combining the NAS and NCW frameworks. The framework estimates a system's ability to handle cyber-attacks, and provides metrics for resilience assessment. All metrics in the framework are interrelated and have implications on other metrics.

The Linkov framework for cyber resilience has been used by several researchers to find solutions to the issue. As businesses and federal government depend on cyber infrastructure for their functions, their vulnerability is extremely high to cyber-attacks by hackers, which can damage the whole organization. Therefore, regulatory authorities require attention on increased infrastructure resilience. An example of such an initiative is by the US President Obama who issued policy directives and executive orders in order to improve security and resilience of cyber infrastructure against cyber threats. Although, resilience has been considered important at national and international levels, resilience metrics to guide the decisions of managers are in the early development stage. There is a need to build an effective metric for cyber resilience. The metrics make a connection between specific system measures and the policy goals (Linkov, 2013b).

3.4.7. Operational Security – Internet of Things (IoT)

As more and more devices are network connected, attackers have more opportunities to damage them through a cyber-attack. Hackers can take control of these devices due to their

software vulnerability. For example, the linkage of medical devices with smartphones can help hackers to interfere. Thus, operational security or protection of the Internet of Things (IoT) is important. For example, Barcelona has planned to connect people with the internet to smart parking, waste management, and bus services. This highlights the maintenance and security challenges too. The increased automation and networking of power plants has created challenges as well for system security and safety in the event of updating the software (Blowers et al., 2016).

The frameworks discussed above have not mentioned the IoT that can enable technologies to sense and communicate with their external environment or internal states. However, most of the components of the NIST and Linkov frameworks address most security issues related to operational security. The vulnerability of technologies revolves around the interaction among different systems. Data protection and coordination with the external environment are the main focus of operational security. There is little research on operational security; however, there is a need to view best practices for internet technology through a different lens with the purpose of applying it to the IoT (Gartner, n. d).

After reviewing different standards and frameworks created by several government organizations, Keys et al. (2016) adapted a framework that can measure cyber resilience in different sectors and industries. The framework is mainly based on the Linkov and NIST frameworks for improving critical infrastructure cybersecurity because the Linkov framework addressed the concern that most risk based assessments combine resilience and risk. Thus, Keys, et al., decided to choose the Linkov framework as it addresses the components required for resilience. However, as the Linkov framework does not address the actions related to threat detection to the same degree

as the NIST framework, there was a need to combine both frameworks and to create a unique framework. The framework introduced by Keys et al., (2016) has the following categories:

- **Plan and Prepare:** This category is the basis for keeping services running and available, as well as, continuing assets functioning if there is cyber-attack.
- **Detect:** This category is about quick recognition of cyber-attacks and starting the use of containment procedures.
- **Absorb:** This category involves the continuity of functions during the attack, and to isolate the cyber-attack.
- **Recover:** This category involves bringing all services and functions back to the pre-attack state.
- **Adapt:** This category requires the use of experience and knowledge gained after cyber-attack to make the organization more resilient.

The writers also used physical, cognitive, information, and social aspects in the framework, which are explained below:

- **Physical:** The physical domain is about design, capabilities, and physical resources
- **Cognitive:** The cognitive domain is about the use of information
- **Information:** The domain of information is aimed to make decisions with that information.
- **Social:** The purpose of the physical domain is to communicate for cognitive decision-making.

All categories in the framework have specific components that are used to estimate the cyber resilience of the organization. In addition to all the above frameworks, researchers continuously struggle to improve cybersecurity models. For instance, Cavelty et al. (2015) stated

that diverse and contradictory practices of resilience have been introduced in different security policies. However, there is need to critically examine those practices, and how different forms of resilience create subjects, change environment, redefine security and insecurity relations, and link temporalities. The researchers highlighted the increased political and scholarly attention given to resilience that has been given in recent times. They argued that resilience should be investigated and conceptualized in plural terms.

3.5. Cybernetic Resilience in the UAE (Dubai Smart Government)

According to Bosen (2017) government in the UAE is taking a pro-active response to the safety of the country's digital infrastructure. The approach of the government is to safeguard the features of digital infrastructure from harm. The network helps in data exchange among government and local entities. The cybersecurity initiative of the UAE government follows the introduction of the cybersecurity strategy in Dubai with the purpose of strengthening the position of the country as a global leader in safety, innovation, and management of cybersecurity risks. The main focus of the strategy is on the domains of being a cyber smart nation, ensuring society's development, innovation, cyberspace security, and cyber resilience.

The government of the UAE is focusing on cyber resilience in order to avoid threats in the changing cyber environment. His Highness Sheikh Mohammed bin Rashid Al Maktoum has recently launched the Dubai Cyber Security Strategy in order to strengthen the position of Dubai as a global leader in safety, innovation and security. The following figure shows the cybersecurity strategy of Dubai that includes cyber resilience as an important element.

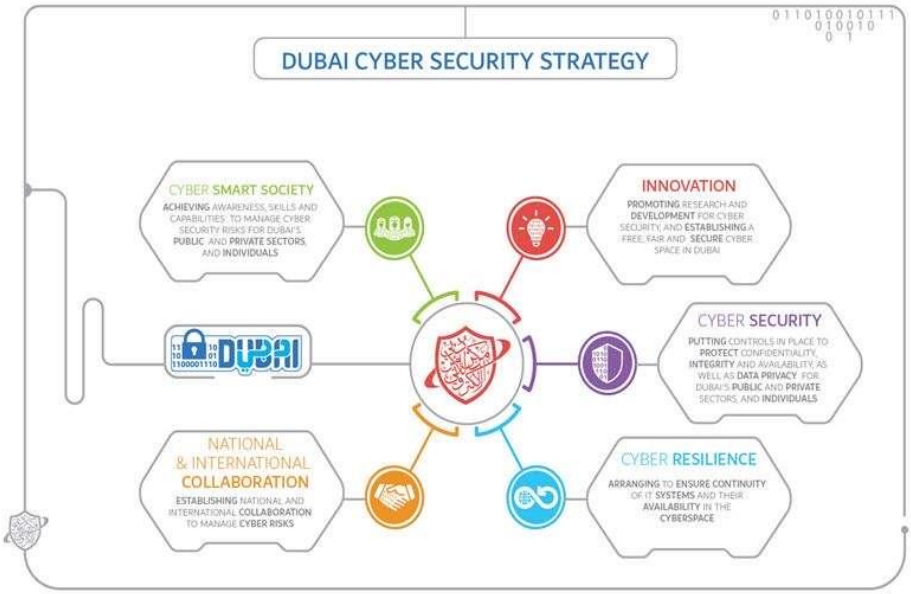

Figure 3.4: The Dubai Cyber Security Strategy

The Dubai Cyber Security Strategy includes the following domains:

- **Cyber Smart Nation:** The domain has the purpose to increase awareness among people about cybersecurity to ensure building a society that understands the threats related to cybercrime, and learns the skills that are important to manage risks related to cybersecurity among private and government institutions.
- **Innovation:** The domain of innovation is about scientific research and innovation in the field of electronic security and development of cyberspace to encourage innovation in the country.
- **Cyber Resilience:** The domain of resilience focuses on flexibility in cyberspace and ensuring the availability of IT systems if there is a cyber-attack. It also aims to build a platform to exchange information and support in managing incidents of a breach of cybersecurity.

- **Cybersecurity:** The purpose of cybersecurity domain is to build control for making cyberspace secure (Emirates 24/7 News, 2017).

3.6. A Conclusive Cybernetic Resilience Framework

After everything that has been said about the cybernetic resilience theories and frameworks, the researcher reached a conclusive framework for this research. This framework reflects the importance of the notion of cybersecurity and the purpose behind it in any organization that shares similar features with Smart Government. By highlighting the main elements of the framework and its functions, any organization that conducts most of its business processes online using IT tools, can definitely benefit from it. Furthermore, this conclusive framework of cybernetic resilience presents the main criteria of how to implement it in an organization besides highlighting the main elements that should be considered and employed by the organization to further build its cybernetic resilience system.

Cyber-attack cases are now one of the main problems for the governments of different countries all over the world. In many cases breaches came from within the organizational staff, which tells us why such organizations are in need for a framework that will help secure work processes within the organization boundaries, which appear to be not safe. Unfortunately, most risks and threats are hidden within the boundaries of the organization itself. A survey conducted in 2006 entitled "Information Security Breaches", and conducted by the DTI and PricewaterhouseCoopers found that approximately 32% of cyber-attacks are performed by internal staff, whereas only 28% of cyber-attacks are performed by external staff, such as stakeholders and external clients or attackers (Patel, 2006). They are called 'third party' and they form a serious risk to any system (Hyslop, 2016). Thus, cyber-risk appears not only from the staff within who have an

access but also outside the government where anyone can have bad intentions to commit a breach of the system.

According to UAE experts, by 2021, the total cost of global cybercrimes will reach $6 trillion compared to $1.2 trillion back in 2017. The Smart Government websites and projects increase the global interconnectedness of business, and the global industry sector is most vulnerable to cyberattacks. The hybrid motive of attackers concerns their faster adaptability and dynamic movement towards technologies than the industry itself. Cybercriminals compromise the security system of smart business organizations for various reasons. Generally, the motive of an attacker is to gain financially by compromising the security posture of a firm. However, there are occasions when they have multiple motives and intensions, such as ideological, financial, or political motives. The organizations need to ensure that they devise functional resilience of cybersecurity, which can help the firm to regain their composure quickly and efficiently.

Nowadays, one cannot separate the business arena from the IT domain; the way business owners and employees are interacting with stakeholders and partners is changed forever. On the other hand, this change has brought a lot of disruptions, such as cyber-attacks which can not only damage the business of an organization but can also be fatal and lead to its own demise. The need for such cybernetic resilience systems have arisen since the business and IT has emerged.

The changing environment brought to the UAE due to smart projects became a problem, along with the growing demands of the enlarged population. In light of all that, the government finds itself obligated to find sustainability, flexibility, resiliency and agile plans, with the right potential and abilities to improve the UAE's infrastructure with longer-term standards of quality

for its people (AlMatroushi, 2017). In order to achieve all the above, the UAE needs a professional framework that will help it fulfil its goals in a safe way, fearless of staying behind due to the extensive changes taking place in the arena, as well as threats and cyber problems.

The conclusive cyber resilience framework identifies the cyber resiliencies' goals along with the main elements and threats, besides presenting measurements and responses. It aims at: 1) maintaining the state of preparedness, which will protect all the system's functions and missions from adverse effects; 2) proceeding and continuing with core mission, even with the existence of cyber-attacks on the system; 3) increasing the ability to restore the business functionality post cyber-attacks; and 4) increasing the ability to change some missions and functions (Bodeau & Graubart, 2011), in order for the organization to reduce adverse effects. The framework is presented below as a conceptual framework for cybernetic resilience.

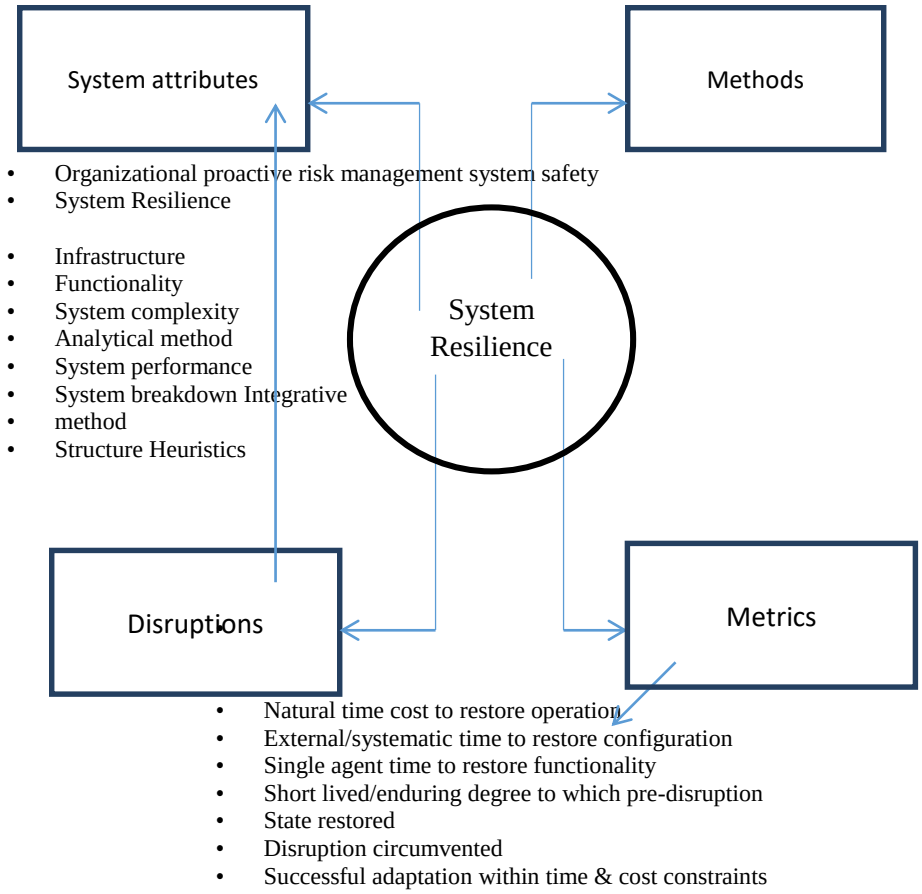

Figure 3.5: A Conclusive Framework

The above framework consists of four pillars:

1) **System attributes** which consists of the characteristics of the system such as complexity along with performance and the system structure's breakdown. All the mentioned characteristics are affected by the disruptions, which is why a resilience framework should be employed depending on the disruption's type and nature.
2) **Disruptions** come in different types, such as systematic disruptions, external ones, single-agent and multi-agents, besides the kinds that are caused by nature or are man-made. Last but not least there are also transient or enduring disruptions.

3) **Methods** which consist of the traditional risk assessments and safety methods that are integrative, utility-costs-trade-offs, risk management plan (which is proactive), and expert inputs or historical inputs deriving heuristics on the on-going basis. Every organization should provide effective trade-offs (Klein, 1998) to maintain resilience.
4) **Metrics** represent the most important element in the resilience framework; where metrics and indicators developments help achieve resilience by alerting the management about some contradictions and conflicts between 1) the production and its pressure, and 2) safety issues and needs. Nevertheless, resilience perceives safety and risks of the system with a systematic perspective, rather than casual framework or model. These metrics can explain how some disruptions happen suddenly and shows the insights of trade-off space by testing resilience indicators of the organization (Leveson, 2002).

Whereas the key indicators of the resilience proactively produce safety to the organization system, some additional roles and insights are needed in the dynamic area of resilience which comes with some cost; therefore, resilience should only be implemented when needed.

Moreover, it is important to employ and implement resilience in organizational processes. These essential points are related to the managerial, political and operational perspectives. That is the reason behind the need for more research and more instruments to derive the system of any organization away from disruptions and unforeseen events, which can lead to its functional failure.

The conclusive framework includes a matrix, technologies, methods and procedures that are developed to protect organizations and individuals from cyber criminals and villains (Nastasiu, 2016). The organization that suffers from cyber-attacks faces many problems, such as loss of

reputation, assets, and business and also faces many fines and lawsuits. According to the 2017 survey of the UK government, for a large business the cost of the average cybersecurity breach is £19,600. However, the average cost for small businesses is £1,570. To cope with cyber-attacks cyber resilience is very important (IT Governance, 2017).

The conclusive framework (figure 3.5) can help to design an integrated and holistic cyber security resilience that will allow the business organization to be empowered against online attackers and criminals. Nevertheless, the hacking industry is a very attractive one due to its immediate, fast and direct financial gains. Therefore, Smart Government must invest in advanced resilient systems to have full immunity against attacks, rather than just reacting to these cyber risks. David Young, declared that the period post-Expo 2020 will be a huge jump for the UAE in particular and the region in general. He said “The Expo 2020 will attract new businesses, talent, new industries and investments to the country”. He added that the UAE will gain benefits in a short-term and long-term from the Expo 2020 this year and in the years to come. This is why cyber resilience plans should be worked on from now, to avoid any disruptive event that might occur on the inauguration night of Expo 2020 by the country’s enemies (Khaleejtimes.com, 23 January 2020).

3.7. Discussion on The Related Theories

Chuong and Tran (2019), in their research study, stated that game theory can be used to obtain a thorough insight into cybersecurity, privacy, and resilience of cybersecurity. The authors used numerical results to showcase how the prediction of the expected motive of a cyber attacker

is possible by using game theory. The quantitative theory was implemented in this research framework to expand the survival lifetime in an unpredictable digital setting.

In Resilience Theory, according to John (1994), that resilience is based on the ability to recover after the disaster by adopting relevant strategies and approaches. This theory has been used by a number of authors such as Linkov (2013) and Kerr (2016) to reflect the fact that a resilient organization is its ability to absorb change, not only risk, good or bad change can form some kind of a risk towards an organization. This theory is used in this research to determine the components of the resilience framework that will upgrade the level of sophistication in dealing with unforeseen events, to be able to regain composure after a cyber incident.

Infrastructure Theory is based on analysing and evaluating the location, environment, and limitations in the design, and the network security. This research has used it in addressing vulnerability of the Smart Government project, due to the greater risk is in the entity of the smart infrastructure of Smart Government. Linkov's (2013) framework has been cited as being used in most organizations. As organizations and federal government entities depend on cyber infrastructure for their functions, their vulnerability to cyber-attacks is high wherein hackers can damage the whole organization. Therefore, regulatory authorities need to pay attention to increased infrastructure resilience.

The Smart Governance theory is based on enhancing the use of techniques and approaches to smartly analyse and overcome potential risks and challenges. According Holtz (2002) we are living in a cyberspace nowadays, and the integrated governance has integrated the whole universe in one place like a small village. When it reaches the political and government level, things get more

serious. The documentation and the files of the government tend to be more sensitive and need more protection. Such data contains a higher level of confidentiality and demands a smarter approach to protect its system and make it more immune to cyber-crimes (Pennauther, 2001).

The Ontology Theory is a philosophical theory that was used in this research to determine the relationship between the dependant variable (resilience of Smart Government) and independent variables of this study (vulnerabilities, capabilities, management control and forces of change). This theory has been used by a lot of authors, such as Onwuldike, Lock and Phillips (2015), who used it in measuring the resilience of Smart Government.

The Disaster Prevention and Mitigation Theory is based on identifying the risks and managing the processes on the basis of preventing disasters so that risk mitigation strategies can be implemented effectively. Resilience processes in this research consist of several moving parts of cyber resilience that should be approached methodologically. There are five interconnected domains of cyber resilience processes, and each of those domains has a different function. The domains are identified, protect, detect, respond, and recover. Barrinha (2016) used this theory in her study about risk mitigation and the need for resilience frameworks.

The resilience in dynamic systems helps in evaluating the risks and challenges involved at multiple levels. The converge model of resilience is grounded in the concept of relational developmental system theory. It is important for the Smart Government to maintain its capacity for competence considering the involved possibilities. Resilience can be characterized as adversity and competence. Adversity presents the negative experiences that create challenges and difficulties in

carrying out the functions. Competence refers to the capacity to adapt and meet the development and cultural expectations. It enables the government to adapt systems according to the need.

The resilience-informed practices are based on fostering the positive adoption and development while considering the high risks and adversity. The concept of resilience has its roots in the field of psychology, which refers to the ability and capability of an individual to withstand the stress and recover from traumatic events. The same resilience is required by a Smart Government so that it can bounce back after disasters and threats by managing the disasters efficiently.

The Contingency Theory was used by Kerr (2016). This theory suggests that a Smart Government can focus on the changing environment to enhance its connectedness with local and international people in the UAE. The in-depth discussion of the cybersecurity skills and cyber threat mitigation and risks can help in the implementation of penetration strategies, which can help in dealing with the emerging risks and opportunities.

3.8. Conclusion

Cyber resilience can be defined as the measure of how effectively an organization can carry out its business operations during a cyber-attack or a data breach incident. Resilience is the desired outcome for managing operational risks that might arise from cybersecurity threats. When the actual crisis arises before a business undertaking, it should be in a position to ensure that the core business functions, processes, and protocols will not be affected. In order to make sure that robust resilience of cybersecurity is in place, it is necessary to measure the cyber resilience. According to Campbell et al., a wide range of resilience metrics can help to conduct a thorough and in-depth analysis of the system behaviour (Campbell et al., 2019).

Some of the security metrics that have been identified by the authors include the assessment of how well systems can offer vital security functions such as identify, protect, detect, respond and recovery and evaluation of how well a system is capable of meeting the core security objectives relating to confidentiality, availability, integrity, and accountability. The risk metrics include the assessment of the likelihood of adverse attack situations and the evaluation of the consequence severity. The resilience metrics include the assessment of the level of performance before, during, and after the detected disruption and the assessment of the time that exists between the distribution stage, detection, response stage, and ultimate recovery.

The association that exists between cyber resilience metrics and cyber resiliency can be understood by using the Cyber Resiliency Engineering Framework (CREF). CREF basically defines the 'what' of cyber resiliency in terms of the goals and objectives. The proper measurement of resilience of cybersecurity is of vital importance as it can help to prevent or curtail the adverse implications that might arise in the organizational setting due to high levels of uncertainty in the cyber context (Hirani, Lasiuk & Hegadoren, 2016). Some of the principal risks that might arise before a business undertaking include the loss of intellectual property, loss of operational capability of the business organization, and the loss of regulatory controlled data. While working in a highly dynamic and unpredictable business environment, it is necessary for business entities to carefully measure the cyber resilience so that its effectiveness can be ascertained in an accurate manner. Thus, measuring cyber resilience has become an extremely critical indicator that can help a business entity to survive and sustain in the dynamic business environment. The proper measurement of resilience of cybersecurity is also necessary as it can help the organization to have a competitive longevity in the dynamic setting.

After developing the theoretical framework of the resilience, the researcher concluded that by focusing on the importance of the resilience, building safe systems that can anticipate then prevent any risk of disruptions is possible only by learning, practicing and adapting. Furthermore, the system can go into fast-recovery status and return to its normal functionality in the pre-attack state. The main element of this theoretical framework is agile and 'holistic practice' to maintain resilience and help in a fast-recovery process and reduce the level of vulnerability in the organization's systems, such as Smart Government systems.

Within different policy topics, resilience has been described as the solution to rapid change, unexpected events, and complexity. Resilience has been a major policy topic that has focused on different issues. Resilience has developed across different disciplines as a universal mode of considering the relationship between some unexpected subjects and their highly complex environment. Due to the close relationship between resilience and uncertainty, its familiarity is shown in the fields of international relations and security studies. A longstanding issue in security practices is the complex environment that makes it unable to identify, foresee and resolve the issues and threats in time. Resilience gives answers to all these problems and provides the basis for dealing with uncertainty. Resilience offers help in understanding the society as a whole system that has changing relations and exists in a changing environment. Thus, the rise of resilience shows a significant change from predictable to highly contingent.

There are a number of factors that contribute to the issue of cybersecurity: increased internet usage, increased vulnerability of intangible assets of corporations, and extensive use of cloud services, mobile and social media that has increased exposure of corporations to outside systems. Thus, the risks of cybersecurity have increased significantly. The UAE federal

government is aware of the importance of cybersecurity and resilience. People in the country are using smartphones to access their online banks, manage investments, transfer funds, carry out vehicle registration, book travel and apply for National IDs. However, this increased connectivity has increased the risks in the country due to the vulnerability of the cyber system. The government of the country has recently introduced its cybersecurity strategy which includes resilience as an important part of the strategy.

In conclusion, the network connected devices, and the internet population has increased dependence on networks. However, the government and private organizations need to address the challenge of breaches in cybersecurity. In order to keep pace with the changing environment, organizations need to learn the appropriate use of the network in order to gain visibility, achieve trust, and provide resiliency to the system. In order to ensure resilience and cybersecurity, public and private organizations need to develop their abilities of resilience through internal structures, and work with external organizations, in order to ensure system resilience.

CHAPTER FOUR: RESEARCH METHODOLOGY

The research strategy is a critical piece of an examination as it encourages the specialists to embrace an orderly and hypothetical frameset of methodologies, models, speculations, strategies, and investigation techniques to direct the exploration as indicated by its key prerequisites. This section is centred on illustrating definite research systems that consider the idea of the examination and shape understanding (Kothari, 2004). It has explored different research strategies and methods to understanding their productivity in various circumstances. The assessment has helped the investigation to receive the best accessible technique to gather and break down information. However, in order to set a focus, it has outlined the limitations and benefits of these models in order to highlight their efficiency for collecting data for the key research theme of cybersecurity and resilience (Kothari, 2004). After reviewing the literature and studying the existing frameworks that employ cybersecurity risk management to measure and achieve resilience, the researcher came up with a methodological framework that will help solve the problem of the research and will help in conducting the research in a scientific and numeric way rather than just assuming things. This framework will also help in testing the hypotheses of the research to identify accurate results in the next two chapters of the thesis (Chapter Five: The Findings and Chapter Six: The Results).

According to Esterbay-Smith, Thorpe & Jackson (2015), the techniques of business management research can differ from one researcher to another; it depends on the worldview an individual or an organization is holding, which will definitely contribute in choosing the research method. The process of the research consists of different stages as follows: 1- Defining variables, 2- Literature review, 3- Hypothesis formulation, 4- Data collection, 5- Analysis, 6- Interpretation and 7- Conclusion.

This methodology will consist of quantitative (survey) data gathering and analysis. The justification is that the relationship between cyber-security risk management and resilience was studied in the literature and the systematic review of seventy previous research articles revealed that they focused on the quantitative approach when studying these relationships. This motivates the researcher to use the same quantitative approach in the current research because of scarcity of quantitative research on resilience in cybersecurity worldwide and especially in the UAE. Relatively few research studies focused on the qualitative and mixed method approach for studying this phenomenon. As a conclusion, it is obvious that more focus is given to the quantitative approach over the qualitative and mixed methods approaches. This reinforces the rationale of going for further quantitative research for a new contextual investigation for achieving the research objectives.

As per Linkov and Kott, a broad range of quantitative and qualitative techniques can be applied to cyber resilience. The authors have stressed the quantitative theories of studying resilience, which have theoretically rigorous modelling and the simulation of networks, systems, and processes (Kwasinski, 2016). Thus, quantitative theories can be applied to study cyber resilience, which is the ability to continuously deliver the desired outcome despite adverse cyber incidents. Linkov and Kott have stated that network science is emerging as a vital tool which enables the quantitative framing for the future of cyber resilience as a scientific discipline. Network science can be defined as the studies of the complex and complicated networks like computer networks, telecommunication networks, and cognitive and semantic networks. In network science, an interconnected network of nodes and links represent the system that exhibits the behaviour in time and space. One of the key challenges that arise relates to the framing of

resilience as the characteristic of numerous major network properties that could offer a universal foundation to the cybersecurity field (Van et al., 2015).

As per Holm and Ostergaard, due to the high level of interconnectedness in the digital setting, the resilience of cybersecurity is of high importance (Holm & Ostergaard, 2015). In the research study, a quantitative, model-free and general-purpose assessment methodology has been implemented to extract resilience indexes from system logs as well as process data. In the study, a synthetic measure acts as the quantitative element that must be provided. This is because it can help to describe the extent of damage that a system can tolerate before it becomes irreversibly damaged, unstable, or exhibits probable dangerous behaviours.

Using version 16.0 of the SPSS program is considered in the statistical analysis of the survey questionnaire. The use of an independent sample in t-test and using one sample is also considered. Nevertheless, the researcher used the correlation and regression analysis method to finalize the analysing process of this thesis.

The assessment measures of this research will be as follows: 1- Demographic Information Questionnaires, 2- Cybersecurity & Privacy Questionnaire, and 3- Smart Government Resilience.

The researcher will present a methodological framework that has emerged from three frameworks: the system's maturity framework (Kerr, 2016), the cybersecurity risk management framework (Hyslop, 2016), and the resilience framework (Linkov et al., 2013). This innovative framework will help in avoiding the previous mistakes in the above frameworks and covers the main elements in a simple way to be able to measure the resilience.

The questionnaire diagram of this thesis is detailed below.

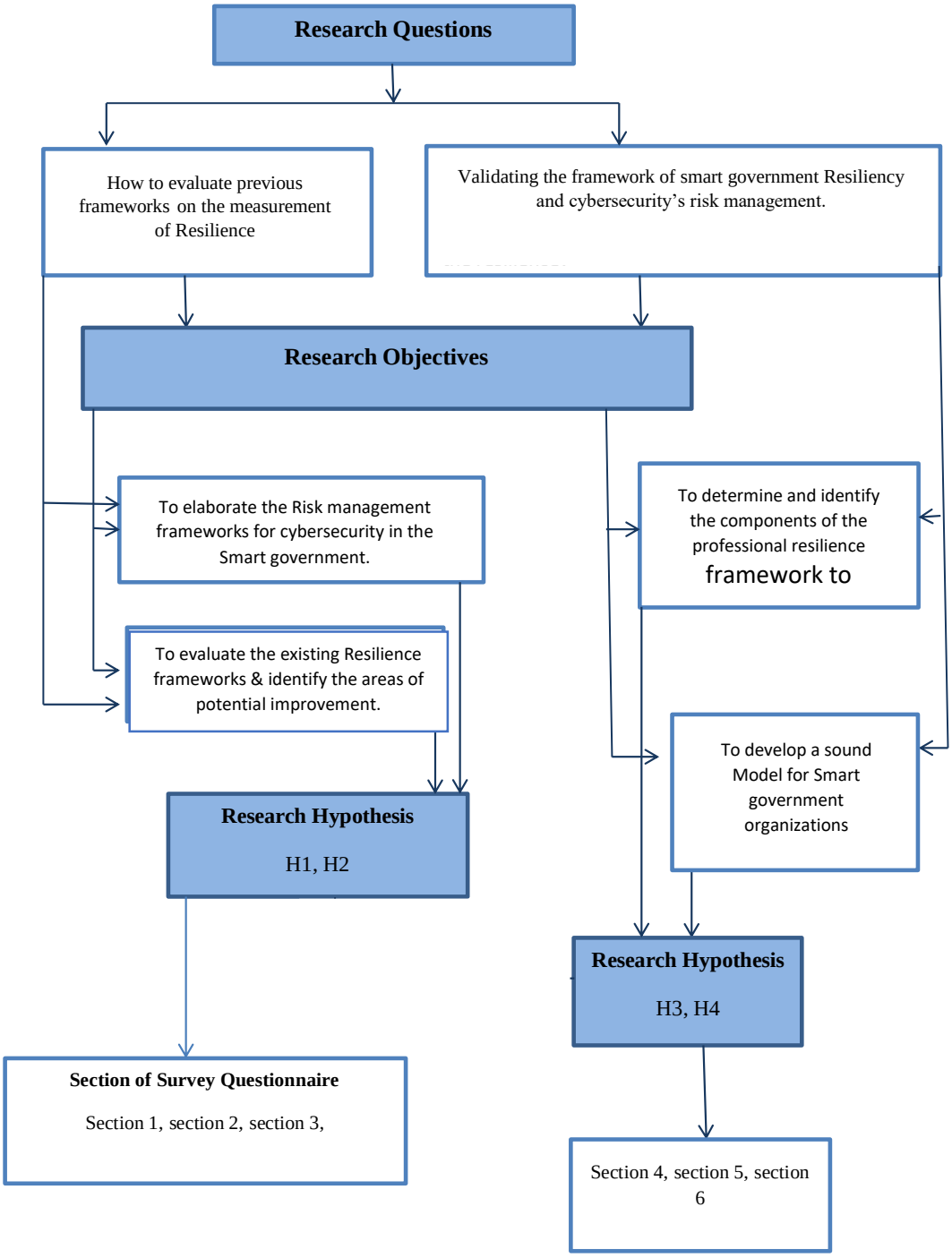

Figure 4.6: Questionnaire Design

The above (figure 4.6) shows how the questionnaire was designed. It shows how the researcher depends on the need of primary and secondary data to determine the methodology of the research.

It shows how the research questions led the objectives of the research. (Figure 4.6) shows how the sections of the questionnaire or the survey has been divided according to the Hypothesis, objectives and questions of the research. This measurement tool was designed in a systematic and accurate way. The researcher designed the questionnaires based on framework, variables, hypothesis, research questions, objectives and topic.

The process of the research:

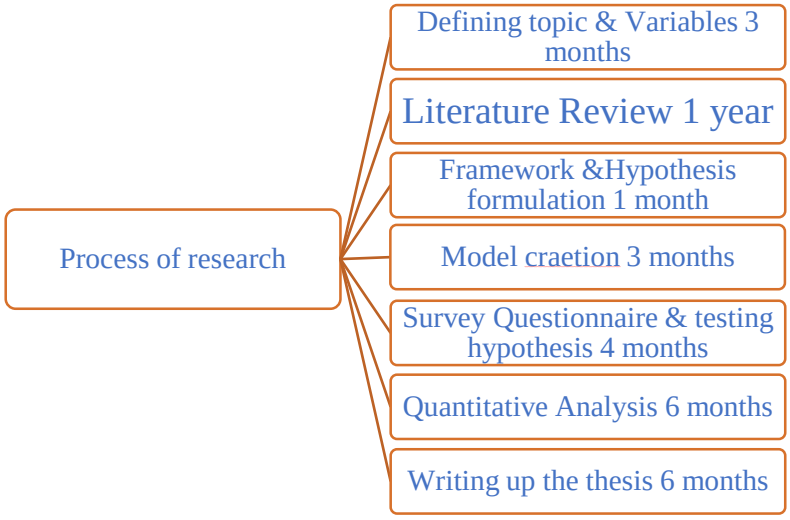

Figure 4.7: Research Process

The above (figure 4.7) explains the process of the research and shows the time consumed by the researcher to be able to accomplish this research. Starting with defining variables and choosing the topic, and ending with writing up the thesis. The whole process of the research took up to three years. In this period of time, the researcher tried to assign certain time for each task; to be able to finish on time and plan the whole process for the sake of the successful of the research.

Pilot one – reliability test:

Table 4.3: Reliability Statistics

Cronbach's Alpha	N of Items
.967	65

Table 4.4: Scale Statistics

Mean	Variance	Std. Deviation	N of Items
150.85	1650.974	40.632	65

Pilot 2 – reliability test:

Table 4.5: Reliability Statistics

Cronbach's Alpha	N of Items
.962	65

Table 4.6: Scale Statistics

Mean	Variance	Std. Deviation	N of Items
154.08	1512.447	38.890	65

The above tables show the details of the pilot study, which was conducted by the researcher to test the time reliability of the test (questionnaire). Reliability is tested by a pilot study for the items of the survey, given to the group of 15 respondents twice to test the time reliability of the test, moreover, the results revealed the stability of the responses of the same 15 respondents through time. Regarding validity and reliability of the measurement method: the researcher did theoretical

validation as well. Along with in-depth analysis of the literature in comparison with the current method is used to validate it.

4.1. Methodological framework

The justification of providing a methodological framework in this thesis is that according to the IT Governance Cyber Resilience Framework (2017), a four-part approach must be followed towards cyber resilience. These parts include ‘manage and protect’, ‘identify and detect’, ‘respond and recover’, and ‘govern and assure’. The very first element of a cyber resilience program involves the ability to identify, manage and assess the risks that are linked with information systems and networks. The second element of the cyber resilience program depends on the on-going monitoring of information systems and networks. This step is highly important as it can help to identify any potential cybersecurity incidents or anomalies. The third element relates to the implementation of a robust and functional incident response management programme and measures, which will make sure that the business undertaking will continue to function and operate even if it has been affected by a cybersecurity incident. The ultimate element of the cyber resilience programme is to make sure that it is overseen from the very top of the business organization and integrated into the business thoroughly. In fact, the resilience program must be aligned with the overall business objectives so that it can act as a safety net that will enable the organization to get back on its tracks even after it is affected by a security incident. These vital components can have a direct effect on the cybersecurity resilience that has been employed by a business entity (Schipper & Langston, 2015).

Thus, a broad range of factors exists that can have a significant impact on the resilience of cybersecurity. It is necessary to carefully consider these elements so that functional and robust cybersecurity resilience is introduced throughout the organizational setting. By taking into account these factors, firms will be empowered to combine cybersecurity and business resilience to introduce the robust resilience of cybersecurity (Sussan & Acs, 2017).

Nevertheless, cyber resilience is the ability of an organization to recover from a cyber-attack. Therefore, cyber resilience is the key element for organizational sustainability. There are several moving parts of cyber resilience that should be approached methodologically. There are five interconnected domains of the cyber resilience framework; and each of those domains has different function. The domains are identified as, protect, detect, respond, and recover.

3.8.1. Architecture of Cyber Resilience Framework

- Asset management
- Configuration and change management
- Controls management
- Incident management
- Vulnerability management
- Service continuity management
- Risk management
- External dependency management
- Situational management

The steps to achieve cyber resilience are:

- System hygiene
- Developing a plan
- Map out risk profile
- Assess and measure
- Mitigate risk
- Cyber insurance
- Get started

The resilience framework is all about detecting, preventing and recovering from a cyber-attack. Therefore, cyber resilience is the key to sustainability of an organization. The resilience framework is detailed below (figure 4.8) which is a very important part of the framework of the thesis and It's the backbone of this research; this is why it is presented again with more details.

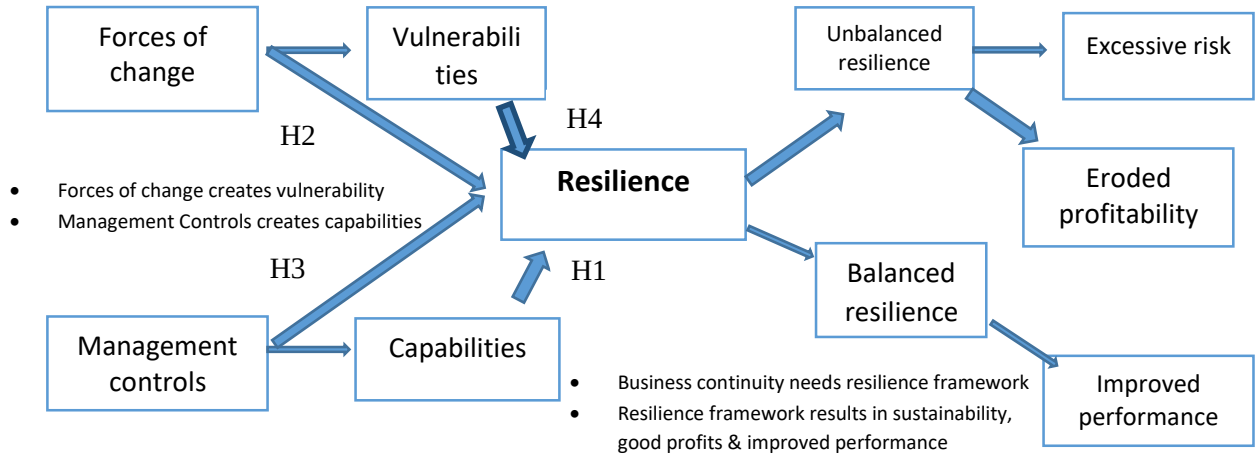

Figure 4.8: Resilience Framework

Thus, resilience is affected by the important variables of vulnerabilities, forces of change, management controls, and capabilities. Finally, resilience shows output in the form of balanced

resilience, improved performance, or unbalanced resilience and eroded profitability. The main factors of vulnerability, management control, capabilities, and forces of change have further factors that control them.

- ***Vulnerability Factors***

Vulnerability factors include turbulence, deliberate threats, external pressures, resource limits, sensitivity, connectivity, and disruption by supplier or buyer of the product/service.

- ***Capability Factors***

The key capability factors are flexibility in sourcing, capacity, flexibility of order fulfilment, efficiency, visibility, anticipation, adaptability, recovery, disruption, collaboration, organization, security, market position, and financial strength.

- ***Forces of Change***

Internal and external change in an organization, such as social change, political change, environmental change.

- ***Management Controls***

Management control creates capabilities for proper functioning and resilience against cyber-attacks. If the capabilities increase in the organization, there is less vulnerability. Thus, there is linkage between vulnerabilities and successfully used capabilities to face those vulnerabilities (Lambert & Knemeyer, 2004).

4.2. Variables

4.2.1. Dependent Variables

Resilience in Smart Government organizations.

4.2.2. Independent Variables

- Forces of Change

Internal and external change in an organization, such as social change, political change, environmental change.

- Vulnerabilities

Vulnerability factors include turbulence, deliberate threats, external pressures, resource limits, sensitivity, connectivity, and disruption by supplier or buyer of the product/service.

- Management controls

Management control creates capabilities for proper functioning and resilience against cyber-attacks.

- Capabilities

The key capability factors are flexibility in sourcing, capacity, flexibility of order fulfilment, efficiency, visibility, anticipation, adaptability, recovery, disruption, collaboration, organization, security, market position, and financial strength.

4.3 Research Hypothesis and Related Theories

The Specific Hypothesis:

H1

The capability factors affect resilience in Smart Government organizations.

H2

The change factors affect resilience in Smart Government organizations.

H3

The management control factors affect resilience in Smart Government organizations.

H4

The vulnerability factors affect resilience in Smart Government organizations.

The Related Theories:

- Resilience is based on the ability to recover after the disaster by adopting relevant strategies and approaches.

- The addressing vulnerability of the project or infrastructure theory is based on analysing and evaluating the location, environment, and limitations in the design, and the network security.

- The Smart Governance Theory is based on enhancing the use of techniques and approaches to smartly analyse and overcome the risks and challenges.

- The Disaster Prevention and Mitigation Theory is based on identifying the risks and managing the processes on the basis of preventing disaster so that risk mitigation strategies can be implemented effectively.

- Resilience can be characterized as adversity and competence. Adversity presents the negative experiences that create challenges and difficulties in carrying out the functions. Competence refers to the capacity to adapt and meet the development and cultural expectations. It enables the government to adapt systems according to the need.

- The resilience in dynamic systems helps in evaluating the risks and challenges involved at multiple levels. The convergence model of resilience is grounded in the concept of relational developmental system theory. It is important for the Smart Government to maintain its capacity for competence considering the involved possibilities.

- The resilience-informed practices are based on fostering positive adoption and development while considering the high risks and adversity.

- The concept of resilience has its roots in the field of psychology, which refers to the ability and capability of an individual to withstand stress and recover from traumatic events. The same resilience is required by the Smart Government so that it can recover after disasters and threats by managing the disasters efficiently.

- The Contingency Theory suggests that the Smart Government can focus on the changing environment to enhance its connectedness with the local and international people in the UAE.

- The in-depth discussion of the cybersecurity skills and cyber threat mitigation and risks can help in the implementation of penetration strategies, which can help in dealing with the emerging risks.

4.4 Empirical Research

Empirical research offers numerous openings, nevertheless, there are no less than two sorts of impediments: from one perspective, mistakes and traps that are specifically identified with the layered assessment approach, and, then again, inalienable constraints of empirical research when all is said and done. Clearly, empirical investigations are not a formal evidence of a reality. They rather yield, support, or reject speculations. In any case, the outcomes are constantly burdened with

vulnerability, which can frequently be communicated in a statistical likelihood sense (Saunders, Lewis & Thornhill, 2012). Furthermore, for most statistical tests certainty interims, test power, and impact sizes are accessible which ought to be accounted for too. This speculation testing strategy is in charge of a critical restriction of empirical research. Empirical investigations are great at recognizing plan blunders and off-base suspicions, yet they do not recommend new hypotheses or methodologies straightforwardly. Indeed, even an explorative think about requires a few theories about conceivable effect factors. In this way, empirical assessments must be joined with hypothetical grounds to yield helpful outcomes (Kumar & Phrommathed, 2005). The imagination confinement, however, a basic motivation behind why assessments are currently overlooked, is the way that assessments are not required for production at global meetings or then again diaries (at any rate regarding client displaying). Accordingly, the empirical element is regularly reserved for the end of a venture and often skipped because of the absence of time. On the off chance that distributers and commentators would be interested in empirical assessments it would soon be an incorporated part of research where empirical and hypothetical elements could empower each other. Furthermore, the frameworks are generally executed by PC researchers who tend to be less acquainted with empirical techniques than individuals with experience in human research collaboration (Taylor, Bogdan & DeVault, 2015).

4.5 Research Philosophy

Research philosophy can present as a conviction to choose a specific style of information to be accumulated and investigated for the examination. The term epistemology is used to fuse distinctive research rationalities to shape comprehension. Comprehensively, two kinds of essential research methods of insight incorporate positivism and interpretivism, the two fuse distinctive

perspectives to set a core interest. For instance, a positivist research philosophy is centred on the truth-based confirmation and portrays data from a specific perspective. The key spotlight on this philosophy anticipates controlling the truth-based information with varieties to decide the connection between various independent and dependent factors. While then again, an interpretive hypothesis is centred on the subjective elucidation of the gathered information as per their regular habitat, the nature of the investigation should use a positive hypothesis, with the goal that the research can attempt a reality-based situation and decide to comprehend (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007).

According to (Saunders, et al., 2007) for the most part, researchers are quick to work with a research onion (figure 4.9) to choose a reasonable and efficient amount of information to gather and break-down techniques as can be observed in the figure below.

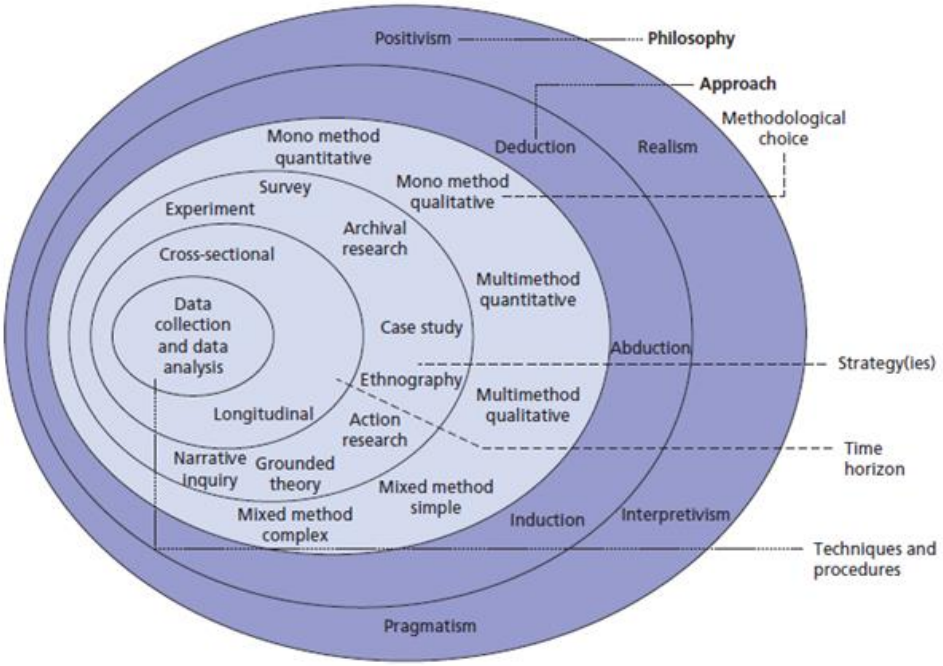

Figure 4.9: Research Onion

(Saunders, et. al, 2007)

Other philosophies in research approach comprise of realism (work with destinations independently in light of the information), and clear-mindedness (centred around both positivism and interpretivism). This approach has assumed a quantitative and mixed research approach for the investigation, it has concentrated on solid apparatuses to extricate information as indicated by the prerequisite of the examination and feature educating and learning process connected with this examination. Different methodologies are not utilized for this investigation as it may befuddle the points and targets of the research with its extricated information in restricting viewpoint.

Along these lines, with a specific end goal to keep things basic for this research, positive philosophy has been attempted to manufacture a concentration, in the meantime, gather and break down the information for this research fittingly (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007).

However, there are certain limitations of positivism that the researcher might face while creating a focused analysis of cybersecurity and resilience. Positivism trusts that target inferring and conclusions can be attained as long as the individual doing the perception is objective and goal-orientated and ignores feelings. Nevertheless, human conduct normally accompanies passionate reactions. Despite the fact that positivism urges researchers to dismiss human feelings and conduct, there is no assurance that this will happen consistently. A few researchers trust positivists think everything can be estimated and ascertained; they have a tendency to be unyielding. Positivists consider things to be as they are and tend to dismiss unexplained phenomena. Therefore, if the hypothesis A separately works until hypothesis B and C worked together, the entire hypothesis is

supposed to work and tested separately in order to set a focus and discover the answers to the research questions (Taylor, Bogdan & DeVault, 2015).

Derived from the research onion (figure 4.9) the researcher used quantitative data collection and analysis techniques and procedures. By employing a survey and mono method quantitative approach, the positivist philosophy of the research was fulfilled. The usage of deductive approach led to the elimination of all unexplained phenomena. All the questions were based on the confirmation of the reality with the elimination of any kind of question that consists of 'how' or 'why' and so on. Thus, the research onion is a simple figure that can be used by other researchers to determine the methodology, philosophy, techniques and procedures of their research.

In addition to the above methodological limitation of positivism there were other limitations, as follows:

1- The study was limited to the timeframe of the sampling.
2- The study is limited to the Smart Government organizations and any other types of organization are out of the scope of this study.
3- The study is limited to the managerial business analysis of resilience rather than to the technical aspect.
4- The study is limited to the responses obtained from the departments belonging to the Smart Government unit or under the umbrella of Smart Government, however, the responses of the Smart Government unit were very weak due to confidentiality issues.

4.6 Research Approach

The researcher adopted positivism research philosophy and conducted a deductive, quantitative and empirical research to fulfil the study objectives and answer its main questions. This study is deductive because it is a quantitative research and has adopted a positivism philosophy. Furthermore, the researcher wanted to test the relationship between two or more variables and has developed hypotheses which can be tested using quantitative analysis only. Nevertheless, this study is empirical because it is quantitative, and it depends on numeric data. The study showed that measuring resilience needs quantitative methods, techniques and procedures. The researcher tested the hypothesis in a numeric way and then prioritized the main factors that had greater impact on resilience; this determined and identified the main components of the resilience framework.

The research approach takes after the study with one distinct technique – deductive. In addition, a hypothesis is produced with the assistance of information to clarify the social spectacle. There are various advantages for the researchers using deductive methodology as per the prerequisite of their examination. The table underneath establishes that regions where the researcher can look for profit using this methodology (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007).

The deductive approach focuses on scientific principles. The aim is to look forward to shifting the focus on the research from theory to raw data in order to set a focus and research it from a different perspective. It aims to identify the relationship between different variables such as in this particular study, the dependent variable is cyber security, meanwhile the independent variables include resilience factors in context to operational, supply chain, information, network, developing organisation, IBM business resilience, and the barriers that directly or indirectly affect

the performance of cyber security in a Smart Government framework. There are certain limitations to the deductive approach; for example, it does not profit the deductive thinking, though it does encourage different limitations that would restrict different perspectives in different topics, thus would lead the research with no value, meanwhile, it does not affect the intellectually challenging approach. Therefore, while working on deductive research, it is important for the researcher to consider these limitations as it might limit the number of perspectives that can be outlined for the study related to cyber security and resilience, it has worked on expert opinion to set a focus and define a habitat relationship. (Saunders, Lewis & Thornhill, 2012; Cohen & Kietzmann, 2014).

4.7 Data Collection Method

Quantitative research techniques were used in this research. The quantitative research techniques used incorporate a survey with the closed-ended questions. This prompts responses delineated in the research recommendation. Hence, the results cannot address the genuine data in a summary format. Moreover, the respondents have compelled options of responses, in light of the assurance made by the researcher. Quantitative research is troublesome, expensive and requires a huge amount of time to play out the examination. This kind of research is orchestrated purposely while remembering the true objective to ensure complete randomization and the right task of controlled social affairs. A broad degree of respondents is reasonable for the depiction of the target respondents (Taylor, Bogdan & DeVault, 2015). Thus, to achieve all-around responses on an issue, data assembling in quantitative research procedures is routinely exorbitantly expensive in contrast to the subjective approach. The quantitative examination requires wide quantifiable examination, which can be difficult to perform for researchers from non-accurate establishments. Quantifiable examination relies upon consistent education and from this time forward it can be troublesome for

non-mathematicians to perform. It is altogether even more confusing for social sciences, preparing, human examinations, and psychological research. The beneficial response should depend upon the research issue instead of just a clear ‘yes’ or ‘no’ response (Kothari, 2004).

The prerequisites for the suitable statistical result are exceptionally extreme in quantitative research. Speculation is demonstrated with few tests because of which there is uncertainty in the outcomes. Results are retested and refined a few times for an unambiguous conclusion. Therefore, it requires additional time, venture, and assets to refine the outcomes.

4.8 Data Analysis Method

It is critical to gather information in a specific way to set a focus for the investigation; one might say that two fundamental kinds of research approach incorporate subjective and quantitative research. In any case, in some circumstances, research requires the accumulation of information through both methodologies, along these lines, a blended approach (quantitative and subjective) is completed by the researcher to gather and examine information. The idea of information gathering varies in both the research approaches; for instance, in the figure below, it can be seen that the quantitative approach follows a trial approach to test the speculation and check or distort the hypotheses identified with the subject. In the interim, subjective information centres on an observational approach to deal with gathering experimental information and shaping understanding in light of clear hypotheses (Kumar & Phrommathed, 2005).

Then, while using a quantitative approach, the researcher should gather and examine the information quantitatively and look into the outcomes to define understanding. As such, quantitative research approach is focused on gathering precise and numerical data for the research

subject, and it is based on factual examination. While then again, subjective information includes the gathering of a deliberate accumulation of subjective data under the state of the base control. The quantitative approach has been attempted with a specific end goal to gather information and break it down as indicated by the prerequisites of the investigation. Accordingly, to set a concentration, essential information has been investigated with the assistance of Pie graphs utilizing MS Excel to fully comprehend the data. In the interim, the writing survey has worked with optional information separated from the examinations accessible on Google Scholar (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007).

For what reason do such numerous instances of information examination end with broken cases? One of the principal reasons is that examining information is an entangled and repetitive process. It is never as simple as connecting numbers to a computer. A few issues that can prompt flawed information examination include not having the correct examination aptitudes. Unexpected announcing of negative outcomes is normally the consequence of an absence of appropriate preparing. More then one investigation (counting this one) found that doctors were ineffectively prepared in the best possible administration of clinical trials. Researchers were likewise inadequately prepared in perusing measurements from large datasets obtained from legitimate setups. For what reason would profoundly instructed individuals have so much inconvenience translating information investigation (Kothari, 2004).

The issues identified with subjective social examination is that this method is repetitive. The second potential issue with subjective research is that a particular issue could go unnoticed. In such a manner, the interpretations of researchers are compelled. A singular experience and learning impact of the discernments and conclusions is related to the research issue. As subjective research is for the most part open-completed, the respondent has more control over the substance of the data

assembled. Therefore, the researcher cannot check the results open-mindedly against the circumstances communicated by the respondents. Researchers imagine that it is difficult to look at causality between different research ponders. Subjective research is able to illuminate the refinement in the quality and amount of information obtained from different respondents and in providing solid conclusions (Kothari, 2004).

4.9 Sampling Method

There are diverse kinds of examining strategies; nevertheless, they are classifications into two distinct classes – likelihood (arbitrary) and non-likelihood (non-irregular) sampling techniques. A portion of the fundamental examining techniques used by the researchers incorporate the random sampling method gathered from arbitrary individuals and it is used if there should arise an occurrence of a significant example. The random sampling strategy is used for a vast population; however, it is very time consuming as it requires the researcher to separate the general populations as per their conclusion. Stratified sampling plans can be used to partition the objective populace into various subcategories. This focuses on inspecting intended interest group (Kothari, 2004).

The limitations of a sampling strategy are that it includes one-sided determination and along these lines drives us to reach mistaken inferences. Inclination emerges when the technique for determination of test utilization is flawed. Relatively few examples that are well-chosen might be significantly more solid than vast examples inadequately chosen. The challenges in choosing a genuinely illustrative example produce solid and exact outcomes are found just when they are illustrative of the entire gathering. Choosing examples is troublesome. The utilization of sampling strategy requires sufficient subject particular learning in the sampling system. A sampling includes statistical examination and computation of plausible mistakes (Taylor, Bogdan & DeVault, 2015).

At the point when the researcher needs particular learning in sampling, they may confer genuine errors. Thus, the consequences of the examination will misdirect. At the point when the units of the populace are not inhomogeneous, the sampling strategy will be informal. In sampling, however, the quantity of cases is limited; it is not simple to adhere to choose cases. The testing of the hypotheses might be generally scattered. A portion of the instances of the test may not collaborate with the researcher and some others might be out of reach. In light of these issues, no one of the cases may be taken up. The chose cases may be supplanted by different cases. The variability of units obstructs aftereffects of the examination (Kothari, 2004).

In this research 432 Smart Government employees will be selected randomly for the survey questionnaire, with an age range of 25-40 years and above using sampling strategy of purposive sampling technique.

4.10 Ethical Considerations

While conducting research, it is essential for researchers to focus on moral contemplations, as it causes them to enhance the concentration and extent of the examination, while helping the investigation to anticipate decreasing the moral issues that it may look like because of the usage of exploitative practices in information gathering and investigation. The moral consideration for this investigation is consolidated. (Schroeder, 2014)

Plagiarism – it is a genuine mistake, particularly in business related to scholastics if the researcher is utilizing optional information, it is fundamental for the researcher to reference the work with the best possible source, the name of the writer, information, and available source. If there should be an occurrence of this research, the researcher has given every one of the references

to the optional information used in the investigation to layout the foundation and writing survey for the examination (Taylor et al., 2015).

Informed Consent – while utilizing essential information, there are sure components that are vital to consider, for instance, written or verbal consent from the general population taking part in the information gathering. However, the issue is typically observed by researchers chipping away at interviews, yet even in online reviews, it is vital to put a note in the study to determine with respect to the idea of the examination, how the information will be completed so no hostile claims can be made over the credibility of the research. With regards to the investigation, an online overview is led; nonetheless, the workers and supervisors were given a brief about the examination and how the information would be used (Taylor, Bogdan & DeVault, 2015).

Reliability and credibility of data – it is imperative to use just solid and sound sources to diagram the information for the investigation, using sources, for example Wikipedia and others, to influence the believability of the examination. Thus, with a specific end goal to set a concentration, information has been accumulated from Google Scholar so just genuine and distributed researchers are used (Cohen & Kietzmann, 2014).

4.11 Conclusion

This research is quantitative as mentioned above. Cyber resilience is better studied quantitively, to be able to measure the resilience and define accurate results rather than just assuming things. It can be said that the research approach sketched out all the conceivable methodologies that can be used by the researcher keeping in mind the end goal to set a spotlight on the research. In any case, thinking about the idea of the examination, it has worked with both essential and auxiliary information gathering by utilizing a blended a to deal with frame setting

about the investigation. This has helped the examination to understand and break down the gathered information with the assistance of software in order to carry out statistical data analysis.

At last, individuals who view themselves as essentially subjective or principally quantitative have a tendency to be nearly as different as those from the restricting scenarios. There are subjective researchers who fit serenely into the post-positivist convention and in contemporary quantitative research. Furthermore, there are quantitative researchers (though, presumably less) who utilize quantitative data as the reason for the investigation, perceiving the innate impediments and complex suspicions underneath all numbers. In either camp, the extraordinary and crucial difference between both philosophical suspicions and the idea of information. Progressively, there are researchers who are intrigued by mixing the two customs, endeavouring to obtain the upsides of each. Social research is wealthier for the more extensive assortment of perspectives and strategies that the investigation produces. The diverse approach is in this manner impossible in instructive research.

By choosing the methodology of the research and employing the methodological framework of the research, the researcher was able to test H3 and H4 of the research (see also Chapter 7: testing hypotheses table). As per Ridley and Channing (1999) resilience is affected by management control because both risks and surprises are difficult to handle; in other words they are difficult to control. By applying management control to the systems, organizations guaranteed risk-control and change-control on a certain level (Bouaziz & Hachicha, 2018).

Hyslop (2016) emphasized the role of management control, he preferred to call it “security controls”. Different types of organizations - including coordination structures sector, associations and organizations - can use a framework for a variety of purposes, including the creation of common profiles. At the same time Hyslop (2016) used the very common NIST Risk Management

Framework. He mentioned, “to demonstrate a mature risk management methodology that would enhance an organization's cyber-security program if implemented properly” (Cyber-Security & Risk Management, an evolving ecosystem, 2016)[vii].

According to CISO there are six steps to implement a risk management process into strategic operations:

• Categorize information systems and data

• Select security controls

• Implement security controls

• Continually assess security controls

• Authorize (verify risk baseline)

• Continually monitor security controls

So, by this matter each step will be reviewed as follows:

- Categorize (Information Systems & Data)

For this essential step NITS has its own tips and techniques for systems guidelines. Every information system has its threats, but not all threats are the same or equal. Furthermore, every threat has vulnerable impact to the organization’s IT assets. Therefore, this describes best how to categorize them and how to prioritize data protection (Anon, 2018).

Cybersecurity is defined as controlling the access to information contained on networked systems. The reliability and trust in the digital infrastructure of cyberspace depends on the

effectiveness of cybersecurity controls. The role of cybersecurity professionals is to plan and design effective controls to ward off any potential attack on the cyberspace components and effective mitigation of the consequences of such an attack. Since all the potential attacks cannot be prevented, it is therefore the key objective of security personnel to detect the attack and take control before any damage is caused (Keys, Chhajer, Liu & Honer, 2016).

As per Leck (2015) and Olson and Anderson (2016) management control consists of operations, technologies, managements' countermeasures that safeguard the organizations systems and information, for the sake of its confidentiality, availability, transparency, integrity, and accessibility. Management control should be categorized (Mienipre et al., 2016). Accuracy and attentive collection of information in the first place is an important process besides choosing an appropriate set of safety measures to adequately reduce the risks by satisfying certain and sometimes specific requirements for safety of the organization is not the least important task as well. This task demonstrates the organization's adherence to safety and the due diligence exercised to its privacy policy, integrity and availability of organizational information and information systems (Harrington & Ottenbacher, 2011).

Management control creates capabilities for proper functioning and resilience against cyber-attack (Arlitsch & Edelman, 2014). By implementing management control the recognized regular controls acquired by the data framework, information system security engineers with support from information system security officers arrange with the normal control supplier to decide the most suitable approach to apply the basic controls to the hierarchical data frameworks. In fact, this does not prevent the utilization of open source devices; to utilize open source arrangements there a couple of focuses to check (Bagheri & Ridely, 2017).

Many authors and scholars explored how management control is an important element in the resilience frameworks, whereas in recent studies (Bagheri & Ridely, 2017) it appears as a number one priority among the rest of the factors affecting resilience (Bosen, 2017) management control and security control mentioned in a lot of studies concerning resilience and cybersecurity risk management (Annareli & Nonino, 2016; Trim & Lee, 2007; Boin & McConnell, 2007; Dess, et al., 2013; Nag et al., 2007).

However, vulnerability which was the number one element that affects cyber resilience (Sikula et al., 2015) due to the endless problems of the internet and computerizations, no longer holds that privilege! After the technological breakthroughs and the advancement in technology worldwide, the importance of this factor has retreated (Schell, 2016)

Vulnerability factors include turbulence, deliberate threats, external pressures, resource limits, sensitivity, connectivity, and disruption by supplier or buyer of the product or service (Jenab & Moslehpour, 2016). There is a strong correlation between management control which creates capabilities and vulnerability factors; if the capabilities increase in the organization, there is less vulnerability. Thus, there is linkage between vulnerabilities and capabilities successfully used to face those vulnerabilities (Lambert & Knemeyer, 2004).

As per Arlitsch and Edelman (2014) resiliency frameworks should consist of more sophisticated elements rather than just focusing on the traditional vulnerability issues. Risk management is not enough in this case, according to a study conducted by Sikula et al. (2015). Risk management is not enough on its own and the need for resilience scientific frameworks has arisen, especially with the existence of vulnerabilities in the virtual means of communication, the team set a conceptual framework of resiliency for the practitioners to adapt and to adjust according to the

needs of their organization to help recover after cyber-attacks and then learn how to evolve and prosper post trauma (p. 222).

The priority switched between the elements throughout time, whereas in the 1990s the care was more about vulnerabilities and capabilities factors, while in the twenty-first century the focus has shifted to emphasize more on forces of change and management control factors. Of course, after realizing that the problem was not just about computers and cybernetic errors, but human errors that have greater impact, especially in this constantly changing cyber and business world. The role of management control shows significant implication on resilience to overcome the new crisis of cyberspace.

The suggested methodological framework of this study consists of the main components of the resilience process or framework, tying them to the business management arena. The framework covers business continuity, business profitability and performance of an organization. The reason is that Smart Government's overarching goal is usually emphasizing the business arena in the country, including e-commerce, e-billing and e-banking.

Many authors and scientists have emphasized the vulnerability impact on the resilience status of an organization (Stolfo et al., 2008; North et al., 2016; Blowers, et al., 2016; Lambert & Knemeyer, 2004; Trim, & Lee, 2007; Barab´asi, 2003; Kahn, Barton & Fellows, 2013).

As per Pauchant and Mitroff (1992) and Trim and Lee (2007), while suggesting for enhanced resilience of organizations, some scholars have developed frameworks to achieve this purpose. Resilience has been described by Buliga et al. (2016) as giving two major parts or characteristics against vulnerability: adaptability and robustness. Robustness is a system that returns to its actual state. In an organizational context, robustness is the ability of an organization to avoid loss by withstanding stress. Resilient organizations can absorb adversity and complexity

by reducing vulnerabilities to risk environments, coping with the unexpected complexities, and recovering from these risk situations. The second important part is adaptability that gained attention in organizational theory in the 1980s. Resilience was considered as reinforcement and adaptation emerging from a traumatic, stressful, and challenging event. However, adaptability is the fast action taken during crises and works well with vulnerability issues.

Vucina and Fabac (2017) have presented simulation-scenarios by exploring the possibilities of using Monte Carlo methods to find some characteristics and design parameters of working units in an organization. Particular attention was paid to protection of information systems and their vulnerabilities. The researchers explained that resilience is the ability of an organization's system to depreciate, effectively recover, and foresee disruptions or stress related events, and is related to its risk management process. However, the researchers have argued that resilience from the perspective of an organization means continued security attention and departure from traditional ways of organizational risk management. Overall, the study is valuable as it has offered a valuable option of simulation to enhance the readiness of an organization against any risks and threats, such as fire and accidents. Therefore, it will be easier for an organization to practice resilience with efficiency as it has practiced risk management using simulations to survive vulnerabilities.

Michael Chertoff (2014) talked about "managing risk in today's security landscape". Chertoff suggested a framework key which is to recognize multiple layers of protection from the potential threats. Meaning, in order to exit the target zone one needs to create a number of solutions, by a continual assessment of risk and measurement of vulnerabilities to be able to deal with them. The researcher highlights the vulnerability of humans rather than the weakness in systems; given the fact that only human beings commit cyber-attacks and human beings also are the dealing with it. He divided the dynamic risks into two main parts of one framework: 1) the risk management

section that consists of recognizing vulnerabilities, anticipating threats and understanding consequences; 2) planning and prevention, where operating and executing phase can began depending on risk management factors to prevent cyber-attacks from occurring (p. 38), for further investigation on H3 and H4 of this research (see Chapter 7: testing hypothesis table).

According to a debate by Morais-Storz et al. (2018) in their research which talked about vulnerabilities, capabilities and management control, organizations around the world are facing cyber threats. Although, there are laws and restrictions to prevent cyber-crimes, hackers are creating new ways to continue their criminal activities. Therefore, it is crucial for organizations to prepare for an unexpected event by maintaining their capability of resilience. The researchers have suggested that application of the rules of management control and change management on organizational resilience will enable organizations to take resilience as a dynamic concept. Therefore, the valuable insight that can be found in this research is that organizations need to identify the change basis of their business to achieve resilience efficiently. An important aspect of incorporating resilience in management control is that it can be achieved successfully with the right team and top management with backgrounds in resiliency and flexibility (Buliga et al., 2016).

CHAPTER FIVE– RESULTS AND FINDINGS

5.1. Introduction to the chapter

This chapter presents the findings obtained from the survey. There are different sections in this chapter, including results and findings, which are further sub-divided. The chapter presents the demographics of the participants and then moves towards the analysis of questions asked. In addition, the summary of correlations and ANOVA tables have also been provided along with the elaboration of reliability analysis. Version 16.0 of the SPSS program is used in the statistical analysis of the survey questionnaire. In addition, an independent sample in t-test and the use of one sample are adopted. Furthermore, the correlation and regression analysis method is used to finalize the analytical process of this thesis. The researcher also conducted regression to determine the direction of the relationship between variables. The researcher adopted a positivism research philosophy and conducted deductive research along with quantitative empirical research to fulfil the research objectives and answer the study's main questions. This study is deductive because it adopts the positivism philosophy and the research is quantitative. Moreover, this is the case because it tests the relationship between two or more variables and the researcher has developed hypotheses which can be tested using quantitative analysis. Nevertheless, this study is empirical as it is quantitative, and it depends on numeric data. The study showed that measuring resilience needs quantitative methods and research. The researcher tested the hypotheses in a numeric way and then prioritized the main factors that have greater impact on resilience. The researcher designed the questionnaires in the following structure:

1- based on framework

2- based on variables

3- based on hypothesis

4- by reviewing different literature

5- with co-operation of the supervisor

6- based on research questions, objectives and title

The total targeted population in Smart Government organizations is 40,000, with 432 responses collected successfully for analysis. Four hypotheses and the null hypothesis were developed for this research. For each hypothesis at least 100 survey responses were obtained from users of the smart system.

A questionnaire was built according to the variables of the research as per the following statements:

a- Capability Factors (Independent)

1) The resilience management in Smart Government organizations will bring flexibility in cyberspace, and continuity of organizational functions despite cyber-attacks.
2) Multiple layers to foster resilience will result in a shorter network and system downtimes.
3) Risk management will be beneficial for all stakeholders.
4) Resilience and risk management will result in better mitigation, reduction or elimination of cyber-related attacks.
5) Smart Governance will introduce a high rate of resilience in institutional platforms and the virtual services provided.

6) The Smart Governance Platform will result in capacity building, better knowledge transfer and the creation of new skill sets for the stakeholders.

7) Resilience and risk management in a Smart Government organization will enhance the capacity of the system to perform better, even if there are issues in the cyber environment.

8) The overall performance of the organization will improve with the introduction of Smart Governance resilience and risk management interventions.

9) The institution will greatly benefit from the new knowledge-base and new skill requirements, occasioned by the introduction of a Smart Governance risk management strategy.

10) The capability factors affect resilience in Smart Government organizations.

b- Forces of Change (Independent)

1) The changing environment and relations in society require Smart Government organizations in the UAE to focus on better resilience policies.

2) The regularity authorities of the country should pay attention to enhanced infrastructure resilience in Smart Government organizations.

3) The Smart Governance Platform will result in faster and more specific responses to stakeholders.

4) The Smart Governance Platform will enable the institution to focus its resources and energy on core activities rather than peripheral ones.

5) External service providers for the Smart Governance Platform are not always reliable and do not always provide consistent services.

6) The safe environment created by risk management will enhance technical competence in Smart Government organizations.

7) There are differences between Smart Government organizations in terms of using resilience and cybersecurity risk management.

8) The change factors affect resilience in Smart Government organizations.

9) The forces of change cause vulnerabilities that provoke the need for resilience in organizations.

10) The Smart Governance Platform and associated risk management interventions will improve the overall satisfaction of the students and staff to the institution's service provision.

11) The purpose of the cybersecurity domain in Smart Government organizations is to build control for making cyberspace secure.

c- Management Control Factors (Independent)

1) Risk management in ICT applications will bring about a lot of benefits to the institution.

2) Better management control in Smart Government organizations can create capabilities and resilience against cyber-attacks.

3) The current ICT policies and frameworks that guide the system are inadequate due to a lack of resilience polices and risk management strategy.

4) Smart Government organizations in the UAE need effective policies and frameworks for the system.

5) Improved risk management and resilience will enhance the performance of employees.

6) Better policies for cyber resilience will help Smart Government organizations to recover quickly from any cyber-attack.

7) The federal government of the UAE is aware of the importance of resilience and cybersecurity management in Smart Government organizations.

8) The introduction of the Smart Governance Platform may result in a dearth of interpersonal skills from minimal staff recruitment.

9) The introduction of Smart Governance risk management will result in higher profit margins and reduced operational costs.

10) The management control factors affect resilience in Smart Government organizations.

11) The resilience framework is about detecting, preventing, and recovering from a cyber-attack.

12) The implementation of balanced resilience can result in improved performance.

d- Vulnerability Factors (Independent)

1) The government is focusing on cyber resilience to avoid threats in the changing cyber environment.
2) Smart Governance Platforms are generally vulnerable to common attacks such as Denial of Service Attacks.
3) Smart Governance Platforms will result in a greater uptake of cloud-based resources by the average person.
4) Risk management interventions will prevent the institution from being exposed to costly legal proceedings in case of data breaches.
5) Smart Governance Platforms will introduce more secure data storage and data management to this facility.
6) Existing and evolving cybersecurity threats will make Smart Government organizations vulnerable.
7) The Smart Governance Platform may cause an institution to lose reliable and more talented staff who may not be that tech savvy and consequently to introduce untrusted third parties.

8) In the event of a data breach, massive volumes of sensitive data could be get exposed to the public domain.

9) The vulnerability factors affect resilience in Smart Government organizations.

10) Unbalanced resilience in organizations can impose excessive frisks and erode profitability.

e- Resilience in E-government Organizations (Dependent)

1) Smart Government organizations require better resilience and risk management policies.

2) There are more risks than benefits attributed to the whole process of Smart Governance.

3) Smart Governance introduces improved techniques and processes to the organization.

4) Smart Governance organizations should consider the implementation of effective resilience.

5) Smart Governance Platforms will be able to accurately predict the unique needs of individual students, instead of providing generic answers.

6) The Smart Governance Platform will enable the institution to maintain its competitive advantage across all spheres of service provision.

7) The Smart Governance Platform will improve service consistency, continuity and overall quality at a minimal cost.

8) The Smart Governance Platform will offer real-time feedback and 24/7 access and resource provision.

9) Resilience in Smart Government organizations will improve performance and output.

10) The organization will perform extremely well in the core functions because of the introduction of Smart Governance resilience and risk management policies.

11) Resilience can help organizations in evaluating risks and challenges involved at multiple levels.

5.2. Main Results and Findings

Table 5.8: Sample Crosstabulation Statistics

Count	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Educational status * Gender	380	99.5%	2	0.5%	382	100.0%
Educational status *Age group	378	99.0%	4	1.0%	382	100.0%
Employment status *Gender	377	98.7%	5	1.3%	382	100.0%
Employment status *Age group	375	98.2%	7	1.8%	382	100.0%
Duration of employment *Gender	379	99.2%	3	0.8%	382	100.0%
Duration of employment *Age group	377	98.7%	5	1.3%	382	100.0%

Department *Gender	380	99.5%	2	0.5%	382	100.0%
Department *Age group	378	99.0%	4	1.0%	382	100.0%

The table above shows that there is missing data in the sample. The total percentage of missing data never reached 2% of the total sample.

Table 5.9: Educational status *Gender Crosstabulation

Count		Gender		Total
		1.00	2.00	
Educational status	1.00	39	42	81
	2.00	25	39	64
	3.00	81	82	163
	4.00	21	32	53
	5.00	6	13	19
Total		172	208	380

The table above compares the of educational status of the respondents by gender. The table shows that the number of highly educated female respondents in the government sector is higher than males. The table shows that the sample consists of a higher number of male respondents with low

educational levels than females. This shows that females in the sample are relatively more educated than males in Smart Government organizations.

Table 5.10: Educational status *Age group Crosstabulation

Count		Age group				Total
		1.00	2.00	3.00	4.00	
Educational status	1.00	48	13	14	5	80
	2.00	32	24	6	1	63
	3.00	87	49	20	7	163
	4.00	14	25	10	4	53
	5.00	2	11	5	1	19
Total		183	122	55	18	378

The table above compares between the different age groups in terms of educational status. The table shows that the ‘below 30 years old’ age group are in the middle level of education, which is the bachelor’s degree. For master’s degree and above, the second age group is the highest. For diploma level or less, most respondents are more than above 40 years old. In general, the ages in the governmental sector are focused between 25 and 45 years of age, and the number of respondents in the sample above 50 were relatively few. In this case, the younger the respondents are the better because the topic of the research is Smart Government, which is a relatively new subject and the younger generation is typically more familiar and experienced with smart tools than older people.

Table 5.11: Employment status *Gender Crosstabulation

Count		Gender		Total
		1.00	2.00	
Employment status	1.00	71	72	143
	2.00	70	72	142
	3.00	30	62	92
Total		171	206	377

The table above shows the comparison between the males and females of the sample in terms of their employment status. The female respondents are the larger sector in all kinds of employment in the sample. This is because this is the typical demographic profile in the governmental sector.

Table 5.12: Employment status *Age group Crosstabulation

Count		Age group				Total
		1.00	2.00	3.00	4.00	
Employment status	1.00	90	33	15	3	141
	2.00	56	53	22	11	142
	3.00	36	36	16	4	92
Total		182	122	53	18	375

The table above shows the classification of age groups based on employment status in the sample. The table shows that most of the respondents are in the first age group as well as in the first

employment status. Relatively few employees above 50 are employed in the first employment status. It is observed that most of the employees in the age group between 30 and 40 are spread across all employment statuses.

Table 5.13: Duration of employment *Gender Crosstabulation

Count		Gender		Total
		1.00	2.00	
Duration of employment	1.00	85	89	174
	2.00	40	44	84
	3.00	25	32	57
	4.00	22	42	64
Total		172	207	379

In the table above, statistics show the duration of employment in the sample for males and females. The sample shows that females spend relatively longer periods of time as employees in the government sector. This is true to all sampling units and to all employment durations when we compare between male employees versus female employees.

Table 5.14: Duration of employment *Age group Crosstabulation

Count	Age group	Total

		1.00	2.00	3.00	4.00	
Duration of employment	1.00	126	35	12	0	173
	2.00	37	38	8	0	83
	3.00	10	37	9	1	57
	4.00	9	12	26	17	64
Total		182	122	55	18	377

In the table above the crosstabulation shows the relationship between the age group and the duration of the employment. The highest sector is the sector of the first age group and the shortest duration of employment, which accounts for 126 respondents. We can conclude that there are no employees in the sample who belong to the fourth age group and reside in the first or second groups of employment durations.

Table 5.15: Department * Gender Crosstabulation

Count		Gender		Total
		1.00	2.00	
Department	1.00	31	43	74
	2.00	20	17	37
	3.00	26	25	51
	4.00	95	123	218
Total		172	208	380

In the table above there are four department groups and the table demonstrates that there are more females than males in the first and the fourth department groups, and vice versa in the second and third department groups.

Table 5.16: Department * Age group Crosstabulation

Count		Age group				Total
		1.00	2.00	3.00	4.00	
Department	1.00	32	28	12	1	73
	2.00	20	11	4	2	37
	3.00	25	20	5	1	51
	4.00	106	63	34	14	217
Total		183	122	55	18	378

In the table above the age groups are distributed by departments. The highest category of the sampling respondents is the fourth group of departments, which accounts for 106 respondents. Generally, most of the employees belong to the fourth category of the department categories.

5.2.1. Descriptive Statistics

In this section the researcher will present the results of the survey according to the answers derived from the survey questionnaire.

5.1.2 Demographics of Participants

Table 5.17: Gender of Participants

		Frequency	Percent
Valid	Male	197	45.6
	Female	231	53.5
	Total	428	99.1
Missing	System	4	.9
Total		432	100.0

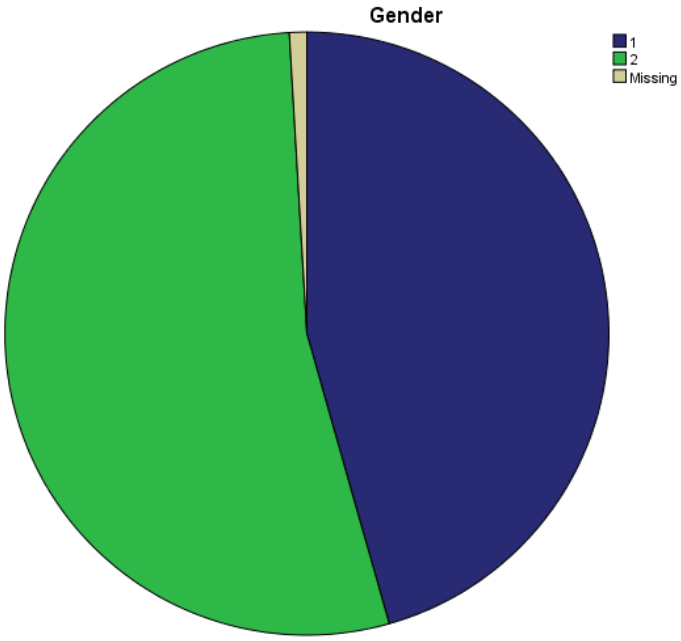

Figure 5.10: Gender

As per the figure given above, there were 432 participants in total in the survey. Forty-five percent of the participants were males, whereas 53% of the participants were females. As per the data given in both Figure 9 and Table 17, it is demonstrated that the majority of participants were females.

Table 5.18: Age of Participants

		Frequency	Percent
Valid	25-30	202	46.8
	31-40	138	31.9
	41-50	60	13.9
	Over 50 years	25	5.8

	Total	425	98.4
Missing	System	7	1.6
Total		432	100.0

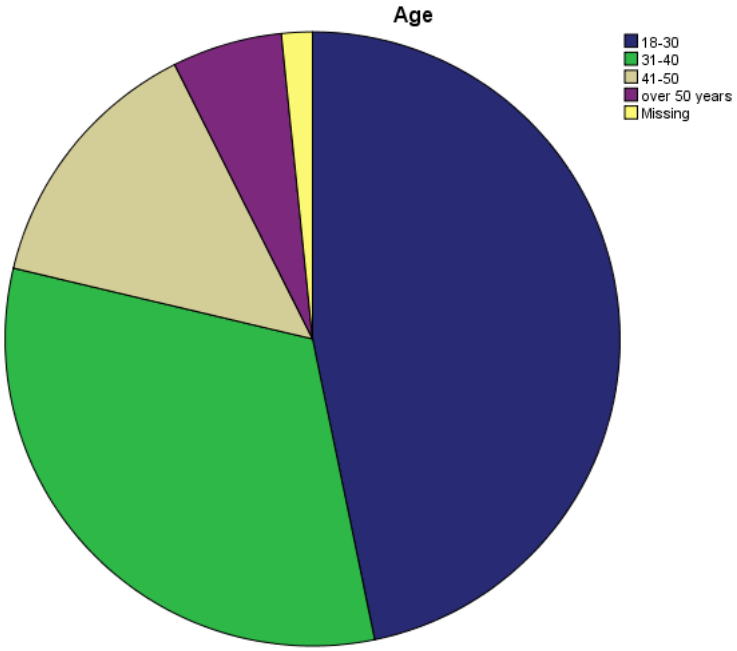

Figure 5.11: Age

As per the data given above, there were 432 participants in total in the survey. Forty-six percent of the participants were between 25-30 years of age, 31% were 31-40, 13% were in 41-50 and 5.8% were above 50 years of age. As per Figure 10 and Table 18, it is demonstrated that the majority of participants were in the age bracket of 25-30.

Table 5.19: Education Level of Participants

		Frequency	Percent
Valid	Secondary	94	21.8

	Diploma	75	17.4
	Bachelor's degree	183	42.4
	Master's Degree	55	12.7
	PhD	21	4.9
	Total	428	99.1
Missing	System	4	.9
Total		432	100.0

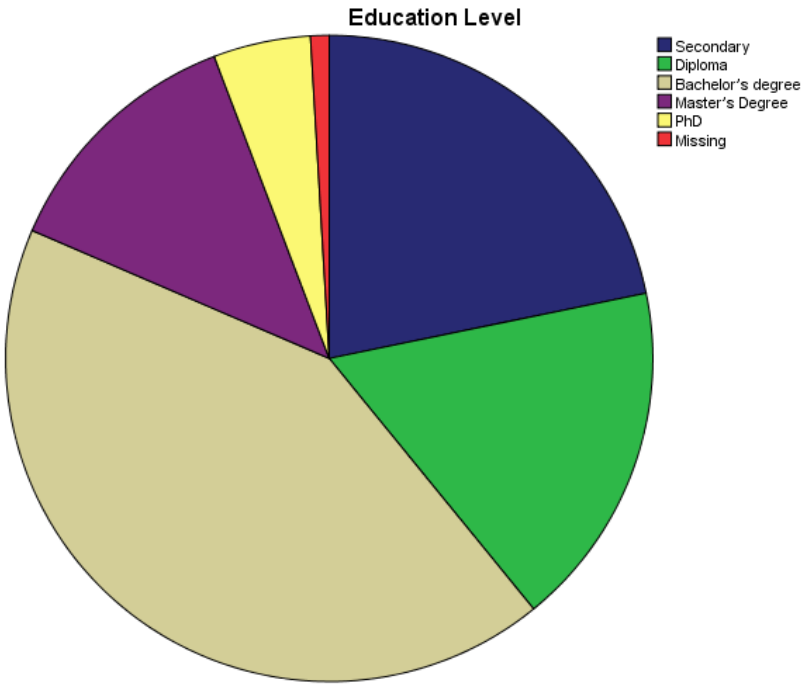

Figure 5.12: Education Level

As per the data given above, there were 432 participants in total in the survey. Almost 22% of the participants were secondarily educated, 17% held a diploma, 42% held a bachelor's degree, 12% held a master's degree, and 4.9% held a PhD. As per the given data in Figure 11 and Table 19, it is demonstrated that the majority of participants held a bachelor's degree.

Table 5.20: Employment Status of Participants

		Frequency	Percent
Valid	Casual	160	37.0
	Permanent	164	38.0
	Contract	100	23.1
	Total	424	98.1
Missing	System	8	1.9
Total		432	100.0

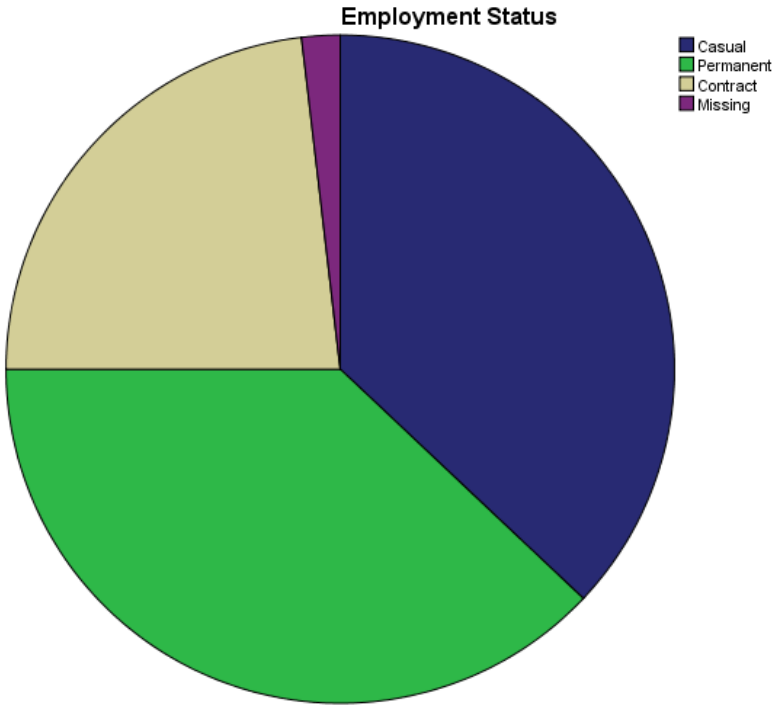

Figure 5.13: Employment Status

As per the data given above, there were 432 participants in total in the survey. Thirty-seven percent of the participants were casual employees, 38% were permanent employees, and 42% were contract-base employees. As per the given data in Figure 12 and Table 13, it is demonstrated that the majority of participants were in permanent employment.

Table 5.21: Duration of Employment of Participants

		Frequency	Percent
Valid	Less than 5 Years	191	44.2
	5-10 Years	100	23.1

	11-15 Years	64	14.8
	Over 15 years	72	16.7
	Total	427	98.8
Missing	System	5	1.2
Total		432	100

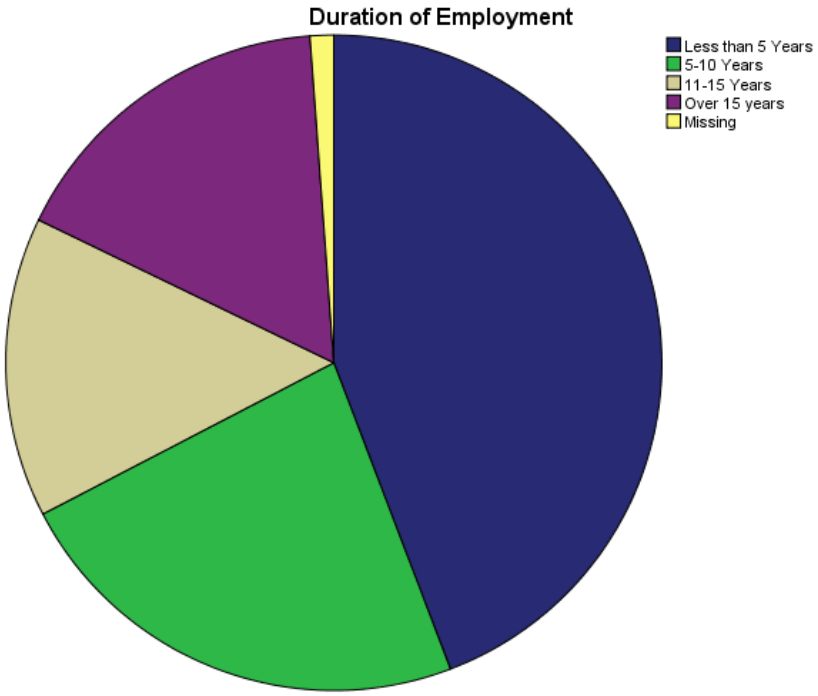

Figure 5.14: Duration of Employment

As per the data given above, there were 432 participants in total in the survey. Forty-four percent of the participants were employed for less than five years, 23% were in between 5-10 years, 14% were between 11-15 years, and 16% had over 15 years of employment. As per the given data in Figure 13 and Table 14, it is demonstrated that the majority of participants had less than 5 years of employment.

Table 5.22: Department of Participants

		Frequency	Percent
Valid	Administration	83	19.2
	Finance	46	10.6
	IT	59	13.7
	Other	238	55.1
	Total	426	98.6
Missing	System	6	1.4
Total		432	100

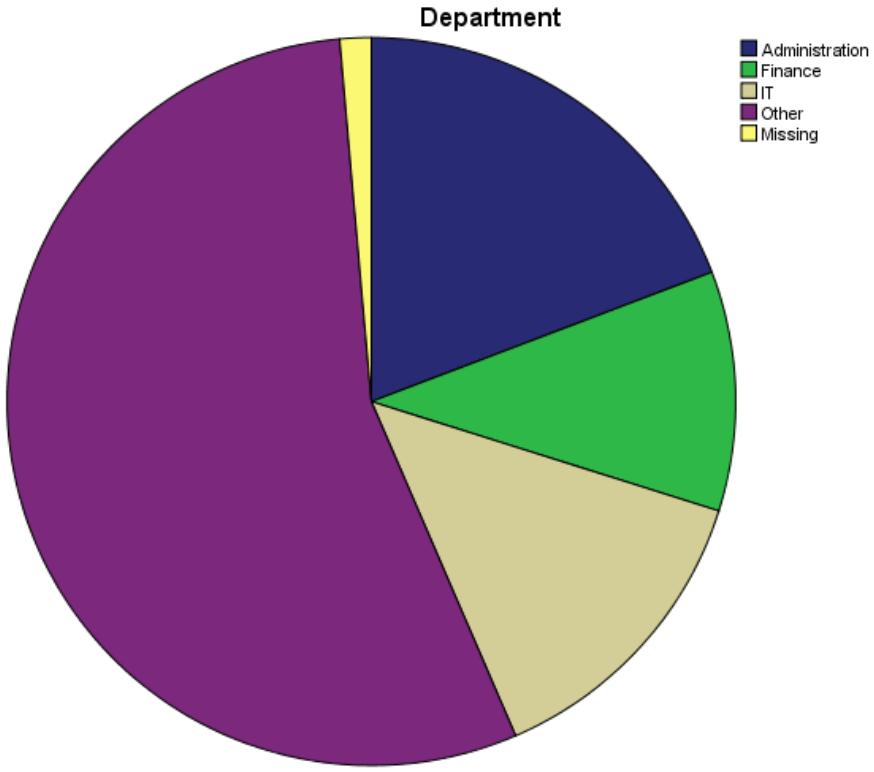

Figure 5.15: Department of Participants

As per the data given above, there were 432 participants in total in the survey. Nineteen percent of the participants were in Administration, 10% were in Finance, 13% were in IT, and 55% were from other departments. As per the given data in Figure 14 and Table 15, it is demonstrated that the majority of participants were employed in the Finance department.

Table 5.23: Survey responses

Statement		Valid						Missing	Total
	Stat	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree	Total	System	
Risk Management in Information Communication Technology Applications will bring about a lot of benefits to the Institution	Frequency	129	214	68	6	12	429	3	432
	Percent	29.9	49.5	15.7	1.4	2.8	99.3	0.7	100
Smart governance organizations need better resilience and risk management policies	Frequency	127	220	59	13	8	427	5	432
	Percent	29.4	50.9	13.7	3	1.9	98.8	1.2	100
The resilience management in smart government organizations will bring flexibility in cyberspace, and continuity of organizational functions despite the cyber attack	Frequency	96	204	102	17	6	425	7	432
	Percent	22.2	47.2	23.6	3.9	1.4	98.4	1.6	100
There are more risks than benefits attributed to the whole process of Smart Governance	Frequency	60	140	125	83	18	426	6	432
	Percent	13.9	32.4	28.9	19.2	4.2	98.6	1.4	100
The changing environment and relations in society require smart government organizations in the UAE to focus on better resilience policies	Frequency	110	198	90	20	7	425	7	432
	Percent	25.5	45.8	20.8	4.6	1.6	98.4	1.6	100
Smart Governance introduces improved techniques and processes to the organization	Frequency	115	217	63	21	9	425	7	432
	Percent	26.6	50.2	14.6	4.9	2.1	98.4	1.6	100
Smart governance organizations should consider implementation of effective resilience	Frequency	96	218	80	18	12	424	8	432
	Percent	22.2	50.5	18.5	4.2	2.8	98.1	1.9	100
Better management control in smart governance organizations can create capabilities and resilience against cyber attacks	Frequency	104	211	82	15	9	421	11	432
	Percent	24.1	48.8	19	3.5	2.1	97.5	2.5	100
	Frequency	84	171	129	25	15	424	8	432

Multiple layers to foster resilience will result in shorter network and system downtimes	Percent	19.4	39.6	29.9	5.8	3.5	98.1	1.9	100
The government is focusing on cyber resilience to avoid threats in changing cyber environment	Frequency	76	195	120	19	15	425	7	432
	Percent	17.6	45.1	27.8	4.4	3.5	98.4	1.6	100
Smart Governance Platforms is generally vulnerable to common attacks such as Denial of Service Attacks.	Frequency	68	153	153	43	5	422	10	432
	Percent	15.7	35.4	35.4	10	1.2	97.7	2.3	100
Smart Governance Platforms will result in a greater uptake of cloud based resources by the average person	Frequency	81	189	121	17	17	425	7	432
	Percent	18.8	43.8	28	3.9	3.9	98.4	1.6	100
Smart Governance Platforms will be able to accurately predict the unique needs of individual students, instead of providing generic answers.	Frequency	83	191	108	30	12	424	8	432
	Percent	19.2	44.2	25	6.9	2.8	98.1	1.9	100
The current ICT policies and frameworks that guide the system are inadequate due to lack of resilience polices and risk management strategy	Frequency	61	180	138	31	13	423	9	432
	Percent	14.1	41.7	31.9	7.2	3	97.9	2.1	100
Smart governance organizations of the UAE need effective policies and frameworks for the system	Frequency	83	207	96	24	13	423	9	432
	Percent	19.2	47.9	22.2	5.6	3	97.9	2.1	100
The smart Governance Platform will enable the institution to maintain its competitive advantage across all spheres of service provision.	Frequency	78	203	110	21	10	422	10	432
	Percent	18.1	47	25.5	4.9	2.3	97.7	2.3	100
The smart Governance Platform will improve service consistency, continuity and overall quality at a minimal cost.	Frequency	88	189	105	30	10	422	10	432
	Percent	20.4	43.8	24.3	6.9	2.3	97.7	2.3	100
Risk Management interventions will prevent the institution from being exposed to costly legal proceedings in case of data breaches	Frequency	79	201	97	31	17	425	7	432
	Percent	18.3	46.5	22.5	7.2	3.9	98.4	1.6	100
	Frequency	88	182	103	24	17	414	18	432

The smart Governance Platform will offer real time feedback and 24/7 access and resource provision.	Percent	20.4	42.1	23.8	5.6	3.9	95.8	4.2	100
Improved risk management and resilience will enhance performance of employees	Frequency	87	201	98	24	11	421	11	432
	Percent	20.1	46.5	22.7	5.6	2.5	97.5	2.5	100
Risk management will be beneficial for all stakeholders	Frequency	93	184	104	33	8	422	10	432
	Percent	21.5	42.6	24.1	7.6	1.9	97.7	2.3	100
Resilience and Risk Management will result in better mitigation, reduction or elimination of cyber related attacks	Frequency	86	202	107	19	9	423	9	432
	Percent	19.9	46.8	24.8	4.4	2.1	97.9	2.1	100
Better policies for Cyber resilience will help smart government organizations to recover quickly from any cyber attack	Frequency	99	199	94	21	10	423	9	432
	Percent	22.9	46.1	21.8	4.9	2.3	97.9	2.1	100
The regularity authorities of the country should pay attention enhance infrastructure resilience in smart government organizations	Frequency	93	204	98	23	4	422	10	432
	Percent	21.5	47.2	22.7	5.3	0.9	97.7	2.3	100
The federal government of the UAE is aware of the importance of resilience and cyber security management in smart government organizations	Frequency	98	175	119	24	6	422	10	432
	Percent	22.7	40.5	27.5	5.6	1.4	97.7	2.3	100
The purpose of cyber security domain in smart government organizations is to build control for making cyberspace secure	Frequency	90	203	86	27	17	423	9	432
	Percent	20.8	47	19.9	6.3	3.9	97.9	2.1	100
Smart Governance will introduce a high rate of resilience in institutional platforms and virtual services provided.	Frequency	86	194	110	17	13	420	12	432
	Percent	19.9	44.9	25.5	3.9	3	97.2	2.8	100
The smart Platform will result in faster and more specific responses to stakeholders	Frequency	101	173	110	26	9	419	13	432
	Percent	23.4	40	25.5	6	2.1	97	3	100
	Frequency	96	190	96	21	15	418	14	432

Smart Governance Platforms will introduce more secure data storage and data management to this facility	Percent	22.2	44	22.2	4.9	3.5	96.8	3.2	100
The smart Governance Platform will enable the institution to focus its resources and energy on core activities rather than peripheral ones.	Frequency	94	172	124	25	7	422	10	432
	Percent	21.8	39.8	28.7	5.8	1.6	97.7	2.3	100
The smart Governance Platform will result in capacity building, better knowledge transfer and the creation of new skill sets for the stakeholders.	Frequency	99	184	100	26	12	421	11	432
	Percent	22.9	42.6	23.1	6	2.8	97.5	2.5	100
Existing and evolving Cyber Security Threats will make the smart government organizations vulnerable	Frequency	79	158	121	44	17	419	13	432
	Percent	18.3	36.6	28	10.2	3.9	97	3	100
The smart Platform may cause the institution will to lose reliable and more talented staff who may not be that tech savvy, and introduce untrusted third parties.	Frequency	88	168	113	38	13	420	12	432
	Percent	20.4	38.9	26.2	8.8	3	97.2	2.8	100
External Service Providers for the smart Governance Platform cannot always reliable and consistent services	Frequency	76	172	129	32	8	417	15	432
	Percent	17.6	39.8	29.9	7.4	1.9	96.5	3.5	100
The introduction of the smart Governance platform may result in a dearth of interpersonal skills from minimal staff recruitment.	Frequency	62	177	130	33	19	421	11	432
	Percent	14.4	41	30.1	7.6	4.4	97.5	2.5	100
In the event of a data breach, massive volumes of sensitive data could be get exposed to the public domain.	Frequency	74	182	122	32	9	419	13	432
	Percent	17.1	42.1	28.2	7.4	2.1	97	3	100
Resilience and risk management in smart government organization will enhance the capacity of the system to perform better even if there are issue in cyber environment	Frequency	84	183	107	33	11	418	14	432
	Percent	19.4	42.4	24.8	7.6	2.5	96.8	3.2	100
	Frequency	83	186	106	30	14	419	13	432

Resilience in smart government organizations will improve performance and output	Percent	19.2	43.1	24.5	6.9	3.2	97	3	100
The management control factors effect resilience in smart government organizations	Frequency	81	191	117	18	13	420	12	432
	Percent	18.8	44.2	27.1	4.2	3	97.2	2.8	100
The safe environment created by risk management will enhance technical competence in smart government organizations	Frequency	96	196	90	27	11	420	12	432
	Percent	22.2	45.4	20.8	6.3	2.5	97.2	2.8	100
The overall performance of my organization will improve with the introduction or smart Governance resilience and risk management interventions	Frequency	88	201	106	17	8	420	12	432
	Percent	20.4	46.5	24.5	3.9	1.9	97.2	2.8	100
I think the organization will perform extremely well in the core functions because of the introduction of an smart Governance resilience and risk management policies	Frequency	89	196	102	21	12	420	12	432
	Percent	20.6	45.4	23.6	4.9	2.8	97.2	2.8	100
The institution will greatly benefit from the new knowledge base and new skill requirements, occasioned by the introduction of an smart Governance risk management strategy	Frequency	94	200	93	22	12	421	11	432
	Percent	21.8	46.3	21.5	5.1	2.8	97.5	2.5	100
The smart governance Platform and associated Risk Management interventions will improve the overall satisfaction of the students and staff to the institution's service provision.	Frequency	74	217	106	15	10	422	10	432
	Percent	17.1	50.2	24.5	3.5	2.3	97.7	2.3	100
The introduction of the smart Governance risk management will result in higher profit margins and reduced operational costs.	Frequency	71	182	119	37	10	419	13	432
	Percent	16.4	42.1	27.5	8.6	2.3	97	3	100
	Frequency	79	198	109	25	8	419	13	432

There are differences between smart government organizations in terms of using resilience and cyber security risk management	Percent	18.3	45.8	25.2	5.8	1.9	97	3	100
The capability factors affect resilience in smart government organizations	Frequency	75	179	127	25	14	420	12	432
	Percent	17.4	41.4	29.4	5.8	3.2	97.2	2.8	100
The change factors effect resilience in smart government organizations	Frequency	79	177	129	24	12	421	11	432
	Percent	18.3	41	29.9	5.6	2.8	97.5	2.5	100
The vulnerability factors effect resilience in smart government organizations	Frequency	92	191	109	17	10	419	13	432
	Percent	21.3	44.2	25.2	3.9	2.3	97	3	100
The resilience framework is about detecting, preventing, and recovering from a cyber-attack	Frequency	95	187	108	19	10	419	13	432
	Percent	22	43.3	25	4.4	2.3	97	3	100
The forces of change cause vulnerabilities that provoke the need for resilience in organizations	Frequency	75	181	124	29	12	421	11	432
	Percent	17.4	41.9	28.7	6.7	2.8	97.5	2.5	100
The implementation of balanced resilience can result in improved performance	Frequency	95	196	97	20	12	420	12	432
	Percent	22	45.4	22.5	4.6	2.8	97.2	2.8	100
Unbalanced resilience in organizations can impose excessive frisks and erode profitability	Frequency	85	200	103	20	13	421	11	432
	Percent	19.7	46.3	23.8	4.6	3	97.5	2.5	100
The resilience can help organizations in evaluating risks and challenges involved at multiple levels	Frequency	98	195	96	17	15	421	11	432
	Percent	22.7	45.1	22.2	3.9	3.5	97.5	2.5	100

Statement: Risk Management in Information Communication Technology Applications will bring about a lot of benefits to the Institution

Twenty-nine percent of respondents strongly agreed, 49% agreed, 15% were not sure, 1.4% disagreed, and the remaining 2.8% disagreed. It is demonstrated that the majority of participants agreed that risk management in ICT applications will bring about a lot of benefits to the institution.

Statement: Smart Governance organizations are need better resilience and risk management policies

Twenty-nine percent of respondents strongly agreed, 50% agreed, 13% were not sure, 3% disagreed, and the remaining 1.9% strongly disagreed. It is demonstrated that the majority of participants agreed that Smart Governance organizations require better resilience and risk management policies.

Statement: Resilience management in Smart Government organizations will bring flexibility in cyberspace, and continuity of organizational functions despite cyber-attacks

Twenty-two percent of respondents strongly agreed, 47% agreed, 23.9% were not sure, 3.9% disagreed, and the remaining 1.4% strongly disagreed. It is demonstrated that the majority of participants agreed that resilience management in Smart Government organizations will bring flexibility in cyberspace, and continuity of organizational functions despite cyber-attacks.

Statement: There are more risks than benefits attributed to the whole process of Smart Governance

Thirteen percent of respondents strongly agreed, 32% agreed, 28% were not sure, 19% disagreed, and the remaining 4.2% strongly disagreed. It is demonstrated that the majority of

participants agreed that there are more risks than benefits attributed to the whole process of Smart Governance.

Statement: The changing environment and relations in society require smart government organizations in the UAE to focus on better resilience policies

Twenty-two percent of respondents strongly agreed, 25% agreed, 45% were not sure, 20% disagreed, and the remaining 4.6% strongly disagreed. It is demonstrated that the majority of participants agreed that the changing environment and relations in society require smart government organizations in the UAE to focus on better resilience policies.

Statement: Smart Governance introduces improved techniques and processes to the organization

Twenty-six percent of respondents strongly agreed, 50% agreed, 14.6% were not sure, 4.9% disagreed, and the remaining 2.1% strongly disagreed. It is demonstrated that the majority of participants agreed that Smart Governance introduces improved techniques and processes to the organization.

Statement: Smart governance organizations should consider implementation of effective resilience

Twenty-two percent of respondents strongly agreed, 50% agreed, 18% were not sure, 4% disagreed, and the remaining 2.8% strongly disagreed. It is demonstrated that the majority of participants agreed that Smart governance organizations should consider implementation of effective resilience.

Statement: Better management control in smart governance organizations can create capabilities and resilience against cyber attacks

Nineteen percent of respondents strongly agreed, 39% agreed, 29% were not sure, 3.5% disagreed, and the remaining 4% strongly disagreed. It is demonstrated that the majority of participants agreed that better management control in Smart Governance organizations can create capabilities and resilience against cyber-attacks.

Statement: Multiple layers to foster resilience will result in shorter network and system downtimes

Nineteen percent of respondents strongly agreed, 39% agreed, 29% were not sure, 5.8% disagreed, and the remaining 3.5% strongly disagreed. It is demonstrated that the majority of participants agreed that multiple layers to foster resilience will result in shorter network and system downtimes.

Statement: The government is focusing on cyber resilience to avoid threats in changing cyber environment

Seventeen percent of respondents strongly agreed, 45% agreed, 27% were not sure, 4.4% disagreed, and the remaining 3.5% strongly disagreed. It is demonstrated that the majority of participants agreed that the government is focusing on cyber resilience to avoid threats in changing cyber environment.

Statement: Smart Governance Platforms is generally vulnerable to common attacks such as Denial of Service Attacks.

Precisely 15.7% of respondents strongly agreed, 35% agreed, 35% were not sure, 10% disagreed, and the remaining 1.2% strongly disagreed. It is demonstrated that the majority of

participants agreed that Smart Governance Platforms is generally vulnerable to common attacks such as Denial of Service Attacks.

Statement: Smart Governance Platforms will result in a greater uptake of cloud based resources by the average person

Precisely 18.7% of respondents strongly agreed, 43% agreed, 28% were not sure, 3.9% disagreed, and the remaining 3.9% strongly disagreed. It is demonstrated that the majority of participants agreed that Smart Governance Platforms will result in a greater uptake of cloud based resources by the average person.

Statement: Smart Governance Platforms will be able to accurately predict the unique needs of individual students, instead of providing generic answers.

Nineteen percent of respondents strongly agreed, 44% agreed, 25% were not sure, 2.8% disagreed, and the remaining 2.1% strongly disagreed. It is demonstrated that the majority of participants agreed that Smart Governance Platforms will be able to accurately predict the unique needs of individual students, instead of providing generic answers.

Statement: The current ICT policies and frameworks that guide the system are inadequate due to lack of resilience polices and risk management strategy

Precisely 14.1% of the respondents m strongly agreed, 41% agreed, 31% were not sure, 7% disagreed, and the remaining 3% strongly disagreed. It is demonstrated that the majority of participants agreed that the current ICT policies and frameworks that guide the system are inadequate due to lack of resilience polices and risk management strategy.

Statement: Smart governance organizations of the UAE need effective policies and frameworks for the system

Nineteen percent of respondents strongly agreed, 47% agreed, 22% were not sure, 5% disagreed, and the remaining 3% strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants agreed that Smart Governance organizations of the UAE need effective policies and frameworks for the system.

Statement: The smart Governance Platform will enable the institution to maintain its competitive advantage across all spheres of service provision.

Precisely 18.1% of respondents strongly agreed, 47% agreed, 25% were not sure, 4.9% disagreed, and the remaining 2.3% strongly disagreed. It is demonstrated that the majority of participants agreed that the smart Governance Platform will enable the institution to maintain its competitive advantage across all spheres of service provision.

Statement: The smart Governance Platform will improve service consistency, continuity and overall quality at a minimal cost.

Twenty percent of respondents strongly agreed, 43% agreed, 24% were not sure, 6.9% disagreed, and the remaining 2.3% strongly disagreed. It is demonstrated that the majority of participants agreed that the Smart Governance Platform will improve service consistency, continuity and overall quality at a minimal cost.

Statement: Risk Management interventions will prevent the institution from being exposed to costly legal proceedings in case of data breaches

Precisely 18.1% of respondents strongly agreed, 46.5% agreed, 22.6% were not sure, 7% disagreed, and the remaining 4% strongly disagreed. It is demonstrated that the majority of participants agreed that Risk Management interventions will prevent the institution from being exposed to costly legal proceedings in case of data breaches.

Statement: The smart Governance Platform will offer real time feedback and 24/7 access and resource provision.

Twenty percent of respondents strongly agreed, 42% agreed, 23% were not sure, 5% disagreed, and the remaining 3.9% strongly disagreed. It is demonstrated that the majority of participants agreed that the smart Governance Platform will offer real time feedback and 24/7 access and resource provision.

Statement: Improved risk management and resilience will enhance performance of employees

Twenty percent of respondents strongly agreed, 46% agreed, 22% were not sure, 5.6% disagreed, and the remaining 2.5% strongly disagreed. It is demonstrated that the majority of participants agreed that improved risk management and resilience will enhance performance of employees.

Statement: Risk management will be beneficial for all stakeholders

Twenty-one percent of respondents strongly agreed, 42% agreed, 24% were not sure, 7.6% disagreed, and the remaining 1.9% strongly disagreed. It is demonstrated that the majority of participants agreed that risk management will be beneficial for all stakeholders.

Statement: Resilience and Risk Management will result in better mitigation, reduction or elimination of cyber related attacks

Precisely 19.9% of respondents strongly agreed, 46% agreed, 24% were not sure, 4.4% disagreed, and the remaining 2.1% strongly disagreed. It is demonstrated that the majority of participants agreed that resilience and risk management will result in better mitigation, reduction or elimination of cyber related attacks.

Statement: Better policies for cyber resilience will help smart government organizations to recover quickly from any cyber attack

Twenty-two percent of respondents strongly agreed, 46% agreed, 21% were not sure, 4.9% disagreed, and the remaining 2.3% strongly disagreed. It is demonstrated that the majority of participants agreed that better policies for Cyber resilience will help Smart Government organizations to recover quickly from any cyber-attack.

Statement: The regularity authorities of the country should pay attention enhance infrastructure resilience in smart government organizations

Twenty-one percent of respondents strongly agreed, 47% agreed, 22% not sure, 5.3% disagreed, and the remaining 0.9% strongly disagreed. It is demonstrated that the majority of participants agreed that the regularity authorities of the country should pay attention enhance *Statement: The federal government of the UAE is aware of the importance of resilience and cyber security management in smart government organizations*

Twenty-two percent of respondents strongly agreed, 40.5% agreed, 27.5% were not sure, 5.6% disagreed, and the remaining 1.4% strongly disagreed. It is demonstrated that the majority of participants agreed that the federal government of the UAE is aware of the importance of resilience and cyber security management in Smart Government organizations.

Statement: The purpose of cyber security domain in smart government organizations is to build control for making cyberspace secure

Twenty percent of respondents strongly agreed, 47% agreed, 19% were not sure, 6.3% were disagreed, and the remaining 3.9% were strongly disagreed. It is demonstrated that the majority of participants agreed that the purpose of cyber security domain in smart government organizations is to build control for making cyberspace secure.

Statement: Smart Governance will introduce a high rate of resilience in institutional platforms and virtual services provided.

Nineteen percent of respondents strongly agreed, 44% agreed, 25% were not sure, 3.9% were disagreed, and the remaining 3% were strongly disagreed. It is demonstrated that the majority of participants agreed that Smart Governance will introduce a high rate of resilience in institutional platforms and virtual services provided.

Statement: The smart Platform will result in faster and more specific responses to stakeholders

Twenty-four percent of respondents strongly agreed, 40% agreed, 25 % were not sure, 6% disagreed, and the remaining 2.1% strongly disagreed. It is demonstrated that the majority of

participants agreed that the smart platform will result in faster and more specific responses to stakeholders.

Statement: Smart Governance Platforms will introduce more secure data storage and data management to this facility

Twenty-two percent of respondents strongly agreed, 44% agreed, 22% were not sure, 4.9% disagreed, and the remaining 3.5% strongly disagreed. It is demonstrated that the majority of participants agreed that Smart Governance Platforms will introduce more secure data storage and data management to this facility.

Statement: The smart Governance Platform will enable the institution to focus its resources and energy on core activities rather than peripheral ones.

Twenty-one percent of respondents strongly agreed, 39% agreed, 28% were not sure, 5.8% disagreed, and the remaining 1.6% strongly disagreed. It is demonstrated that the majority of participants agreed that the Smart Governance Platform will enable the institution to focus its resources and energy on core activities rather than peripheral ones.

Statement: The smart Governance Platform will result in capacity building, better knowledge transfer and the creation of new skill sets for the stakeholders.

Twenty-three percent of respondents strongly agreed, 42% agreed, 23% were not sure, 6% disagreed, and the remaining 2.8% strongly disagreed. It is demonstrated that the majority of participants agreed that the smart Governance Platform will result in capacity building, better knowledge transfer and the creation of new skill sets for the stakeholders.

Statement: Existing and evolving Cyber Security Threats will make the smart government organizations vulnerable

Eighteen percent of respondents strongly agreed, 36% agreed, 28% were not sure, 10% disagreed, and the remaining 3.9% strongly disagreed. It is demonstrated that the majority of participants agreed that existing and evolving cybersecurity threats will make the smart government organizations vulnerable.

Statement: The smart Platform may cause the institution will lose reliable and more talented staff who may not be that tech savvy, and introduce untrusted third parties.

Twenty percent of respondents strongly agreed, 38.9% agreed, 26% were not sure, 8.8% disagreed, and the remaining 3% strongly disagreed. It is demonstrated that the majority of participants agreed that the Smart Platform may cause the institution will to lose reliable and more talented staff who may not be that tech savvy, and introduce untrusted third parties.

Statement: External Service Providers for the smart Governance Platform cannot always reliable and consistent services

Precisely 17.6% of respondents strongly agreed, 39% agreed, 29% were not sure, 7% disagreed, and the remaining 1.9% strongly disagreed. It is demonstrated that the majority of participants agreed that external service providers for the Smart Governance Platform cannot always reliable and consistent services.

Statement: The introduction of the smart Governance platform may result in a dearth of interpersonal skills from minimal staff recruitment.

Precisely, 14.4% of respondents strongly agreed, 41% agreed, 30% were not sure, 7% disagreed, and the remaining 4.4% strongly disagreed. It is demonstrated that the majority of participants agreed that the introduction of the Smart Governance Platform may result in a dearth of interpersonal skills from minimal staff recruitment.

Statement: In the event of a data breach, massive volumes of sensitive data could be get exposed to the public domain.

Precisely 17.1% of respondents strongly agreed, 42% agreed, 28% were not sure, 7.4% disagreed, and the remaining 2.1% strongly disagreed. It is demonstrated that the majority of participants agreed that in the event of a data breach, massive volumes of sensitive data could be get exposed to the public domain.

Statement: Resilience and risk management in smart government organization will enhance the capacity of the system to perform better even if there are issue in cyber environment

Nineteen percent of respondents strongly agreed, 42% agreed, 24% were not sure, 7% disagreed, and the remaining 2.5% strongly disagreed. It is demonstrated that the majority of participants agreed that resilience and risk management in smart government organization will enhance the capacity of the system to perform better even if there are issue in cyber environment.

Statement: Resilience in smart government organizations will improve performance and output

Precisely 19.2% of respondents strongly agreed, 43% agreed, 24% were not sure, 6.9% disagreed, and the remaining 3.2% strongly disagreed. It is demonstrated that the majority of participants agreed that resilience in smart government organizations will improve performance and output.

Statement: The management control factors effect resilience in smart government organizations

Precisely 18.8% of respondents strongly agreed, 44% agreed, 27% were not sure, 4.2% were disagreed, and the remaining 3% were strongly disagreed. It is demonstrated that the majority of participants agreed that the management control factors effect resilience in smart government organizations.

Statement: The safe environment created by risk management will enhance technical competence in smart government organizations

Twenty-two percent of respondents strongly agreed, 45% agreed, 20% were not sure, 6.3% disagreed, and the remaining 2.5% strongly disagreed. It is demonstrated that the majority of participants agreed that the safe environment created by risk management will enhance technical competence in smart government organizations.

Statement: The overall performance of my organization will improve with the introduction or Smart Governance resilience and risk management interventions

Twenty percent of respondents strongly agreed, 46% agreed, 24% were not sure, 3.9% disagreed, and the remaining 1.9% strongly disagreed. It is demonstrated that the majority of

participants agreed that the overall performance of my organization will improve with the introduction or Smart Governance resilience and risk management interventions.

Statement: I think the organization will perform extremely well in the core functions because of the introduction of a Smart Governance resilience and risk management policies

Twenty percent of respondents strongly agreed, 45% agreed, 23.6% were not sure, 4.9% disagreed, and the remaining 2.8% strongly disagreed. It is demonstrated that the majority of participants agreed that respondents think the organization will perform extremely well in the core functions because of the introduction of a Smart Governance resilience and risk management policies.

Statement: The institution will greatly benefit from the new knowledge base and new skill requirements, occasioned by the introduction of a Smart Governance risk management strategy

Twenty-one percent of respondents strongly agreed, 46% agreed, 5.1% were not sure, 4.9% disagreed, and the remaining 2.8% strongly disagreed. It is demonstrated that the majority of participants agreed that the institution will greatly benefit from the new knowledge base and new skill requirements, occasioned by the introduction of an smart Governance risk management strategy.

Statement: The smart governance Platform and associated Risk Management interventions will improve the overall satisfaction of the students and staff to the institution's service provision.

Seventeen percent of respondents strongly agreed, 50% agreed, 24.5% were not sure, 3.5% disagreed, and the remaining 2.3% strongly disagreed. It is demonstrated that the majority of

participants agreed that the Smart Governance Platform and associated risk management interventions will improve the overall satisfaction of the students and staff to the institution's service provision.

Statement: The introduction of the smart Governance risk management will result in higher profit margins and reduced operational costs.

Precisely 16.4% of respondents strongly agreed, 42% agreed, 27.1% were not sure, 8.6% disagreed, and the remaining 2.3% strongly disagreed. It is demonstrated that the majority of participants agreed that the introduction of the Smart Governance risk management will result in higher profit margins and reduced operational costs.

Statement: There are differences between smart government organizations in terms of using resilience and cybersecurity risk management

Precisely 18.3% of respondents strongly agreed, 45% agreed, 25.2% were not sure, 5.8% disagreed, and the remaining 1.9% strongly disagreed. It it is demonstrated that the majority of participants agreed that there are differences between smart government organizations in terms of using resilience and cybersecurity risk management.

Statement: The capability factors affect resilience in smart government organizations

Precisely 17.4% of respondents strongly agreed, 41% agreed, 41.4% were not sure, 29.4% disagreed, and the remaining 5.8% strongly disagreed. It is demonstrated that the majority of participants agreed that the capability factors affect resilience in Smart Government organizations.

Statement: The change factors effect resilience in smart government organizations

Precisely 18.3% of respondents strongly agreed, 41% agreed, 29% were not sure, 5.6% disagreed, and the remaining 2.8% strongly disagreed. It is demonstrated that the majority of participants agreed that the change factors effect resilience in smart government organizations.

Statement: The vulnerability factors effect resilience in Smart Government organizations

Precisely 21.3% of respondents strongly agreed, 44.2% agreed, 25% were not sure, 3.9% disagreed, and the remaining 2.3% strongly disagreed. It is demonstrated that the majority of participants agreed that the vulnerability factors effect resilience in smart government organizations.

Statement: The resilience framework is about detecting, preventing, and recovering from a cyber-attack

Twenty-two percent of respondents strongly agreed, 43% agreed, 25% were not sure, 4.4% disagreed, and the remaining 2.3% strongly disagreed. It is demonstrated that the majority of participants agreed that the resilience framework is about detecting, preventing, and recovering from a cyber-attack.

Statement: The forces of change cause vulnerabilities that provoke the need for resilience in organizations

Precisely 17.4% of respondents strongly agreed, 41% agreed, 28% were not sure, 6.7% disagreed, and the remaining 2.8% strongly disagreed. It is demonstrated that the majority of participants agreed that the forces of change cause vulnerabilities that provoke the need for resilience in organizations.

Statement: The implementation of balanced resilience can result in improved performance

Twenty-two percent of respondents strongly agreed, 45% agreed, 22.5% were not sure, 4.6% disagreed, and the remaining 2.8% strongly disagreed. It is demonstrated that the majority of participants agreed that the implementation of balanced resilience can result in improved performance.

Statement: Unbalanced resilience in organizations can impose excessive frisks and erode profitability

Precisely 19.7% of respondents strongly agreed, 46% agreed, 23.8% were not sure, 4.6% disagreed, and the remaining 3% strongly disagreed. It is demonstrated that the majority of participants agreed that unbalanced resilience in organizations can impose excessive frisks and erode profitability.

Statement: The resilience can help organizations in evaluating risks and challenges involved at multiple levels

Precisely 22.7% of respondents strongly agreed, 45% agreed, 22.2% were not sure, 3.9% wee disagreed, and the remaining 3.5% strongly disagreed. It is demonstrated that the majority of participants agreed that the resilience can help organizations in evaluating risks and challenges involved at multiple levels.

5.2.2. Reliability Analysis

Table 5.24: Reliability analysis

Variables	Alpha
Management Control Factors	0.852
Capability Factors	0.835
Vulnerability Factors	0. 189
Change Factors	0.802
Resilience in Smart government Organizations	0.850

As per Table 24 above, it can be said that there is sufficient reliability in the factors used. The reliability of the Management Control Factors revealed that 85% of the data set was reliable, whereas reliability and validity of the Capability Factors revealed that 83% of the data was reliable. In addition, Vulnerability Factors accounted for a reliability of 18% in addition to reliability of 80% in the Change Factors. Furthermore, the reliability in the Resilience in Smart Government Organizations Factor was 85%.

Table 5.25: Average of all management control factors

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	1	.2	.2	.2
	Strongly Agree	38	8.8	8.8	9.0
	Agree	260	60.2	60.2	69.2
	Not Sure	125	28.9	28.9	98.1
	Disagree	6	1.4	1.4	99.5
	Strongly Disagree	2	.5	.5	100.0
	Total	432	100.0	100.0	

As per Table 25 above, it can be said that there is sufficient reliability in the factors used. The reliability of the Average Management Control Factors revealed that 100% of the data set was reliable. The majority (60.2%) agreed with the statement.

Table 5.26: Average of all variables related to resilience in smart government organizations

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	1	.2	.2	.2
	Strongly Agree	40	9.3	9.3	9.5
	Agree	277	64.1	64.1	73.6
	Not Sure	108	25.0	25.0	98.6
	Disagree	3	.7	.7	99.3
	Strongly Disagree	3	.7	.7	100.0
	Total	432	100.0	100.0	

As per Table 26 above, it can be said that there is sufficient reliability in the factors used. The reliability of the average of all variables related to resilience in e-government organizations revealed that 100% of the data set was reliable. The majority (64.1%) agreed with the statement.

Table 5.27: Average of all capabilities factors

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	1	.2	.2	.2
	Strongly Agree	37	8.6	8.6	8.8
	Agree	255	59.0	59.0	67.8
	Not Sure	126	29.2	29.2	97.0
	Disagree	12	2.8	2.8	99.8
	Strongly Disagree	1	.2	.2	100.0
	Total	432	100.0	100.0	

As per Table 27 above, it can be said that there is sufficient reliability in the factors used. The reliability of the Average Management Control Factors revealed that 100% of the data set was reliable. The majority (59%) agreed with the statement.

Table 5.28: Average of all vulnerability factors

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	5	1.2	1.2	1.2
	Strongly Agree	32	7.4	7.4	8.6
	Agree	226	52.3	52.3	60.9
	Not Sure	160	37.0	37.0	97.9
	Disagree	7	1.6	1.6	99.5
	Strongly Disagree	2	.5	.5	100.0
	Total	432	100.0	100.0	

As per Table 28 above, it can be said that there is sufficient reliability in the factors used. The reliability of the Average Management Control Factors revealed that 100% of the data set was reliable. The majority (52.3%) agreed with the statement.

Table 5.29: Average of All Change Forces Factors

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	2	.5	.5	.5
	Strongly Agree	44	10.2	10.2	10.6
	Agree	256	59.3	59.3	69.9
	Not Sure	121	28.0	28.0	97.9
	Disagree	8	1.9	1.9	99.8
	Strongly Disagree	1	.2	.2	100.0
	Total	432	100.0	100.0	

As per Table 29 above, it can be said that there is sufficient reliability in the factors used. The reliability of the Average Management Control Factors revealed that 100% of the data set was reliable. The majority (59.3%) agreed with the statement.

Table 5.30: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.954
Bartlett's Test of Sphericity	Approx. Chi-Square	6593.744
	df	666
	Sig.	.000

The sample shows that there are five factors explaining the variance in the study. It shows significant adequacy (.000) which is less than (0.05).

Table 5.31: Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	14.037	37.937	37.937	13.506	36.503	36.503	4.137	11.182	11.182
2	1.667	4.505	42.442	1.133	3.061	39.564	3.954	10.687	21.870
3	1.564	4.227	46.669	1.058	2.860	42.424	3.616	9.774	31.644
4	1.225	3.310	49.979	.715	1.933	44.357	2.540	6.864	38.508
5	1.059	2.862	52.841	.538	1.454	45.811	1.676	4.530	43.038
6	1.033	2.793	55.634	.518	1.400	47.212	1.544	4.174	47.212
7	.903	2.442	58.076						
8	.889	2.403	60.479						
9	.806	2.177	62.656						
10	.794	2.145	64.801						
11	.780	2.107	66.909						
12	.740	2.001	68.910						
13	.708	1.914	70.824						
14	.684	1.849	72.673						
15	.667	1.804	74.477						
16	.662	1.790	76.267						

17	.620	1.677	77.944						
18	.599	1.618	79.562						
19	.582	1.573	81.135						
20	.543	1.468	82.603						
21	.521	1.409	84.013						
22	.494	1.336	85.349						
23	.469	1.267	86.615						
24	.452	1.221	87.837						
25	.433	1.170	89.007						
26	.433	1.169	90.176						
27	.417	1.126	91.302						
28	.383	1.036	92.339						
29	.375	1.012	93.351						
30	.366	.990	94.341						
31	.348	.942	95.283						
32	.336	.909	96.192						
33	.327	.884	97.075						
34	.302	.816	97.891						
35	.288	.778	98.670						
36	.269	.728	99.397						
37	.223	.603	100.000						

Extraction Method: Maximum Likelihood.

The total cumulative percentage of variance explained by the factors of this study is equal to 47.212

Table 5.32: Goodness-of-fit Test

Chi-Square	df	Sig.
725.302	459	.000

According to the Chi-square test the model shows goodness of fit, meaning that the number of factors is sufficient to answer the research questions.

Table 5.33: Rotated Factor Matrix[a]

	Factor					
	1	2	3	4	5	
x48	.637					
x51	.593					
x52	.566					
x49	.540					
x32	.531					
x53	.527					
x46	.518					
x50	.479					
x47	.478					
x41		.657				
x43		.603				
x42		.592				
x40		.543				
x44		.433				
x39		.412				
x20		.408				
x54		.365				
x28		.360				
x1			.545			
x			.539			
x31			.525			
x7			.469			
x15			.466			
x3			.431			
x16			.431			
x19			.416			
x29			.349			
x8				.626		
x22				.564		
x24				.450		
x23				.429		
x27				.406		
x26					.460	
x38					.423	

x6					.430		
x2					.406		
x21					.355		

Extraction Method: Maximum Likelihood.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 18 iterations.

All the items were uploaded in the questionnaire on the exploratory factor analysis using the maximum likelihood method, which is used in the case of this study when the relationship between the variables is linear.

Table 5.34: Correlations

		REGR factor score 1 for analysis 1	REGR factor score 2 for analysis 1	REGR factor score 3 for analysis 1	REGR factor score 4 for analysis 1	REGR factor score 5 for analysis 1	REGR factor score 6 for analysis 1
REGR factor score 1 for analysis 1	Pearson Correlation	1	.096	.109*	.058	.088	.008
	Sig. (2-tailed)		.062	.033	.258	.084	.876
	N	382	382	382	382	382	382
REGR factor score 2 for analysis 1	Pearson Correlation	.096	1	.077	.064	.134**	.072
	Sig. (2-tailed)	.062		.131	.210	.009	.162
	N	382	382	382	382	382	382
REGR factor score 3 for analysis 1	Pearson Correlation	.109*	.077	1	.129*	.080	.103*
	Sig. (2-tailed)	.033	.131		.011	.119	.044
	N	382	382	382	382	382	382
REGR factor score 4 for analysis 1	Pearson Correlation	.058	.064	.129*	1	.090	.138**
	Sig. (2-tailed)	.258	.210	.011		.079	.007
	N	382	382	382	382	382	382

REGR factor score 5 for analysis 1	Pearson Correlation	.088	.134**	.080	.090	1	.072
	Sig. (2-tailed)	.084	.009	.119	.079		.159
	N	382	382	382	382	382	382
REGR factor score 6 for analysis 1	Pearson Correlation	.008	.072	.103*	.138**	.072	1
	Sig. (2-tailed)	.876	.162	.044	.007	.159	
	N	382	382	382	382	382	382

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

5.2.3.Regression Analysis

Table 5.35: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.222	.073		3.041	.003
	Average of all management control factors	.335	.051	.343	6.548	.000
	Average of all capabilities factors	.217	.045	.228	4.797	.000
	Average of all vulnerability factors	.109	.036	.120	3.065	.002
	Average of All Change Forces Factors	.214	.044	.225	4.841	.000

a. Dependent Variable: Average of all variables related to resilience in e-government organizations

Table 35 above shows the effect of each independent variable on the dependent variable (resilience) being observed in this research at the standardized coefficient. The relationship between management control and resilience is .343 which is significant at below .001.

The more coefficient at .343 management control is the highest impact or affect resilience. The second the capabilities at .228, the third is forces of change at .225 the last is vulnerability at .120.

5.2.4. Hypothesis Testing

The researcher tried to test the hypotheses of the research in many ways in the previous chapters, theoretically and from the Smart Government online gate and analysing their websites, along with a systematic review of the literature and the context of Smart Government resiliency and cybersecurity risk management. In this section the hypotheses will be tested numerically and scientifically, rather than just assuming things. The specific hypotheses of this thesis that were tested according to the variables and factors that affect Smart Government resilience the most and

the ones that have lower impact on the resilience or do not have any impact, are as follows: H1: The capability factors affect resilience in Smart Government organizations. H2: The change factors affect resilience in Smart Government organizations. H3: The management control factors affect resilience in Smart Government organizations. H4: The vulnerability factors affect resilience in Smart Government organizations.

Table 5.36: Correlations

Correlations					
Constructs	**1**	**2**	**3**	**4**	**5**
Management control factors	1				
Resilience	.759**	1			
Capabilities factors	.787**	.713**	1		
Vulnerability factors	.610**	.599**	.533**	1	.660**
Change Forces Factors	.729**	.707**	.673**	.660**	1

**. Correlation is significant at the 0.01 level (2-tailed). Sample size = 432

The table above shows significant correlation between the variables. It also demonstrates that all the factors that were suggested by the researcher do have a great impact on Smart Government resilience, although they vary from high to low, they have a significant correlation between each other.

Table 5.37: Model Summary[b]

Model	R				Change Statistics	

		R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change	Durbin-Watson
1	.808[a]	.653	.650	.378	.653	201.230	4	427	.000	1.987

a. Predictors: (Constant), Average of All Change Forces Factors, Average of all vulnerability factors, Average of all capabilities factors, Average of all management control factors.

b. Dependent Variable: Average of all variables related to resilience in Smart Government organizations.

There is a significant relationship between the means of two variables, as the sig. values were under 0.05.

Table 5.38: ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	114.873	4	28.718	201.230	.000[b]
	Residual	60.939	427	.143		
	Total	175.813	431			

a. Dependent Variable: Average of all variables related to resilience in Smart Government organizations.

b. Predictors: (Constant), Average of All Change Forces Factors, Average of all vulnerability factors, Average of all capabilities factors, Average of all management control factors.

There is a significant relationship between the means of two variables, as the sig. values were under 0.05. Hence bringing any change in the independent variable would result in a change in the dependent variables.

Nevertheless, after analysing each variable and testing each factor's impact on Smart Government, by assigning a group of items to each hypothesis for that purpose, the researcher summarized the result on each hypothesis as follows:

Table 5.39: Summary of hypotheses and impact

Hypothesis details	Impact on resilience	Priority	Survey items	Outcomes
The capability factors effect resilience in Smart Government organizations.	the capabilities factors have 22% impact on the resilience	second	10	Supported
The forces of change factors effect resilience in smart government organizations.	the forces of change factors have 22% impact on the resilience	third	11	supported
The management control factors effect resilience in Smart government organizations.	The management control factors have 34% impact on the resilience	first (a priority)	12	Supported
The vulnerability factors effect resilience in Smart government organizations.	The vulnerability factors have 12% impact on the resilience	fourth	10	Supported

The table above shows that the management control factors hold the priority among all factors that affect Smart Government resilience. These are followed by the capability factors, which makes sense because management control creates capabilities for the system of Smart Government, which increase the resiliency level. The correlation table shows a significant correlation between these two variables, which supported the theoretical context of this thesis.

As per the table above, the forces of change affect Smart Government resilience at 22%, which is significant considering the great focus on the forces of change factor in the literature. Whereas many authors, scientists and risk managers highlighted the role of vulnerability factors in the past, recently they emphasize the role of the change factor as the new concern in the whole process of resiliency and cybersecurity risk management. The table shows that vulnerability factors have the least impact on resilience among all factors, which is why this result supports the theoretical context of the thesis which suggested that the concern shifted through time, from talking about vulnerability factors to emphasizing the role of change factors on cybersecurity risk management and resilience; this is due to many factors, such as advancements in the computerization and programming world and not having connectivity or vulnerability issues. While in recent times the biggest challenge is to cope with change, and to learn how to absorb it in order to survive in this constant changing world. We are witnessing a rapid change, in every aspect and we have to take attacks and opportunities as serious risks to our systems, in order to regain composure following a significant change in our system; we need to use a professional resilience framework.

5.3. Summary

The responses to the survey that were submitted during the data collection phase of this study were summarised in this chapter and found to be positive. Most of the participants selected the options of ‘agree’ and ‘strongly agree’, which reveals their apparent agreement with the questions asked. There were more than 400 participants, which comprised of both males and females. Most participants were female and the study results show that the survey participants were aware of Smart Government and the initiatives associated with it. Based on the survey

analysis, it was found that resilience is a very important factor that can help to determine the risk and opportunity and support the stability of Smart Government in the UAE.

CHAPTER SIX– DISCUSSION

6. Introduction to the chapter

The aim of this chapter is to present an evaluation of the results obtained from the survey and compare those results with the literature that was investigated in the literature review chapter. The chapter has been divided into different parts, including a discussion on both the research questions and research objectives. Meanwhile, the discussion on the research hypotheses is developed and a summary of the entire chapter provided.

6.1. Discussion on Research Questions and Objectives

This research objectives are as follows:

Objective 1: To determine and identify the components of the resilience framework.

Objective 2: To elaborate upon the risk management frameworks suitable for cybersecurity in Smart Government.

Objective 3: To evaluate the existing resilience frameworks and identify the areas of potential improvement.

Objective 4: To develop a sound model for Smart Government organizations, on the measurement of resilience.

This Research will be guided by two main questions:

Q1: What are the components of the resilience framework?

Q2: What are the evaluation criteria of the existing frameworks on the measurement of resilience?

The division of research questions and their breakdown into the research objectives helped the researcher to complete the entire work. Based on the research questions embedded by the research objectives, the researcher developed themes, survey questions, and consulted the relevant literature. The findings obtained from both the survey questions and literature review are further discussed. Based on the findings, the researcher has developed themes followed by the research questions, research objectives and the hypotheses. The main findings and surprises are discussed in detail in the following table.

Table 6.40: Primary research findings

Cyber resilience	Main findings

The importance of Smart Government	What was surprising, most participants agreed that there are more risks than benefits to the whole project of Smart Government, which implicates the high level of concern about security and privacy issues among the public. In light of this, this research seeks to emphasize the importance of Smart Government projects. The following observations regarding Smart Government are made in this research: 1- It helps in rethinking the democracy in the new millennium. 2- It consists of a lot of challenges, such as transparency, equity and privacy. 3- It facilitates the daily processes of individuals and companies, which can change the perception of individuals regarding the role of recent governments in improving their environment. Smart Government also works on the development of different policies related to the validity and security of information, through the use of new technologies. 4- It fosters the idea of electronic government, which has allowed the UAE to be an international investment destination, even in the media, commerce and economic arenas. 5- Through its massive investments in new technologies and the launch of this project in the early 1990s, the UAE attracted international companies in ICT, amongst other sectors.

	6- Government projects represent a remarkable movement towards a new century. Smart Government in the UAE is setting the pace and acting as a global benchmark, especially when it comes to electronic services. 7- The Smart Government project of the UAE has a strong impact in the IT field and also significantly helps in the advancement of IT strategies and processes. 8- Furthermore, the survey respondents agreed that the project provides financing for important projects in the ICT sector that are related to this field, such as Internet City, a free trade zone and free trade zones for electronic commerce. It also financed media projects, which have been successful through its various media channels and electronic services, which have helped facilitate the process of communication with the public. 9- The above reasons are recognized as reasons why research should explore business profitability, and financial loss in the Smart Government resilience model. 10- It saves time and effort, which encourages efficiency and provides a customer-centred approach. 11- Meanwhile, the findings indicated that the Smart Government system of Dubai innovates new processes and governmental services.

	12- Various investments are currently being made to support the Smart Government project. 13- By taking advantage of ICT, cities with a highly integrated telecommunications infrastructure are established as knowledge-based economies, which plays an important role in improving service efficiency and cybersecurity. 14- Smart Governments expect to consolidate their achievements by creating an organizational culture of cybersecurity and the creation of systems with high resistance to risk and to ensure sustainable growth in public and private industries. 15- At the same time, it creates a powerful infrastructure and expands its services.

Table 6.41: Primary research findings – Hypotheses

Cyber resilience	**Main findings**
Smart Government using risk management and resilience H1	The Smart Government is using risk management strategies but has not yet reached the resilience maturity level. The Smart Government launched its resilience strategy earlier this year and

	it has been expected to reach its maximum maturity when the project is completed by the end of 2020.
Maturity level of Smart Government has reached the resilience stage H2	The Smart Government, at least in the UAE, is not yet fully mature. After conducting this survey and studying Smart Government strategies it can be said that there is a lot to do to reach the resilience maturity level; the UAE system is still in the risk management level (proactive). The levels are: 1- reactive; 2- proactive; 3- resilient (mature)
Risk management and resilience are different to each other	Despite other studies and authors stating that resilience is a tool of risk management. The study reveals that these two notions have major differences and are considered two different domains. In fact, enterprise resilience can be more affective in these cases of technological breakthroughs than risk management. The differences are: 1- resilience is more than just risk management, rather it is a broad phenomenon that entails every change that an organization faces and not just a crisis; 2- risk management is a strategy to be followed in times of crisis, whereas resilience enables organizations to exercise resiliency plans in a systematic way to increase readiness in the face of all business disruptions;

	3- resilience will form a complete picture or vision right after the implementation of the resiliency scoring plan. The planners will set specific goals and strategy of what organizational resilience will look like after performing the resiliency scoring in business continuity plans; 4- the suggested methodology of resiliency scoring will help improve the ability to evaluate the quality of an organization's business plan; 5- whereas the resiliency method can help in removing any undesirable ambiguity besides offering multiple suggestions to enhance the quality of the plan which were not previously noticed by planners; 6- risk management deals with potential risks or disastrous change, whereas resilience has the ability to address both the positive and negative forces of change; 7- risk management strategies are different to resiliency plans, which have the ability to be exercised over and over again until the maximum maturity level of system resilience is reached.
Awareness and culture of Smart Government in the UAE towards resilience and	The study reveals that the majority of the participants are aware of the risk management and resilience framework, and the culture is ready to adopt the enterprise resilience model, because the level of awareness and culture regarding the importance of

readiness level to apply resilience	this plan is already established among the users of the Smart Government system. However, as stated earlier, they are still in the risk management stage and have not yet reached the resilience level in the sense of their current maturity status.

Table 6.42: Primary research findings – Framework

Cyber resilience	**Main findings**
What is resilience?	The ability of an organization to absorb change.
Methodological framework	The study shows that the conceptual model of the research is explained very well at 65% (see the model summary in statistical analysis).
Specific hypotheses	The study tested all specific hypotheses and measured the relationship between the independent variables and the dependent variable (resilience) and the impact of these variables on resilience in both direct and bath relationships (the bath relationship is when forces of change provoke vulnerabilities and affect resilience and the direct relationship is when forces of change affect resilience directly).
The impact of the independent	The impact of 1- forces of change, 2- vulnerabilities, 3- management control, and 4- capabilities on resilience turns out to

variables on the dependent variable	be significant and the average of the answers that agreed on this impact for each variable is high for all the factors.
Forces of change	Harnessing the experience and embracing opportunities is the best resilient case scenario against forces of change.
Vulnerability factors	1- Vulnerability factors include turbulence, deliberate threats, external pressures, resource limits, sensitivity, connectivity, and disruption by supplier or buyer of the product/service; 2- the concern is shifted from vulnerability factors after witnessing a rapid and huge development in technologies. The concern became less about connectivity issues because it has been discovered that the fault does not reside with technology but with human error. Consequently, it is people who should be held accountable during a cybersecurity crisis; 3- the concern became more on management control and forces of change factors to address the new issues of cybersecurity, as no matter how many IT instruments are applied to a system the risk still exists and requires managerial, not technical, solutions in most cases.
The management control	Management control turns out to be the most independent variable that has an impact on resilience. It creates capabilities for proper

	functioning and helps in achieving and measuring resilience against cyber incidents.

Table 6.43: Primary research findings – the importance of resilience

Cyber resilience	**Main findings**
The importance of resilience for Smart Government	The study reveals resilience plans are very important to Smart Government for the following reasons: 1- Protecting Smart Government from long-term consequences of cyber-attacks which are of great importance from an economic point-of-view; 2- Protecting organizations from loss of all types of intellectual property; 3- Promoting integrity, confidentiality and availability. These are cybersecurity information security objectives. 4- However, some of these cybersecurity goals are mutually exclusive, for example, the easy availability of information makes the confidentiality of information more complex; the role of resilience is important here. 5- Offering a backup system solution that is not electronic and is not associated with any electronic system. This offers reviewing the crisis plan with respect to the Smart Government initiative, in

	addition to being part of an alliance with key functions and/or players. 6- The NIST Plan included framework design workshops that can receive feedback from its current users. 7- A skeleton key, which should recognize several levels of protection against potential threats. To exit the target zone, an individual needs to create a series of solutions, constantly assessing risk and measuring vulnerabilities in order to be able to cope with them. 8- The factors were divided into the dynamic risks into two main parts of the same structure: 1) the risk management section, which consisted of recognizing vulnerabilities, predicting threats, and comprehending the consequences; 2) planning and prevention, when the stages of work and implementation could begin, depending on factors affecting the risk, to prevent the appearance of cyber-attacks. 9- The need for a stronger, more modern structure is imperative. The good news in this relatively new cybersecurity is that it is based on risks, which means it can provide maximum security for the security systems. 10- The research indicated that teaching students during a school period would lead to many years of IT experience and give them enough time to develop a complex and high level of IT skills.

	11- The only way to be prepared is to make sure that the information infrastructure and IT staff are ready, which can only be realized through a cybersecurity scientific base and special cybersecurity skills. 12- The agency must control potential risk, otherwise it faces problems of trust from stakeholders and customers. 13- The research highlighted the gap in personal and cybersecurity literature, where the relationship between the citizen and the organization should be defined, and the responses of the organizations are very limited. 14- A review of cybersecurity revealed the absence of a number of models aimed at protecting cybersecurity. There are only two or three structures and articles due to the lack of research on this relatively new topic. 15- Despite all the most innovative IT tools and applications, there is always a chance that they could be broken. A resilience approach is one of the most useful strategies in this environment. 16- Shown that integration of privacy and cybersecurity can benefit organizations by increasing customer confidence, providing more standardized information sharing and streamlining operations for legal regimes 17- That organizations should prioritize risks and activities, recognizing the sustainability of risks to cybersecurity, which can

	also help organizations have a complete idea and make the right decisions about financial and management costs in cybersecurity.
The importance of resilience for smart government	18-This structure provided a common language for understanding, managing, and expressing the concept of the life cycle of cybersecurity risk, both inside and outside. Hence, it can be stated that the IT infrastructure and its security is the basic component for the Smart government systems regardless of the country or nations, they are being adopted. 19- the resilience refers to the characteristics of an organizational system to withstand stress and overcome external or internal threats or attacks, and this applies to the system as a whole, and not to its individual parts 20- To assess the sustainability of an organizational system, the capabilities and interactions of various parts of an organization after a destructive event are considered decisive how they interact and communicate with each other. Sustainable organizations encourage advisory and joint decisions 21- the rules are not just dictated, but encourage employees to behave in the way that is consistent with the expectations of customers.

	22-the rules are not just dictated, but encourage employees to behave in the way that is consistent with the expectations of customers. 23- sustainability is the ability of an organization to predict and recover from changes, events, and events of any unforeseen events. It is believed that this is more than just risk management and does not entail a crisis-related organization or supply chain. Rather, it is a widespread phenomenon that entails all the changes that the organization faces, and not just the crisis 24- resilience is an alternate concept of sustainability of a business organization is the ability to open and use opportunities against competitors by taking risks 25- sustainability in a business context refers to overcoming the problems largely dependent on planners that are distributed throughout the organization to create executive strategies, as well as significant leadership involvement 26-resilience is the ability to anticipate and undergo change, not only overcome but also evolve because of its existance. 27-The researchers talked about the different features that each organization must apply to be able not only to overcome this change, but also to be resilient to it, knowing what happened and what is happening, and what is yet to come, to be well prepared in accordance with scientific standards.

	28-the concreteness of the plans for resilience and sustainable development was also confirmed by the survey participants of our study. Usually, in the plans and programs in most organizations, there are elements of the standards of textbooks, but only some of them are innovative and detailed, which could create a large gap between what is happening in reality and what was indicated in these plans 29- it has been found that the main criteria here are the ability to select the most distinctive information in terms of business continuity, and then document it, benefit from it, use it properly, develop it and share it with members of an organization.
The importance of resilience for smart government	30- the idea of recovery and the thrive to any disruptive event is a standard set of documented plans. 31- Such plans are called Failover Plans, which allowed the organizations to mitigate potential risk by giving them the opportunity to implement such a plan on a systematic basis in order to increase preparedness for all business failures 32- the resistance team differ from risk management team because of the assessment, in the case of resilience, the assessment depends on the content analysis of the documented plans.

	33- it describes the operational improvements related to business processes, as well as products and services of the organization as well as with people and the control mechanism. 34- with increasing the complexity the of supply chain due to globalization of organization, the resilience came to avoid reputational risk, operational risk that derives from this situation. 35- sustainable and resilience means having alternatives to counter failure. 36- resiliency and sustainability are perceived as a new quality for a professional system. 37- to insure cyber resilience and to keep it safe from any cyber-attack along with embracing every opportunity to employ new IT products and programs to its system without fear of change or risk of weakening the system because once you reach the maturity level of resiliency then you can harness your experience and embrace every opportunely out there to keep your business sustained. 38- the security of systems could be achieved effectively in a "non-computable" way by applying up-to-date methods with the new systems demands in the risk arena. 39- resilience has been described as the solution to rapid change, unexpected events and complexity.

	40- resilience has developed across different discipline as a universal mode of considering the relationship between some unexpected subjects and their highly complex environment such as smart government. 41- resilience helps understand the society as a whole system that has changing relations and changing environment. 42- As compared to risk analytics that focus on prevention risks and prepared for disruptive future, resilience combines present with future, and deals with insecurity and risks.

Table 6.44: Primary research findings – the risks of absent resilience

Cyber resilience	**Main findings**
The risks of the absent of cyber resilience in Smart Government	Failing in resiliency plans will stop the innovation process in the Smart Government organization and will lead to financial loss and in most cases the death of its business. Change is a continuous phenomenon across the globe, and resilience is the ability of an organization to absorb that change and even prosper post-trauma. Which will help in business continuity and the survival is not enough you need to learn and prosper from this change.

	The problems will remain the same if we continue using the current system of risk management which does not have a firm requirement to maintain the right level of security.
Resilience is a business issue	After studying the existing frameworks and analysing the survey it has been found that cyber resilience is a business issue which determines the survival of a business and will define business continuity and will lead a business loss, as well as affecting its performance in case of unbalanced resilience.
Cybersecurity is human errors not technical. Cyber resilience is beyond the IT domain	To start with, people are the ones who commit cyber-attacks and people participate in this where most highly qualified employees already have a criminal record, because they know their ways around information technology. This is why organizations such as Smart Governments should be careful when hiring them. This is primarily as the greater risk comes from within, and humans can be responsible for weak passwords and sharing classified information through their personal devices.

	The study reveals that cybersecurity is beyond the IT domain. The components of Smart Government consists of people, processes and technology. The first and second one involves human action and the third is designed by humans. In many cases the same hackers are being used to design cybersecurity programs due to their high intelligence in the IT domain. Employees also tend to use easy passwords which compromise the security of an organization's data. Furthermore, some employees also bring their personal laptops to work and transfer their own information and files, which affects the privacy of their personal information. These breaches turns out to come from within the organization's employees simply because they have the access. In addition, the processes and workflows of an organization should start and end within the organizational system instead of engaging third parties, which exposes the system to further risk and potential cyber-attacks. Nevertheless in times of crisis, management should not blame others or take a long time when it comes adopting the appropriate decision. Rather, they should be aware of the smart distribution of planners

	across the organization besides keeping them highly engaged whenever a disruptive event occurs.

Table 6.45: Primary research findings – the human role

Cyber resilience	**Main findings**
Human role and the level of engagement (managerially) of planners or the resilience team	1- Hayslip (2016) suggested that an immediate response to these disasters depends on the resilience of citizens, operational commanders and those in charge of the first places, such as firefighters or emergency medical specialists, while strategic leaders can make a difference in the long-term. 2- It has been found that improving institutional quality, experience and resources are expected to lead to an increase in recovery from a crisis. 3- Sustainability is still a phased quality of the system, which can be gradually acquired and improved only through trial and error and an organization's ability to adapt and learn from its responses to future disasters and system failures.

	4- The first step in the development of sustainability is the preparation of first respondents who are well-trained to make independent decisions and work effectively in situations of critical situations with the system. 5- They must be knowledgeable and convinced of core organizational values, ethics, and clearly defined priorities for responding to a crisis in the interests of the organization. 6- The next step is business continuity planning, which includes setting up a backup centre in a remote location, which reflects current business operations in the backup storage of IT memory, as well as in the event of a disaster. An individual can use this centre to continue business operations from a remote site. 7- The third stage is joint planning with the participation of all interested parties, in which all possible threats are identified, and possible decisions are regularly reviewed to cope with the ever-changing nature of people. 8- The fourth step is the joint preparation of all stakeholders by familiarizing with the contingency plan and modelling its ability to respond to the threat. 9- The final step is to prepare a guide on how to enhance resilience in a crisis.

	10- Leadership should avoid traditional pathology of leadership in a crisis situation; for example, blaming others, waiting for facts and figures before making a decision, waiting for outside help, sticking to the original plan or spreading rumours without verification. 11- It has been found that organizational sustainability outperforms the leading positions that over the years have not been an excellent factor for a successful business, adding that enterprise resilience is the most important success factor in any business; where sustainability becomes more measurable and manageable. 12- It has been found that planners are the key to a succession of programs, not the CEOs or the leadership. 13- This is why control management is better than strategic management, wherein the first one helps in times of crisis but the second (leadership) helps organizations in the long-term. 14- Planners and developers are the key to organizational resilience and sustainability. 15- It was found that planners are key to each business continuity program; the more they are involved, the more the plan is ready for implementation at any

	moment, to fill any gap. In addition, fault tolerance assessment helps motivate planners to a goal. 16- More active participation and participation in all activities of their continuity programs and, moreover, with the support of the senior counsel is critical. The high level of participation would increase the level of commitment between planners, which can help them to strive to achieve better results in their activities. Furthermore, it can assist them to increase their confidence that they can manage their plan on a more sustainable basis than before the concept of sustainability. 17- Planner reviews are an important tool of this methodology in the arena of organizational resistance, which emphasizes the role of a sustainability assessment, which gives them a great value. 18- Resilience in Smart Government initiative cannot only survive in the face of change but also benefit from this and show a great example in the market. 19- This can be achieved through greater returns from young people and their new thinking, which will create a more sustainable environment in such Smart Organizations.

	20- Planners should focus on the lifecycle of the program, which should consist of an assessment stage and then a planning stage, and then carry out exercises to reach a level of maturity and assist in quick recovery to ensure the continuation of such a program. 21- To help the recovery process reach a level of maturity, planners need to be more active and ensure that risks are constantly identified and evaluated, as well as documenting resiliency plans, to ensure resilience to potential obstacles or even natural disasters. 22- Assistance helps in evaluating the content of such continuity plans, which aim to guide the planning process to the maturity stage. This type of assessment can maintain compatibility and visibility in addition to improving compliance in a business continuity program. 23- However, attractive planners and executives are not an easy task. Hence, this is a complex task, while the company's culture is not ready for such a decision or change. 24- Culture influences strategy, while in some cases leaders are isolated from employees and find it difficult to be more involved or even associated with planners. The perspectives of survey participants revealed that

	good leaders must work in the interests of their business, and not as per their culture or personal needs. 25- Sustainability has a huge impact on the target, where a successful organization usually evaluates its perception of achievements, hires the right flexible team and the right plan of organizational flexibility to ensure business continuity. 26- It has been found that the concept of enterprise resilience consists of six attributes that are divided into two categories. The first set consisted of the adaptive capacity, coherence and flexibility, and the second consists of trust, relevance and reliability. 27- It has been found that if a firm adheres to this structure, it can withstand both opportunities and threats at the same level as benefits. In addition, the firm can develop in response to risky and possible types of changes that occur during the implementation of the strategy, sustainability, the organization must ensure that planners and managers are distributed throughout the organization. 28- In addition, the functions of planning and documentation would lead to the best practices and have simple, predetermined resiliency standards for their

	operations. While continuity plans tend to cross normal work tasks and go beyond their requirements, developers and managers find it difficult to find time to prioritize their standard work tasks and prepare for unexpected failures that may or may not occur in the future. 29- It should be noted that the participants of the survey agreed that the planners are not professionals in business continuity programs; rather, they are experts in their fields, which affects the continuity program and resiliency of an organization. 30- These important planners will help document important activities and differentiate information in their field to help the continuity program and its owners, but this goes beyond the priorities of their work and responsibilities, and the problems arising from this fact are explained earlier.

Table 6.46: Primary research findings – system maturity

Cyber resilience	**Main findings**

System maturity (resiliency level) and different stages	1- The first object of a system includes financial, operational, production, disaster recovery strategy, which regulate the daily activities of an organization. 2- The second level is the objects related to the organizational structure, such as communication, skill level and duties of employees, which are emphasized by the human resources and communication processes. 3- The next level is the applications and software used for business and database management, such as customer relationship management and ERP applications used to process business transactions. 4- Processes are the next level of the facility, which include critical business processes and IT systems; for example, receivables and payables and problem management. 5- Systems consists of people, processes and technology. Processes demand both people and technology. 6- It was found that the technologies and tools include networks, systems and technologies that are used to process data and run business applications, and objects are buildings and warehouses and factories used to house an organization and its technologies.

	7- These layers conceptualize the components of an organization's business sustainability and help organizations identify key areas that need to be focused on when building a resilience model. 8- Some confirmed that this model also classified business attributes as per the functions that determine its ability to respond quickly to any failures. 9- Business resilience basics offer the following five attribute classes that are an integral part of a sustainable business organization. 10- The first key attribute is control and compliance, which describes the ability to identify, predict, evaluate and control the risk associated with compliance with social, economic, technical, environmental and regulatory factors. 11- The second attribute is the ability to predict and detect any events that represent a potential security risk or privacy concern for business transactions (the ability to measure such events can save a business from operational risks). 12- The third attribute is the deflection and hardening. The attributes protect and preserve and indicate the organization's ability to defend itself from harm. Be it

	accidental or intentional damage, the attribute preserves its data and resources. 13- Attributes of the system insures the sustainability of business. 14- It has been found that the most important barrier is organizational beliefs and values that hinder the development of sustainability because the organization is more focused on customer service, profits, and so on, than on the critical events and potential threats to the system. 15- Most organizations are designed so that they are not resistant to critical system failures. 16- Another barrier also confirmed by the survey participants in this study is a management system that usually emphasizes centralized control and is incompatible with the concept of sustainability, which emphasized self-confidence and willingness to cope. 17- The application of sustainability assessment has a huge impact on the assessment of business continuity plans, and this can be achieved by analysing alignment of a business with a given definition criterion that can be adapted and configured in accordance with all types of programs.

	18- This patented resilience tool has been successful in many cases. It covers three main elements, such as improving the reporting process, identifying risk, and helping to assess organizational sustainability. 19- Such systems have three stages in terms of reacting to disruptive events: reactive (has no plans), proactive (has risk management plans), and mature (uses resiliency plans). 20- All types of organizations face opportunities and threats at the same time, so they raised an important question here. The question was: Do we need to predict what kind of violation we will face, good or bad? Answer: was 'no' in the survey, and by correcting the question in how good it is for the sustainable development of a company or organization, the enterprises face or predict these unforeseen threats and opportunities and the ability to withstand. This was in addition to the notion of how the enterprises react if they intend to create a sufficiently stable organization. 21- The concept of start-ups consisted of three attributes: 1) how to respond to feedback, value (adaptive), 2) when to move quickly immediately after

	determining the correct signal value (moving), and 3) then trying to maintain focus, which means consistency. 22- It was found that large organizations, for example, in the current case, Smart Government, learn from the lean process, especially when it comes to product development in the field of Smart Government (development of their services). 23- In the Elastic concept, organizations must respond to such a violation as an opportunity, and must creatively perceive big failures in order to be able to benefit from them, learn and recover, and then, of course, find a way to succeed in a disaster; to achieve the highest level of maturity. 24- Systems phenomenal structure to maintain organizational sustainability is compulsory for criteria of risk management and business improvement that should be equally oriented.

6.2. Smart Government and Telecommunication Infrastructure, a Modern Tool of Public Administration

It has been found that an electronic government is a public and virtual portal that provides information, services and help to citizens, especially in business. It also facilitates the daily processes of individuals and companies, which can change the perception of individuals regarding

the role of recent governments in improving their environment. Smart Government also works on the development of different policies related to the validity and security of information, through the use of new technologies (Zamoum, 2007). Similarly, this was confirmed by the wide portion of respondents who agreed that Smart Government is a new era in information technology. It has been found that the scholars like Oliver and Sanders (2004) preferred to use the concept and as per them, the integrated governance is necessary instead of the electronic government.

The findings revealed that this concept is more accurate and reflects the nature of the combination of interactivity that exists between the citizen, IT and government electronic services. This is especially true when IT is halfway to directing and organizing individual and organizational problems. In addition, it directly affects the government's relationship with its citizen and contributes to rethinking the democracy in the new millennium, which consists of challenges, such as transparency, equity and privacy. However, the response of most survey participants was that the UAE smart governance is better and has sufficient resilience. Furthermore, the electronic governments have three bases: information, computerization and communication technology. It has been found that the Smart Government project became reality with the existence of different elements. One of them is the communication infrastructure of modern cities in particular and developed countries in general.

Hence, it can be said that some countries have adopted these technologies and have adopted the idea of electronic government, which has allowed them to become international investment destinations, even in the media, commerce and economic areas (Kumari & Kumar, 2015). Through its massive investments in new technologies and the launch of this project in the early 1990s, which attracted international companies in information technology, the electronic government of the US achieved progress in this field. In addition, the electronic government systems of Canada and the

UK, together with Dubai, have demonstrated that government projects represent a remarkable movement towards a new century, as these projects are leading the world, especially when it comes to electronic services (Zamoum, 2007).

The Smart Government project of the UAE has a strong impact in the IT field and also helps significantly in the advancement of IT strategies and processes. Furthermore, the survey respondents agreed that the project provides financing for important projects in the information communication industries that are related to this field, such as Internet City, a free trade zone and free trade zones for electronic commerce. It also financed media projects, which have been successful through its various media channels and electronic services, which have helped facilitate the process of communication with the public (Zamoum, 2007). Smart Government is a project that has different characteristics and is becoming a reality through different stages, which include achieving a customer-centred approach with government electronic services (Oliver & Sanders, 2004).

In addition, the nationals/citizens are considered customers of this new system and can benefit to the maximum of their ability to save time and effort with such a high level of technological tools and online processes in a secured cyberspace (Zamoum, 2007). This increases effectiveness and efficiency, as well as simplifying and streamlining government services using technology as a key enabler (Bayuk et al., 2012). Meanwhile, the findings indicated that the Smart Government system of Dubai innovates new processes and governmental services (DEG, 2008). At the local level, the electronic government of Dubai and the electronic government of Sharjah in the UAE are making progress, while Sheikh Mohammed Bin Rashid declared that Dubai is heading towards a new smart century, which means a great leap in the development of the infrastructure of telecommunications (Lanz, 2016).

In addition, investments are currently being made to support the Smart Government project. The city of Dubai, especially for the Smart Government project and the Smart Government initiative, which was launched in Dubai, is to be completed in 2020 (Conteh & Schmic, 2016). By taking advantage of ICT, cities with a highly integrated telecommunications infrastructure are established as knowledge-based economies in the UAE, which plays an important role in improving service efficiency and cybersecurity. In addition, it has been found that it is beneficial for all types of organizations, both in the public and private sectors. Electronic governments expect to consolidate their achievements by creating an organizational culture of cybersecurity and the creation of systems with high resistance to risk and to ensure sustainable growth in public and private industries (Mougan, 2010). At the same time, it creates a powerful infrastructure and expands its services.

This would be possible due to highly qualified personnel, as well as good strategies and scientific methods of confronting potential risk before it occurs in order to be able to minimize the impact of risk in the future(Ruggeri, 2016). The agreement of the respondents to the questions asked showed that the Smart Government project includes several sub-projects in which a knowledge-based economy uses ICT as a key factor. These included Smart Government initiatives. Another important aspect of cybersecurity is a triad of three important security aspects, that is, integrity, confidentiality and availability. These are cybersecurity information security objectives. Likewise, most of the respondents agreed that confidentiality is the extent to which the system prevents unauthorized access to information, while timely availability, accuracy and reliability of information is also equally important.

However, some of these cybersecurity goals are mutually exclusive, for example, the easy availability of information makes the confidentiality of information more complex (Kumar &

Kumari, 2015). Ruggeri (2016), who wrote an article on risk in financial institutions, found cases offering a backup system solution that is not electronic and is not associated with any electronic system. The author offered some tips for reviewing the crisis plan with respect to the Smart Government initiative, in addition to being part of an alliance with key functions and/or players. This could be, for example, CISO, IT and Risk Management. Once these two phases are completed, this could form the basis of robust cybersecurity and Smart Government. It was confirmed by Victoria Pellittari (2014) that the cybersecurity structure of NIST can be applied to various organizations and corporations, each organization has its own risks and a unique critical infrastructure.

The NIST Plan included framework design workshops that can receive feedback from its current users. The structure of NIST is explained on a theoretical basis and the focus of the research was on two concepts of IT and ICS (industrial control systems). The findings indicated that in those concepts, the needs of both could differ depending on the type of organization and over time. Furthermore, the findings of Michael Chertoff (2014), as discussed in the literature review, spoke about risk management in the modern safety landscape. The author proposed a skeleton key, which should recognize several levels of protection against potential threats. To exit the target zone, an individual needs to create a series of solutions, constantly assessing risk and measuring vulnerabilities in order to be able to cope with them.

Meanwhile, Guo et al. (2009) and Walser et. al. (2009) emphasized and confirmed the people's vulnerability is the issue to focus on, not weakness in systems, considering that it is only people who commit cyber-attacks. The factors were divided into the dynamic risks into two main parts of the same structure: 1) the risk management section, which consisted of recognizing vulnerabilities, predicting threats, and comprehending the consequences; and 2) planning and

prevention, when the stages of work and implementation could begin, depending on factors affecting the risk, to prevent the appearance of cyber-attacks. Another study by Hoffman Jooffman (2014) in the form of an article criticizing the structure of NIST, found that this structure contains no details and requires research so that a government organization can use it, where risk is very important. He added that the frameworks form a brilliant start, but ultimately, they disappointed their customers.

As the issue of cybersecurity has expanded in the US, the author found that the need for a stronger, more modern structure is imperative. The good news in this relatively new field of cybersecurity is that it is based on the risk that can provide maximum security for the US security system, as well as the UAE, with some changes in its structure from this research point of view. Moreover, it has been noted that survey participants agreed that cyber risk would be the major issue in the Smart Government system of the UAE. A study of Eva and Barry (2006), which they conducted for the risk assessment while using a macroeconomic framework for protecting intellectual property. The research focused on the effects of cyber-attacks, which lasted a long time.

The basis for IP theft is cyber-based, this concerns the long-term consequences of such attacks, which are of great importance from an economic point of view. In their studies, it has been found that the sub-models and variables of the International Impact Analysis Framework (ICAF) are explained in detail in their studies and are used to estimate the loss of intellectual property due to foreign theft (Chanopas et al., 2006; Esteves & Joseph, 2008). Meanwhile, an examination of the piracy and loss in all types of intellectual properties, such as books, images, recordings, music, and so on, was found in a study conducted by Matook et al. (2009). The research used the stock model and input-output models for specific countries to evaluate IP piracy in different countries.

A research conducted by Newman (2007) by asking a fundamental question about potential preparedness for cybersecurity attacks identified the cybersecurity skills and structures that currently need to be prepared for such crimes.

The research indicated that teaching students during a school period would lead to many years of IT experience and give them enough time to develop a complex and high level of IT skills. On the other hand, giving them the opportunity to explore the IT world to decide whether they want to specialize in it or not. Furthermore, the participants of the survey agreed that this career requires certain types of values and ethics; where most highly qualified students already have a criminal record, because they know their ways around IT. The only way to be prepared is to make sure that the information infrastructure and IT staff are ready, which can only be realized through the cybersecurity scientific base and special cybersecurity skills.

In 2015, Greenaway and her colleagues in their research in the US on a conceptual structure, found that the model can be implemented in the field of cybersecurity. He also discusses privacy theory and management theory. The research highlighted the gap in personal and cybersecurity literature, where the relationship between the citizen and the organization should be defined, and the responses of the organizations are very limited. These problems can lead to distrust between the two parties; because of the endless problems that may be caused by citizens due to cyber-attacks or a new concept of confidentiality in the new era of the internet. They added that the agency must control potential risk, otherwise it faces problems of trust from stakeholders and customers.

A review of cybersecurity revealed the absence of a number of models aimed at protecting cybersecurity. There are only two or three structures and articles resulting in a lack of research on

a relatively new topic. In this research, Harry Hyslop (2016) used to manage cybersecurity risks. It is clear that cybersecurity is difficult to achieve and there are currently insufficient resources to protect everyone at the same level (Rotchanakitumnuai, 2007). Despite all the most innovative IT tools and applications, there is always a chance that they could be broken. A risk management approach is one of the most useful strategies in this environment. Many organizations have already implemented solutions to protect privacy and civil liberties. The theoretical bases are intended to complement these processes and provide guidance for the convenience of confidentiality of risk management in accordance with the organization's approach to managing cybersecurity risks (Ruizhong et al., 2010).

Meanwhile, the responses from survey participants have shown that integration of privacy and cybersecurity can benefit organizations by increasing customer confidence, providing more standardized information sharing and streamlining operations for legal regimes. It has been found from the research of the business dictionary, that risk management is analysing, evaluating, controlling, and preventing, minimizing or eliminating unacceptable risks (BD, 2012). To be able to manage risks, organizations must understand that when events occur, they could be somehow affected. Furthermore, the survey participants agreed that organizations should prioritize risks and activities, recognizing the sustainability of risks to cybersecurity, which can also help organizations have a complete idea and make the right decisions about financial and management costs in the cybersecurity domain.

In applying and implementing risk management programs, organizations are given the opportunity to quantify and propose their adjustment programs in the cybersecurity arena (Montagna, 2005). However, cybercrime and internet hacking are becoming a huge business, which leads to the electronic suffering of companies from cybersecurity breaches. A recent

example of a cyber-attack is the hacked emails of the chairman of the US presidential campaign during the US election period (Bandyopadhyay et al., 1999).

This high-profile event had a tremendous impact on the election campaign mentioned, with the result that the competent party won the elections and the presidential period in the US for four years. It has been found that to establish an approach to managing cybersecurity threats within the existing frameworks, the research could be done by the Chief Information Security Officer (CISO) for the city of San Diego. This structure provided a common language for understanding, managing, and expressing the concept of the lifecycle of cybersecurity risk, both internally and externally. Hence, it can be stated that the IT infrastructure and its security is the basic component for the Smart Government systems regardless of the country or nations they are being adopted by.

6.3. The Resilience: A Compulsory Component in Government Administration

It has been found that the resilience refers to the characteristics of an organizational system to withstand stress and overcome external or internal threats or attacks, and this applies to the system as a whole, and not to its individual parts (Adger, 2000). To assess the sustainability of an organizational system, the capabilities and interactions of various parts of an organization after a destructive event are considered decisive in how they interact and communicate with each other. Sustainable organizations encourage advisory and joint decisions (Schneider, 2010). Furthermore, it has been found from the research of Belanger and Hiller (2006) that the rules are not just dictated, but encourage employees to behave in the way that is consistent with the expectations of customers. Thus, a sustainable organization seeks to articulate, recognize and demonstrate its values (Kerr, 2016).

Meanwhile, the survey participants agreed that sustainability is the ability of an organization to predict and recover from changes and events whether expected or unforeseen. It is believed that this is more than just risk management and does not entail a crisis-related organization or supply chain. Rather, it is a widespread phenomenon that entails all the changes that the organization faces, and not just the crisis (Montagna, 2005). It includes managing unforeseen disruptions from suppliers, as well as changing purchasing habits. A sustainable organization also provides and adapts to be able to serve its customers with the products and services they prefer, taking care of supply shocks (Iribarren et al., 2008). This is a valuable feature because change is a continuous global phenomenon.

It has been found that the studies show that the average age of the company at the S & P 500 was 61 years in 1958 and only 18 years in 2012. This indicates how rapid the changes are and the inability of companies to survive in this economic dynamism. On the other hand, it was found that resilience, an alternate concept of sustainability of a business organization, is the ability to open and use opportunities against competitors by taking risks (Newnham & Crask, 2015). The sustainability of an enterprise depends on the sustainability of its various components. This is a multidimensional concept, covering aspects of business organization. It was found from the review conducted by Chesley and Amitrano (2015) that sustainability is an organization's ability to anticipate and undergo change, not only to overcome but also to evolve because of its existence.

Meanwhile, it was also confirmed by Olson and Anderson (2016) that sustainability in a business context refers to overcoming the problems largely dependent on planners that are distributed throughout the organization to create executive strategies, as well as significant leadership involvement. In the late 1990s, researchers like Featherman and Pavlou (2003) talked a lot about leadership development in business firms and large-scale programs, and in recent years,

the risk management came to the surface so that the organization could survive in the fast-growing business arena and emerged from hundreds of contests. The idea of recovery and the ability to thrive in any destructive event is a standard set of documented plans.

Such plans are called Failover Plans, which allow organizations to mitigate potential risk by giving them the opportunity to implement such a plan on a systematic basis in order to increase preparedness for all business failures. Furthermore, Ratnasingham (1999) and Chesley and Amitrano (2015) conducted research on the new opportunities needed by business initiatives. They found that not every organization is ready for the changes that are taking place around them if they do not have a good new sustainability plan for survival and cannot evolve in the face of new changes or intermittent events. The researchers talked about the different features that each organization must apply to be able not only to overcome this change, but also to be resilient to it, knowing what happened and what is happening, and what is yet to come, to be well-prepared in accordance with scientific standards.

Meanwhile, one of the points in this regard, such as the concreteness of the plans for resilience and sustainable development, was also confirmed by the survey participants of our study. Usually, in the plans and programs in most organizations, there are elements of the standards of textbooks, but only some of them are innovative and detailed, which could create a large gap between what is happening in reality and what was indicated in these plans (Langfield-Smith, 2008). In the conventional plans that are used in any organization, there are no scientific ways to assess its quality, since this is a continuity plan or simply a textbook plan that is not related to the actual business of such an organization.

On the other hand, it has been found that the main criteria here are the ability to select the most distinctive information in terms of business continuity, and then document it, benefit from it, use it properly, develop it and share it with members of an organization. This was confirmed by Olson and Anderson (2016) in the research, which they conducted on the resilience and sustainability of business continuity to their needs. The research showed that the resistance team differs from the risk management team because of the assessment, while fault tolerance depends on if there is any risk. In addition, it depends on any undesirable event at the stage of implementation of the business continuity plan, which stated that the assessment, in this case, depends on the content analysis. In addition, the risk assessment also depends on the implementation resulting in a continuation of work even when confronted with disruptions.

Meanwhile, the difference between risk management and resiliency is that the latter will first prevent or mitigate the risk and secondly reduce it even after interrupting an event that the plan consistently fulfils the main objectives of an enterprise. The respondents knew about the activities and environmental challenges of Smart Government initiatives of the UAE government. It describes operational improvements related to business processes, as well as products and services of the organization, as well as with people and the control mechanism (Kerr, 2016).

With the increasing complexity of supply chains due to the globalization of organizations, an organization’s ability in assessing and managing supply chain risks during the procurement, production, delivery and marketing cycle is of paramount importance (Bradley & Pratt, 2011). It has been found that any violation of the supply chain can lead to reputational risks, as well as operational, financial and reputational risks. Sustainability of the supply chain is an important factor in the modern business environment since the supply chain is considered the foundation of

the modern economy. It has been found that any disruptions in the supply chain and the ability of businesses to withstand this will determine the sustainability of the supply chain to the system.

However, sustainability means having alternatives to counter-failures, which leads to layoffs, so it is expensive (Battersby, 2015). Thus, the problem of sustainability in the supply chain is to ensure sustainability and efficiency (2015 edition). Organizations deal with confidential information, and this information can be crucial to the success of a business. Therefore, it is necessary to provide this information. It is important that a sustainable organization manage its information security and protect its intellectual property rights. This requires the organization to apply practices that allow interested parties to collect, process, store and use information in a reliable form (Kerr, 2016). Networks are connected to each other through communication nodes, and the stability of the network determines the degree to which faulty communication systems affect the overall structure of the network, and also disrupts inter-organizational communication and how adaptively the network responds to it.

In most cases, deleting network messages or deleting nodes can lead to the exchange of information with alternative nodes or routes to exchange information (Ougut, 2011). However, it was also confirmed by Hoffman (2014), as discussed in the literature review, that some network structures are more sensitive than others to removing links to nodes when the network is divided into subgroups that are not connected to each other (Barab'asi, 2003). The most stable network structures are networks without networks since they are not sensitive to the removal of random nodes. However, even these networks can be destroyed when critical nodes are removed (Kahn, Barton & Fellows, 2013). Network hierarchy, network diameter, and network clustering are some of the determining factors for network resilience. While traditional crisis management strategies

can be helpful, you can increase administrative and social capacity to cope with crisis management situations by developing resilience (Newman, 2007).

The research of Hyslop (2016) suggested that an immediate response to these disasters depends on the resilience of citizens, operational commanders and those in charge of the first responders, such as firefighters or emergency medical specialists, while strategic leaders can make a difference in the long-term (Drabek, 1986). Thus, efforts should be directed towards the development of sustainability, which is perceived as a new quality for a professional system (Longstaff, 2005). It has been found that improving institutional quality, experience and resources are expected to lead to an increase in recovery from the crisis, but sustainability is still a phased quality of the system, which can be gradually acquired and improved only through trial and error of its response to future disasters and system failures.

Furthermore, the views of respondents indicated that resilience to construction has two prerequisites: first, the realization that a system failure, destruction or catastrophe can occur, and the second condition is that the stability of the building does not replace the basic elements of emergency response operations. The first step in the development of sustainability is the preparation of first respondents who are well-trained to make independent decisions and work effectively in situations of critical situations with the system (Adger, 2000). They must be knowledgeable and convinced of core organizational values, ethics, and clearly defined priorities for responding to a crisis in the interests of the organization. The next step is business continuity planning, which includes setting up a backup centre in a remote location, which reflects current business operations in the backup storage of IT memory, as well as in the event of a disaster.

An individual can continue business operations from a remote site. The third stage is joint planning with the participation of all interested parties, in which all possible threats are identified, and possible decisions are regularly reviewed to cope with the ever-changing nature of people (Kerr, 2016). Meanwhile, Longstaff (2005) found that the fourth step is the joint preparation of all stakeholders by familiarizing with the contingency plan and modelling its ability to respond to the threat. The final step is to prepare a guide on how to mitigate resilience in a crisis. Management should avoid traditional pathology of leadership in a crisis situation (Newnham & Crask, 2015), for example, blaming others, waiting for facts and figures before making a decision, waiting for outside help, sticking to the original plan or spreading rumours without verification.

They need a realistic approach to what can be done, and they need to take the necessary steps that can be useful for change (Boin & McConnell, 2007). It has been found from the research of Chesley and Amitrano (2015) that change is the key to each plan for organizational sustainability. They raised the question of how an organization responds to a change in its business plan. They found that strategy is important for any type of organization, but after its presentation, it becomes vulnerable to change; when they encounter interruptions, the strategy cannot be completed on time (Chesley & Amitrano, 2015). Moreover, Olson and Anderson (2016) talked about adaptability and how it relates to culture, which also influences strategy. It has been found that organizational sustainability outperforms the leading positions that over the years have not been an excellent factor for a successful business, adding that enterprise resilience is the most important success factor in any business; where sustainability becomes more measurable and manageable (Chesley & Amitrano, 2015).

As for organizational sustainability, developers play a key role. Olson and Anderson (2016) found that planners are key to each business continuity program; the more they are involved, the

more the plan is ready for implementation at any moment. In addition, fault tolerance assessment helps motivate planners to a goal. Hence, more active participation and participation in all activities of their continuity programs and, moreover, with the support of the senior counsel. Moreover, the high level of participation would increase the level of commitment between planners, which can help them to strive to achieve better results in their activities. Furthermore, it can assist them to increase their confidence and self-belief that they can manage their plan on a more sustainable basis than before the concept of sustainability (Barab´asi, 2003).

Kahn et al. (2013) and Longstaff (2005) added that planner reviews are an important tool of this methodology in the arena of organizational resistance, which emphasizes the role of sustainability assessment, which gives them a great value. Chesley and Amitrano (2015) found that enterprise resilience is measurable and manageable, unlike the traditional risk management system that has been used in recent decades. They added that an individual needs to know the key elements of enterprise sustainability in an organizational context. Chesley and Amitrano (2015) identified that the traits they offer are more likely to be designed in accordance with any business initiative so that they cannot only survive in the face of change but also benefit from this and show a great example in the market.

This can be achieved through greater returns from young people and their new thinking, which will create a more sustainable environment in such firms. After examining criticism regarding organizational resiliency in the literature, it was found that sustainability research focused on increasing the participation of planners, especially in the continuity plans of programs or projects. The focus was on the lifecycle of the program, which should consist of an assessment stage and then a planning stage, and then carry out exercises to reach a level of maturity and assist in quick recovery to ensure the continuation of such a program (Boin & McConnell, 2007). To

help the recovery process reach a level of maturity, planners need to be more active and ensure that risks are constantly identified and evaluated, as well as document resiliency plans, to ensure resilience to potential obstacles or even natural disasters.

Assistance helps in evaluating the content of such continuity plans, which aim to guide the planning process to the maturity stage. This type of assessment can maintain compatibility and visibility in addition to improving compliance in a business continuity program. However, attractive planners and executives are not an easy task. Hence, this is a complex task, while the company's culture is not ready for such a decision or change (Chesley & Amitrano, 2015). As noted and found in most studies, such as Olson and Anderson (2016), Chesley and Amitrano (2015), and Olson and Anderson (2016), culture influences strategy, while in some cases leaders are isolated from employees and find it difficult to be more involved or even associated with planners. The perspectives of survey participants revealed that good leaders must work in the interests of their business, and not as per their culture or personal needs.

Furthermore, Olson and Anderson (2016) confirmed that sustainability has a huge impact on the target, where a successful organization usually evaluates its perception of achievements, hires the right flexible team and the right plan of organizational flexibility to ensure business continuity. In addition, the sustainability assessment will lead to an increase in the level of participation of the highest council of any organization and could create direct contact between them and the planners; who are more equipped and more aware of how to deal with intermittent events and have a specific resiliency plan with details. Moreover, Chesley and Amitrano (2015) found the concept of enterprise resilience to consists of six attributes, divided into two categories. The first set consisted of the adaptive capacity, coherence and flexibility, and the second consists of trust, relevance and reliability.

They found that if a firm adheres to this structure, it can withstand both opportunities and threats at the same level as benefits. In addition, the firm can develop in response to risky and possible types of changes that occur during the implementation of the strategy, sustainability, the organization must ensure that planners and managers are distributed throughout the organization. In addition, the functions of planning and documentation would lead to the best practices and have simple, predetermined resiliency standards for their operations. While continuity plans tend to cross normal work tasks and go beyond their requirements, developers and managers find it difficult to find time to prioritize their standard work tasks and prepare for unexpected failures that may or may not occur in the future (Cocchiara, 2005).

It should be noted that the participants of the survey agreed that the planners are not professionals in business continuity programs; rather, they are experts in their field, which is part of a continuity program. These important planners will help document important activities and differentiate information in their field to help the continuity program and its owners, but this goes beyond the priorities of their work and responsibilities, and the problems arising from this fact are explained earlier (Pauchant & Mitroff, 1992). It was found that IBM had provided and created a business resilience infrastructure that is designed to determine the level of organizational resilience. It included a set of objects, called layers, that emphasize the ability of any business to fail. A detailed discussion of the various levels of such model was discussed by Boin and McConnell (2007).

The first object is a strategy and includes financial, operational, production, disaster recovery strategy, and so on, which regulate the daily activities of firms. The second level is the objects related to the organizational structure, such as communication, skill level and duties of employees, which is emphasized by the human resources and communication processes. The next

level is the applications and software used for business and database management, such as customer relationship management and ERP applications Kerr, (2016), used to process transactions in business transactions. Processes are the next level of the facility, which included critical business processes and IT systems, for example, receivables and payables and problem management (Ward, 2015).

It was found that the technologies and tools include networks, systems and technologies that are used to process data and run business applications, and objects are buildings and warehouses and factories used to house an organization and its technologies. These layers conceptualize the components of an organization's business sustainability and help organizations identify key areas that need to be focused on when building a sustainable model (Gordon & Larry, 2005). However, Bucy and Gregson (2001) also confirmed that this model also classified business attributes as per the functions that determine its ability to respond quickly to any failures. IBM Business Resilience basics offer the following five attribute classes that are an integral part of a sustainable business organization. It has been found that the first key attribute is control and compliance, which describes the ability to identify, predict, evaluate and control the risk associated with compliance with social, economic, technical, environmental and regulatory factors.

The second attribute is the ability to predict and detect any events that represent a potential security risk or privacy concern for business transactions (Coleman et al., 1991). The ability to measure such events can save a business from operational risks. The third attribute is the deflection and hardening. The attributes protect and preserve and indicate the organization's ability to defend itself from harm. Be it accidental or intentional damage, the attribute preserves its data and resources (Cocchiara, 2005). By focusing on the main objects of sustainability, organizations can create a sustainable structure by applying and acquiring the necessary attributes necessary to

ensure sustainability (Tapscott et al., 1989). The development of organizational sustainability has some barriers that are primarily related to the degree of organizational readiness (Pauchant & Mitroff, 1992).

Furthermore, it has been found that the barriers also reflect on the factors of management and society. There are various social constraints for a flexible approach to disasters and disruptions. People usually respond to the potential threat potential in a dysfunctional manner, including denying or lowering the importance of the threat or its likelihood, and this is just a mental barrier that creates resistance. It has been found that the most important barrier is organizational beliefs and values that hinder the development of sustainability because the organization is more focused on customer service, profits, and so on, than on the critical events and potential threats to the system. When such events are observed in other places, organizations rationalize the occurrence of an event and justify the improbability of an event happening to it.

The obstacle to sustainability also includes the institutional design (Orlikowski & Robey, 1991). Most organizations are designed so that they are not resistant to critical system failures and failures. It has been found that any emergency response requires flexible decision-making, while organizations have limited powers (Boin & McConnell, 2007). An increased resiliency requires time and resources for an unforeseen event that may or may not occur. It also requires the cost of educating people and using them through imitations to prepare them for unforeseen events. It also requires collaboration with different stakeholders and adaptation to their own programs, values and cultures. All these costs create serious barriers to the development of organizational sustainability. Another barrier to sustainability also confirmed by the survey participants in our study is a management system that usually emphasizes centralized control and management and is

incompatible with the concept of sustainability, which emphasized the self-confidence and willingness to cope.

The barrier to sustainable development is most important for the sustainability of Smart Government systems, which are the socio-economic framework (Pan, 2006). As communities that are in disarray themselves live in modern cities, the poor, homeless and immigrants are the least sustainable communities. Thus, it is becoming increasingly difficult to develop and implement a sustainable Smart Government mechanism for such socio-economic classes (Boin & McConnell, 2007). The application of sustainability assessment has a huge impact on the assessment of business continuity plans, and this can be achieved by analysing alignment of a business with a given definition criterion that can be adapted and configured in accordance with all types of programs. This patented tool has been successful in many cases. It covers three main elements such as improving the reporting process, identifying risk, and helping to assess organizational sustainability.

Chesley and Amitrano (2015) found a structure for assessing organizational sustainability. The structure consisted of six powerful functions that make any type of organization more resilient to risk and other types of sudden changes or interruptions. Those factors included technological breakthrough and the two researchers talked about how all types of organizations face opportunities and threats at the same time, so they raised an important question here. The question was: Do we need to predict what kind of violation we will face, good or bad? The answer was ‘no’ in the survey, and the question was revised to ask how well a company or organization faces or predicts these unforeseen threats and opportunities and the ability to withstand them. Furthermore, the notion of how the enterprises react if they intend to create a sufficiently stable organization was explored.

It has been found that there is a need to understand the basic elements that increase the likelihood that this practice threatens the sustainability process. These first three features are found to be fundamental in accordance with two researchers when responding to risk time and periods. Although these functions work to serve their ability to benefit from risk or make the most of all kinds of changes (Chesley & Amitrano, 2015). Some researchers, including Ridley and Channing, (1999) and Chesley and Amitrano (2015), talked about the concept of start-ups. This concept consisted of three attributes: 1) how to respond to feedback, value (adaptive), 2) when to move quickly immediately after determining the correct signal value (moving), 3) then trying to maintain focus, which means (consistency). The authors found that large organizations, for example, in the current case, Smart Government, learn from the lean process, especially when it comes to product development in the field of Smart Government (development of their services).

The concept of lean start-ups can be applied to Smart Government services from the point of view of launching new e-services to find out whether people can achieve this in general and, in particular, at the same time, to see if there are any great opportunities. There is also another concept proposed in the same arena, called Fast-Works, based on the launch of the same elements and principles (Olson & Anderson, 2016). This sustainability culture can be implemented throughout the organization, not just in product development. However, at the market level, organizations must be creative in how to serve talented youth and anticipate both opportunities and risk while creating powerful communities. These different traits are important for an organization's relationship with its stakeholders, customers, and its business partners. It has been found that the sets of characteristics may seem easy to achieve, but in fact, they are quite difficult to maintain.

Research conducted by Schell (2016) found that most leaders of in the 21st century are convinced that the element of trust is the most important element in maintaining relations and

business between organizations and their stakeholders or business partners. The perception of trust as a threat to the growth of any business creates a bottleneck that prevents it from flourishing and behaving with such business relationships. Both researchers found that the positive relationships of the organization and its customers, stakeholders, partners and business leaders are an important basis for business growth. It brings the people back to the strategy and the best way to achieve its goals. Moreover, the sign of importance is now the main focus of a larger number of managers who are convinced that the current world is filled with industrial violations.

While failures provide the best opportunity for an unconventional organization, the same violations can create a risk for existing organizations. However, it was found from the study of Zaklina (2014) that the problem is that an individual does not know when risk turns into a catastrophe and becomes part of this big failure, it is not the decision of any single person. In the elastic concept, organizations must respond to such a violation as an opportunity, and must creatively perceive big failures in order to be able to benefit from them, learn and recover, and then, of course, find a way to succeed in a disaster, to achieve the highest level of maturity (Edelman, 2014). The findings of Ackerman and Rushe (2014) and Kerr (2016), which conducted a research on the sustainability of the organization, suggested that the phenomenal structure to maintain organizational sustainability is compulsory for criteria of risk management and business improvement are equally oriented. The model of Kerr (2016) emphasized the qualities that form organizational resilience.

6.4. Discussion on Research Hypothesis

Moreover, the specific Hypothesis of this thesis will be as follows:

H1: The capability factors affect resilience in Smart Government organizations

Cybernetic resistance is a broader term that encompasses business management and cybersecurity. It not only defends the organization from cyber-attacks, but also helps to cope with the situation and guarantees the survival of the organization against attacks. Resilience is equal to the ability of the organization to succeed and thrive when it prepares, anticipates and adapts to sudden changes and disruptions in the organization. Organizational resilience means that the business owner can take risks with more confidence as a strategy. There are three main domains of resilience, which are very necessary for each type of organization, large or small.

The first is operational resilience. The organization that is resilient has a deep knowledge of the operations of the organizations and their operation and functioning. To meet the needs of customers, operational resilience is the identification of specific operational developments or improvements in their products and processes. It showed the consistency and potential of the organization that can achieve and grow completely under any circumstances (Kerr, 2016). The second is the resilience of the supply chain. In this sense, to achieve resilience, the organization must focus more on identifying risks to minimize interruptions and maintaining financial reputation. The third is informational resilience that is very important and critical. To maintain the capacity for recovery, the organization must protect the information of its clients and guarantee the security of all types of information. This requires information security techniques to collect information safely and process it (Kerr, 2016).

H2: The change factors affect resilience in Smart Government organizations

This hypothesis was developed based on the research of Johnson (1994), which indicated that the notion of change strongly appears in the industry of information and communication

technology. Reviewing the key factors of change motivate the researcher to include if the change factors can influence the resilience in Smart Government organizations. It is considered as the most important change in the 20th century and even before that, and in many scenarios, this industry is becoming a creator and innovator for more changes in every aspect of life and other industries. The research discussed that the change reached out to both public and private sectors, where new information and communication technologies have been implemented. Therefore, the hypothesis was tested, and the results showed a positive relationship between the factors at a level of 59% relationship.

Meanwhile, the background knowledge supported that hackers have grown bolder and bolder every day; consequently, cities that are joining the Smart Government project must be fully aware of all kinds of risks. Such risk factors would affect the governmental field and, in some cases, will lead to catastrophic results, depending on whether the Smart Government risk management practitioners are ready, aware, equipped and prepared for such a huge transformation. It was found that there were not enough studies concerning the measurement of resilience, and also a lack of resources about models exploring the system maturity of Smart Government frameworks as a means of risk management. Raising a system's maturity issues like compatibility, effectiveness, and accountability, the Smart Government employees must employ the cybersecurity strategies to achieve the overarching goals of their organizations as well as clients (Johnson, 1994).

H3: The management control factors affect resilience in Smart Government organizations

This hypothesis was developed while considering the research work of Sikula et al. (2015), which involved the analysis of the level of maturity of electronic government in terms of resilience and management control. This also explored what they are doing and how they are doing it, determining cybersecurity risks accompanied by those processes, to find out how to measure resilience in relation to the cybersecurity. This was done through the use of control management theories and the resistance of the system. Therefore, the hypothesis was developed to determine to what extent they can control the risks faced by electronic government systems, they must realize how to mitigate such risks through management control. This was to meet research demands and meet the overall objective and try to provide a scientific framework that has the capacity to measure resistance in the electronic government system, especially when it comes to cybersecurity.

This could have happened for the good of the professionals of the electronic administration and professionals to know how to control the risk of the cybersecurity. Meanwhile, the development and testing of hypotheses have shown a positive relationship and therefore, to be able to minimize the risk in the future. This risk management control capacity in the government field is not easy (Sikula et al., 2015). Brian Kuyfyt (2017) also mentioned in the background of this research that an individual cannot easily prove it in the government, how about an electronic government? This is what the research is expected to reveal.

In this regard, this researcher attended The Enterprises Risk Management of Cyber Security 2017 event, which takes place in Dubai. At this event, one of the most famous British hackers spoke about how cybersecurity is very difficult to achieve. The research also explored how to effectively use of the internet and how it can be a dangerous tool with its characteristics, as well as how can we find a piracy tool for hundreds of companies registered in a minute with the click

of a hacker? Finally, the research tried to demonstrate that risk can be controlled at a certain level, but traditional risk management methods do not work for long and there is a need for new strategies. For example, the notion of maturity of the system is fundamental for any government.

H4: The vulnerability factors affect resilience in Smart Government organizations

This hypothesis was developed based on different studies (Widmer, 2013; Sikula al., 2015; Pennathur, 2001), which worked on the vulnerability factors. As most governments are implementing Smart Government and smart governance, the risk has increased crucially since the internet tends to be easier to hack and the management of risk is questioned by their acquittal in most cases (Widmer, 2013). It has been discovered that the management of risks is not enough in many cases of cybersecurity, and the need for security theories of the system has arisen, especially when it comes to a vulnerability in the electronic government system (Sikula et al., 2015). This brought this researcher back to the main problem of this cybersecurity risk project.

After all, it raises a fundamental question: is cyber space vulnerable to risk? In addition, can this risk be controlled or not? Some found that risk management in cyberspace is just a theory that is far from reality, while others are more optimistic about the risk management of cybersecurity in the internet age (Pennathur, 2001). Furthermore, when the respondents were asked and tested the hypothesis, the results showed that vulnerability factors have a significant impact on the resilience in Smart Government organizations. This remarkable step towards a world of communication in cyberspace has its own disadvantages, such as vulnerability to risk; where thieves and hackers do not slow down in the short-term, and always look for weaknesses in new systems to violate.

These numbers point to the enormous amount of risk that the media faces every day. The findings indicated it is difficult to manage from a security perspective. At this point, the problem of cybersecurity arises and it is even more important for some countries to develop their risk management in cybersecurity; where recent studies show that cities are becoming targets due to their highly integrated infrastructure system as mentioned above. The internet constitutes a backbone of Smart Government projects, which depends entirely on the cybernetic space where all its processes are carried out online.

6.5. Summary of the Chapter

It is summarised that the industry has been slow to adopt the technology because of the risk that lies beneath the vulnerability of the system's online processes. It is a means that requires innovative thinking and implementation of cuts. Cybersecurity strategies and new IT plans, tactics and tools that Smart Government personnel cannot ignore can influence the performance of Smart Government service frameworks. It is necessary to know which tool to use and when a strategic problem is encountered, especially when it comes to cybersecurity risks. The role of the notion of the maturity of the system and many of its associated methods offer a solution to the challenges of resistance, variation, differentiation and measurement of risk. When integrated into electronic communications, the internet can facilitate the achievement of more effective win-win scenarios. It has been concluded that there is a whole network of security strategies that allows the monitoring and controlling of risks, which also helps increase resilience, minimize costs, and increase flexibility.

7. CHAPTER SEVEN: CONCLUSION AND RECOMMENDATIONS

7.1. Conclusion

The purpose of this study was to study the risk-based cybersecurity frameworks which are using cybersecurity developments. These systems are used to create a strong, protected, complete and hard to break E-system in the UAE. The framework could be adopted by Smart Government projects. This would help the projects to not repeat the mistakes that were made while conducting the processes of Smart Government which were used previously. The objectives pursued in the thesis were:

Objective 1: To determine and identify the components of the professional resilience framework to achieve Smart Government resilience and cybersecurity risk management.

Objective 2: To elaborate the risk management frameworks for cybersecurity in Smart Government.

Objective 3: To evaluate the existing resilience frameworks and identify the areas of potential improvement.

Objective 4: To develop a sound model for Smart Government organizations, on the measurement of resilience.

This Research was guided by two main questions:

RQ1: Validating the framework of Smart Government resiliency and cybersecurity risk management.

RQ2: How to evaluate previous frameworks on the measurement of resilience.

On the basis of an in-depth investigation, it is concluded that the security control is based on classification. The accuracy and accumulation of data in any case is a necessary procedure for launching progress. It is necessary to choose the right place for social security measures to sufficiently reduce risks by performing certain measures. In some cases, the prerequisites for organizational security is also not a minimal task. This commitment demonstrates the firm's desire for well-being and due diligence, as practiced in its approach to protection. It involves the reliability and availability of authoritative data and data structures. For the perceived traditional management tools provided by the information structure and data infrastructure security engineers, with the help of data infrastructure security officers, together with a conventional control provider, the most appropriate way to work using basic management tools for various levels of information systems could be chosen.

This does not interfere with the use of open source gadgets. There are several concentrations to test the use of open source plans. It is concluded that the US, Canada and the UK have reliably become pioneers in adjusting new strategies and innovations. They speak of a genuine case of a Smart Government for every improvement that moves it forward. By implementing and participating in Smart Government, they observe how quickly its foundation for media transmission is improving. A strong link was found between the two components. The first is the use of Smart Government and the rapidly growing and improving coordinated foundation of any nation around the world.

This also expands the possibilities of being a target for psychological fighters and robbers around the world. Consequently, these countries may be subject to pressure from many risks because of their highly integrated structure. For example, the US has been identified as the centre

of attention for cyber-attacks around the world. It is further concluded that these countries were able to flourish financially in the light of their monstrous oil and characteristic wealth. In addition, regardless of whether the UAE has oil reserves, it should have a plan to increase the money supply in non-oil sectors. The countries dominate this area, as they began to significantly improve what is happening from liberal susceptibility and an experienced business supported by an advanced media transfer system. It is concluded that the legislative bodies of the UAE, the UK and the US, used the new arrangements and laws to help make their jurisdictions increasingly suitable for new business.

Another advantage would be derived from new rules, which should help financial professionals from around the world to start a business in their own countries, which may encourage business pioneers. Currently, the US, Canada and the UK have invested heavily on their media content transfer systems. Therefore, they have advanced broadcast funds that contrast with different countries around the world. At the local level, Dubai is sometimes called the wired state in the Middle East. Indigenous peoples are suitable for all compliance methods used in western countries. UAE citizens have learned how to put forward and maintain increased demand in e-services, much like the services in Western social orders. At this point, the researcher has discovered how to reduce this risk, assessing its versatility.

It is concluded that a Smart Government enterprise is moving towards a new era of virtual government with the introduction of numerous online services. For example, e-learning, e-payments, Smart Government, and e-managers, which will stimulate the organizations that the business manages. This establishes a structure originated from a protective fence that works to protect from cybercrime and psychological oppressors. Although some argue that in case the UAE

government creates a system, programmers would make a passage to break their electronic structure. Therefore, there is a real cybersecurity risk regarding what is happening. Although for some time this is far from the reality that cyber-attacks affect security, the internet has become a correspondence mechanism for governments that makes it essential to make it even safer for this underlying condition.

It is concluded that Smart Government is a reliable, innovative, progressive and logical mechanism. Furthermore, it is a system that can work around the world. It has universal applications inside and outside associations. The study has recognized the risk of social engineering and structured the stages of displaying the thought in the Smart Government system of the UAE government. It is concluded that the cybersecurity risk problem is worsening every day. Due to the recently implemented platforms, the PC platform is becoming more fragile, much more helpless than the usual PC platform in earlier times. These new projects and structures contribute to the growth of helplessness in the field of cybersecurity.

It is concluded that programmers are the persons who create these new security structures for cybersecurity. Even after much research on this issue and the huge amount of funds spent on cybersecurity, the problem has not been resolved. It is also concluded that the issue of cybersecurity risk exists within the framework of the CPA firms, despite external hazards. It would be wiser for such firms to have paperless services called Smart Government services. These can save time, effort and money to attract more people to study the targets, although in this situation the risk of cyber-attacks would increase. Especially from representatives of companies that are suitable for electronic records, the Smart Government framework could be a better solution. It is concluded that if the UAE needs to return the package to cyberspace it must bring together

specialists and engineers for the platform in one place. The UAE can be able to get around this problem and offer better support for national security.

A systematic review of the literature leads to the criticism of the current theoretical frameworks in quantitative studies. The researcher systematically derived the research questions and hypotheses. New terms, new divisions, and new elements are provided in the research framework.

The relationship between the cybersecurity risk management and resilience was studied in the literature and the systematic review of seventy previous research articles revealed that they are focusing on the quantitative approach when studying these relationships as shown in the table (2.1) explains the relationship between cybersecurity risk management and resilience. It also explains why the researcher used the same quantitative approach in the current research because of scarcity of quantitative research on cybernetic resilience in Smart Government both worldwide and in the UAE.

Relatively few research studies have focused on the qualitative approach for studying this phenomenon. There were a couple of studies that used qualitative methods (Osho, Onoja, 2015; Vandebosch & Van Cleemput, 2008) and two more that used mixed methods (Dondossola, Deconinck, 2012; Vugrin & Turgeon, 2014).

As a conclusion, it is obvious that more focus is given to the quantitative approach over the qualitative and mixed methods approach. This reinforces the rationale of going for further quantitative research for a new contextual investigation for achieving the research objectives and determine and identify the components of the professional resilience framework to achieve Smart

Government resilience and cybersecurity risk management. Furthermore, to elaborate the risk management frameworks for cybersecurity in Smart Government. In addition to the above to evaluate the existing resilience frameworks and identify the areas of potential improvement and to develop a sound model for Smart Government organizations, on the measurement of resilience. Which also help to answer the Research questions by validating the framework of Smart Government resiliency and cybersecurity risk management and emphasizing on how to evaluate previous frameworks on the measurement of resilience.

The evaluation criteria on the previous frameworks of cybersecurity resilience was explained in (table 3.2). This is used in developing a sound model of resilience that addresses the main issues in the previous frameworks and tries to cover all the missing areas. Good metrics are also required to have some non-technical aspects; and should be relevant, to organizational missions, easily obtainable, and work for the improvement of resilience. The previous frameworks did not cover the managerial aspect (only few of them), it looked at cybersecurity as a technical issue only which is far from truth. Most frameworks missed that cyber problems are not all IT errors, but human errors as well. Also it is not a 'one size fit all' answer to security issues.

Previous frameworks missed the business area as it was talking about the status of cyber war and seemed to give less attention to financial and profitable business issue. In addition, frameworks lacked a proposed matrix and was found to be complex and unorganized taking into consideration the huge amount of restricted information it should be protecting. Although, resilience has been considered important at national and international levels, resilience metrics to reveal decisions of managers are in the early development stage. There is a need to build an effective metric for cyber

resilience. Some metrics make a connection between specific system measures and the policy goals, and some were technical only, not business or managerial.

Some frameworks tries to fill the gap in previous frameworks by combining three of them together, however, it carries the same problem that some of them have and lacks the resilience and focus more about the traditional risk management tools and strategies. After studying resilience and cybersecurity risk management in Dubai in-depth, it has been found that they are still in the proactive risk management stage when it comes to the maturity of their system. However, the environment and culture in the UAE and especially in Dubai encourages innovation and its readiness to implement resilience plans is high according to the survey and this research investigation. The Dubai Smart Government is willing to adopt new ways of thinking and new strategies concerning cybersecurity because it is trying to protect the upcoming event of EXPO 2020 which cannot be vulnerable to the risk of shutting down its system on the night of inauguration. Dubai has received a lot of threats and has been number two in targeting its systems after Israel, due to its highly integrated infrastructure. Sheikh Mohammad bin Rashid, the ruler of Dubai assigned a million dirhams prize for the best cybersecurity plan to be adopted by the smart Dubai system.

Things are moving really fast, from e-government to Smart Government to smart Dubai. More and more issues are derived from this fast moving and changing business environment. Dubai also launched an experimental small smart district, which is a complete city that uses only smart systems, which is a great step towards resilience. Whereas resilience depends on resilience scoring, repeating plans, repeating training, mocking cyber-attacks and the number of time resilience plans are being tested and put under trial until they reach the level of agility and rapid

detection, adaption, recovery, and prosper from the attack. It is noteworthy that agility is an important factor in the process of resilience, otherwise the organization will not be considered resilient but rather unprepared.

However, this framework concerns business resilience and missed technical and resilience assessments measures for achieving political and business goals. Although this suggested framework tried to cover all the important matrices and elements to a balanced resilience system, besides emphasizing the main factors that have a great impact on resilience status, it is subject to criticism by scholars and researchers. Planners admit that no framework is best but practitioners try to do their best to create a simple tool that can be used in all kinds of organizations, governmental, private, big or small. This thesis framework talked about four factors that exist in all research investigating resilience and cybersecurity risk management, especially in complex-natured organizations such as Smart Government. In General, it's not addressing technical part in depth, but rather emphasizes the managerial and business dimensions in depth.

The contribution of this research (plus the contribution in the 1st chapter) in the light of the previous analysis contains the following points:

1- Review of the existing frameworks
2- Evaluation of the previous frameworks based on certain criteria
3- Develop a sound model that covers all the missing areas in the previous frameworks
4- Built criteria for evaluating the resilience in cybersecurity and the relationships among these criteria
5- Linked the new criteria to the literature review on how to measure resilience

The thesis contributed in a positive way to strengthen the work of others by simplifying and adding a thorough analysis for the relationship between resilience and cybersecurity from a managerial point-of-view. This was built on the criticism of the previous contributions and how previous frameworks had criticized weaknesses. The business contextual analysis of the relationship between the resilience and cybersecurity is an added value to the current research relevant to the previously criticized frameworks.

This research explores resilience in the business context, which emphasizes good or bad disruptive events. The result will be either higher business profitability or lower business profitability because any opportunities that appear to be beneficial to the system must be taken to survive in the business arena. It is still considered a risk to the system though.

This study, unlike previous studies, did not neglect the three elements in business contexts, which are the business continuity, business profitability, and business performance. This study will be provided to the Smart Governments in the UAE. It is a simple reliable tool to achieve and maintain resilience to address cybersecurity risks. The current period of time has special importance in using the contribution of this work in the UAE before the EXPO 2020 because it is a relatively global and highly evaluated event that needs special care in facing risks of shutting down the system on the night of inauguration. The thesis tests the readiness of the UAE to apply resilience and in which stage are they effectively operating and applying resilience. The maturity of their systems is critically evaluated using the framework of the current study. The UAE did not reach resilience yet; however, they are ready to adapt it. However, the longer-term goals of this work are to provide further research on the resilience in cybersecurity and how it can be improved

in the region and expose this research framework to other contexts and organizations that have different environmental natures and levels of complexity, such as Smart Governments.

Cybersecurity resilience is considered to be extremely important in the digitalized era of the 21st century. This is because it can assist a business undertaking to avoid the catastrophic failure that is by an "all or nothing" approach to cyber risks. It will also make sure that the conversation goes far beyond Information Security and Information Technology. A number of elements exist that have an impact on the resilience of cybersecurity. Some of the common factors are the vulnerable aspects of an organization's cybersecurity, and the human factors of the entity (Holm & Ostergaard, 2015).

This study has practical and theoretical implications, in addition to what has been said, on the developing countries such as the UAE. First, it was the E-government, then the Smart Government, and now it is the Smart City. On a practical level, Smart Governments need to embrace opportunities and harness their experience to survive. Smart Governments need to consider the forces of change and realize the role of management control in this rapidly changing environment. It is an evaluation method to measure the resilience as shown in the following table, to be used theoretically and practically in the Smart Government projects.

Table 7.49: Evaluation methods to measure resilience

The framework details & focus areas	Forces of change	Vulnerabilities	Management Controls	capabilities	Resilience balanced / unbalanced	Business profitability	risk	performance
European Union Agency for Network and	Better process for creation and impleme	Technical aspects need for the use of matrices in a process	Authorized officials control the informati	Informed decision and competent security evaluative	Balanced resilience as improvements in the	Competent security acts as competitive	Cost of the secures standards can reduce	The framework is quantifiable, comparab

Information Security Standards (ENISA)	ntation of programs, metrics based		on that provides standard security system.	is ensured by this framework	resilience is confirmed through this framework	advantage	the profitability	le, and repeatable
Network Centric Warfare (NCW) Framework	Decision making issues and know how toward employees	The complexity of the framework is only weakness of the framework.	Information is controlled by the hubs as everyone able to see similar information	Decentralized decision making and awareness	Balanced resilience	Quality of collaborative decision ensures the profitability.	Jammed pathways can stop the flow of information	The framework is helpful to create understanding and quality of decision also improves
Network Centric Warfare (NCW) Framework	Decision making issues and know how toward employees	The complexity of the framework is only weakness of the framework.	Information is controlled by the hubs as everyone able to see similar information	Decentralized decision making and awareness	Balanced resilience	Quality of collaborative decision ensures the profitability.	Jammed pathways can stop the flow of information	The framework is helpful to create understanding and quality of decision also improves
IBM Business Resilience Model	Versatile hierarchy and more flexibility in operations.	Flexibility limitations of the business	Technologies, application, software, ERP,	Governing day to day business,	It identifies resilience capacity.	It ensures business continuity. The arrangement of the attributes protect and preserve the business activities.		It has the ability to identify, anticipate, evaluate and control the risk associated with compliance of social, economic, technical, environmental and regulatory factors.
National Academy of Science (NAS)	Cyber resilience and IT relationship	Cyber-attacks on the business practices.	IT management and other manager working on	Characterization of the risks like cyber-attacks and attacks on the	Balanced resilience for business practices	The framework provides information regardin	Lack of understanding	Performance in actual business practices to maintain

Framework			business practices	business practices		g IT and other business practices to reduce cyber-attacks on the business practices		all operation's security
Internet of Things (IoT)	Rapid knowledge, ease of working, ease of reach	Hacking attacks and software vulnerabilities and limitations	It is controlled by the networks and devices, passwords and security protocols are used	To provide on time information, reduce the stress of instant communication and many software that are used in financial management and products marketing	Unbalanced resilience due to more risks	Business can be profitable in case of using proper security measures	Hacking of information and business tactics	It performs faster while using efficient tools.
Internet of Things (IoT)	Rapid knowledge, ease of working, ease of reach	Hacking attacks and software vulnerabilities and limitations	It is controlled by the networks and devices, passwords and security protocols are used	To provide on time information, reduce the stress of instant communication and many software that are used in financial management and products marketing	Unbalanced resilience due to more risks	Business can be profitable in case of using proper security measures	Hacking of information and business tactics	It performs faster while using efficient tools.
Smart Dubai resilience Framework	Economic growth, infrastructure change and proper resources allocation	Network protocols attacks indicates its sensitivity	It is managed by central information center to spread the information effectively	To determine the right place of resources allocation, control over the infrastructure	It indicates balanced resilience	Economic growth indicates the business profitability	Skilled staff	It is performing properly to meet he needs of entire business structure

Linkove Framework	Need of information for further decision making	Highly vulnerable to cyber-attacks that enhances the external pressure	It works on the visual and procedural controls	The framework explains operational domains of information, and cognitive, physical, and social factors to develop resilience metrics	Unbalanced resilience	Business profitability in terms of security measures.	Attacks by the cyber hackers that can damage entire business	Operational security measures are provided by the framework efficiently
Kerr Framework	Better organizational resilience from core business	Strategic adaptability and robust governance and external pressure	Agile leadership takes the entire control of this framework	It has the capabilities of Strategic adaptability, Agile Leadership and Robust Governance	Balanced resilience due to the instant change implement	Costs are minimized that enhances agility in this framework	To achieve resilience in every function operational resilience, supply chain resilience, and information resilience are necessary to meet the challenges	Long lasting success of the business
Kerr Framework	Better organizational resilience from core business	Strategic adaptability and robust governance and external pressure	Agile leadership takes the entire control of this framework	It has the capabilities of Strategic adaptability, Agile Leadership and Robust Governance	Balanced resilience due to the instant change implement	Costs are minimized that enhances agility in this framework	To achieve resilience in every function operational resilience, supply chain resilience, and information resilience are necessary to meet the challenges	Long lasting success of the business

Hayslip Framework	Proper data inflow in the organization, storage of data, understanding of the data needs	Categorization of the data into different departments	Applications, hardware portfolio and centralized, categorized information system	Provides storage of data and inflow towards various stakeholders according to their requirements.	Balanced resilience	In case of proper data inflow the tasks will be easily performed by the each department	Hardware failure and cyber attacks	Proper delivery of information as well as understanding for various purposes.

The above table shows the practical implication of this research. The theoretical implication by testing the hypothesis of the research is as follows:

Table 7.50: Hypothesis testing details

Hypothesis details	**Impact on resilience**	**priority**	**Survey items**	**Outcomes**
The capability factors effect resilience in Smart government organizations.	the capabilities factors have 22% impact on the resilience	second	10	Supported
The forces of change factors effect resilience in smart government organizations.	the forces of change factors have 22% impact on the resilience	third	11	supported
The management control factors effect resilience in Smart government organizations.	The management control factors have 34% impact on the resilience	first (a priority)	12	Supported
The vulnerability factors effect resilience in Smart government organizations.	The vulnerability factors have 12% impact on the resilience	fourth	10	Supported

Theoretically, a wide range of factors come into play that can have an implication on the resilience of cybersecurity. The idea of cybersecurity resilience in the basic form is to conduct a thorough evaluation of what happens before, during, and after a digitally networked system faces a threat. The resilience of cybersecurity accrues over a long period of time, and it must be integrated with the strategy of a business organization. In the cyber-context, resilience basically helps organizations to be prepared so that they can face threats and vulnerabilities. An organization is said to have robust cybersecurity resilience if it is able to have an in-depth understanding of risks in strategic planning (Kwasinski, 2016). Thus, it has to go way beyond IT planning, and making a risk evaluation strategy should become a normal segment of its strategy.

Suggestions for further research:

1- Further studies should be carried out on the economic value of the relationship between resilience and cybersecurity: the thesis hypothesized the left side of the suggested model, whereas the right side needs to be hypothesized in further studies concerning business profitability, business continuity, financial loss and performance. These studies are talking more about the impact of balanced and unbalanced resilience from an economical point of view.
2- A comparative research on resilience framework in political stability contexts and political instability. As Smart Government projects primarily depend on the socio-economic status of the country, poor countries cannot apply them because nobody can use them due to the lack of money and lack of internet connection. Furthermore, countries with challenging political situations will have different perspectives on Smart Government projects given the fact that they lack democracy and other transparency issues with their public. This

relationship between the government and the public should be studied before initiating integrated governance, which needs more studies to be conducted in different political contexts in terms of stability.

3- Reapplying this framework on different regions and social contexts to validate that it is possible to use it in different countries and regions. As clarified earlier in this chapter this research and its suggested framework should be applied in different context and regions than the UAE, to check its validity and ability to work with different styles of Smart Government that have different perspectives about Smart Government and its cybernetic resilience.

7.2 Recommendations

- Cybersecurity risks when put in a business context reflects the reality of similarity between the traditional pre-automated and pre-internet business risk. Therefore, the risk should be viewed as a business problem, not a mechanical problem. In this case, the correct explanation ultimately focuses on the greatest risk. In the opinion of the government enterprise, currently controls it, as a rule, it would be prohibitively expensive if the government concentrates around each risk.
- Organizations with complex natures, in our case Smart Government, tends to have very unpredictable events and crisis in their environment. The proposed skeleton, i.e. a Smart Government framework, should recognize several levels of protection against potential threats. To exit the target zone, the government needs to create a series of solutions, constantly assessing risks and measuring vulnerabilities in order to be able to cope with them.

- The relationship between the citizen and the organization should be defined. The responses of the Smart Government are very limited. These problems can lead to distrust between the two parties such as public and government. As of the endless problems that may be caused by citizens due to cyber-attacks or a new concept of confidentiality in the new era of the internet.
- Readiness is developed by behaviours and beliefs of employees of the organization. It is recommended that the level of readiness should be increased throughout conducting resilience workshops and raise the awareness about this process. Due to lack of awareness on resilience cybersecurity risk management, the employees still think that the danger that comes with an electronic Smart Government system is not manageable nor measurable.
- Cybersecurity is hard to achieve because the internet infrastructure was built to serve connectivity not security in the first place. This puts a lot of pressure on Smart Government practitioners to keep its system safe by applying more systematic professional resilience frameworks to address this issue. It is recommended that the UAE, especially Dubai Smart Government, should start exercising resilience frameworks day after day to be able to achieve and maintain resilience once the Smart Government project is completed, for the sake of their system to be resilient to risk.
- Strategies should have been put technically not theoretically in the Dubai Smart Government resilience plan, whereas resilience professional plans consist of workshops and plans that can be exercised over and over again until your organization reaches a certain level of resilience.
- It is recommended that Smart Government organizations hire professionals and experts in business continuity, as they help in two ways: planning and readiness.

- To be able to manage risks, organizations should understand that when events occur, they could be somehow affected. It is also recommended that the organizations should prioritize risks and activities, recognizing the sustainability of risks to cybersecurity. They can also help organizations have a complete idea and make the right decisions regarding the financial and management costs in cybersecurity.
- It is recommended that efforts should be directed towards the development of sustainability, which are perceived as a new quality for the Smart Government system. For improving institutional quality, experience and resources are expected to lead to a recovery from the crisis. However, sustainability should still be a phased quality of the system, which can be gradually acquired and improved only through trial and error of its response to the future disasters or system failures.
- The cyber villains are growing faster than the security solutions. It is recommended that Smart Government projects should focus on four factors when applying resilience, management control, forces of change, vulnerabilities and capabilities. The resilience overall plan should serve the business continuity otherwise it will lead to a complete shutdown of the Smart Government organization.
- The Smart Government project in the UAE has the main goal of developing the business arena in the country; it also funds a lot of governmental and local departments, therefore it is recommended to study business profitability to protect it from financial loss. This can be achieved by balanced resilience which guarantees the avoidance of eroded profitability.
- The leadership should avoid traditional pathology in a crisis situation. For example, blaming others, waiting for facts and figures before making a decision, waiting for outside

help, sticking to the original plan or spreading rumours without verification about the e-governance.

- The focus should be on the program lifecycle, which should consist of an assessment stage, then a planning stage, and then perform exercises to reach a level of maturity and help with quick recovery to ensure the continuation of such a program.

- It is recommended that planners should be professionals in business continuity programs. Rather, they are experts in their field, which is part of a succession program. These important planners would help document important activities and differentiate information in their field to help the succession program and its owners in the e-governance framework. However, this goes beyond the priorities of their work and responsibilities, and the problems arising from this fact should have been explained earlier.

- It is recommended to emphasize the management control role instead of strategic management. The study shows that leadership and strategic management are not elements of program succession but resilience, management control, planners and resistance teams are.

- Research on integrated governance risks is rather limited, because of the wrong view of the public sector as rigid and risk-averse. In order to fully address the Smart Government main cybernetic issues, it is recommended that researchers should conduct more studies in this arena.

References

‘The Enterprise RISK Management of Cyber Security Conference’, (2017).

‘The USA Guardian Newspaper’ (2013).

‘USA Today Newspaper’ (2013).

Ackerman and Rushe, (2014). ‘Microsoft Handed the NSA Access to Encrypted Messages’.

Adger, W. N. (2000). Social and ecological resilience: Are they related? *Progress in Human Geography, 24:* 347–364.

'AGILIANCE TRANSFORMS CYBER SECURITY RISK MANAGEMENT' 2015, Computer Security Update, 16, 2, pp. 7-8, Academic Search Complete, EBSCOhost, (viewed 21 December 2016).

Aicholzer, G., & Schmutzer, R (2000). An interview of the change management process in Smart government organizational challenges to the development of electronic government. Proceedings of 11th International Workshop on Database and Expert Systems Applications, 79-83.

Alkuwaiti, S. (2017) *Information security strategy for smart government in United Arab Emirates – investigating future effectiveness, threats and vulnerabilities*. dissertation. British University in Dubai (BUiD).

Al Matrooshi, Shaikha Rashed Obaid Khalfan (2016) *The challenges of developing smart services projects in the United Arab Emirates*. dissertation. British University in Dubai (BUiD).

Amoroso, E., (2006). Cyber Security. New Jersey: Silicon Press.

Andrijcic, E. & Horowitz, B., (2006), 'A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property', Risk Analysis: An International Journal, 26, 4, pp. 907-923, Environment Complete, EBSCOhost, (viewed 21 December 2016).

Annarelli, A. & Nonino, F. (2016) Strategic and Operational Management of Organizational Resilience: Current State of Research and Future Directions, Omega, 62, pp. 1–1.

Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience: current state of research and future directions. Omega, 62, pp. 1-18.

Annon (2018). Strategic resilience: the secret to longevity, Strategic Direction, 34(6), pp. 28-29.

Anthopoulos, L. G. (2015). Understanding the smart city domain: a literature review, Springer nature Switzerland AG.

Arlitsch, K. & Edelman, A. (2014), 'Staying Safe: Cyber Security for People and Organizations', Journal Of Library Administration, 54, 1, pp. 46-56, Education Research Complete, EBSCOhost, (viewed 21 December 2016).

Bagheri, S. & Ridley, G. (2017). Organizational cyber resilience: research opportunities. Australasian Conference on Information Systems, 2017, Hobart, Australia. Available at: https://www.acis2017.org/wp-content/uploads/2017/11/ACIS2017_paper_238_FULL.pdf.

(Accessed: 17 January 2018).

Bandyopadhyay, K., Mykytyn, P. P. and Mykytyn, K., (1999) A framework for integrated risk management in information technology, *Management Decision 37(5)*, 437- 444.

Barab´asi,A.-L. (2003). *Linked: The new science of networks.* Cambridge, MA: Perseus Publishing.

Barrinha, A. (2016) "Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy," European Security, 25(3).

Battersby, ME 2015, 'Cybersecurity Risk Management 101', *EC&M Electrical Construction & Maintenance*, 114, 7, pp. C18-C22, Energy & Power Source, EBSCO*host*, (viewed 17 December 2016.)

Bayuk, L.J., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J., Weies, J. (2012). *Cyber security policy guidebook*. John Wiley & Sons Inc.

Belanger, F. and Hiller, J. S. (2006) A framework for Smart government: privacy implications, *Business Process Management Journal, 12(1),* 48-60.

Blanchet, K., Nam, S., Ramalingam, B., & Martin, F. (2017). Governance and Capacity to Manage Resilience of Health Systems: Towards a New Conceptual Framework. International Journal of Health Policy Management, 6(8), 431-435.

Blowers, M., Iribarne, J., Colbert, E. & Kott, A. (2016). The future internet of things and security of its control systems. Available at: https://webcache.googleusercontent.com/search?q=cache:WuOX0wSzPyEJ:https://arxiv.org/pdf/1610.01953+&cd=4&hl=en&ct=clnk&gl=ae. (Accessed: 20 January, 2018).

Boin, A. and McConnell, A. (2007) Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience, *Journal of Contingencies and Crisis Management (15),* 50-59

Bosen, M. (2017). Cyber resilience: implementing smart security to match smart city developments. Available at: http://www.intelligentcio.com/me/2017/10/19/cyber-resilience-implementing-smart-security-to-match-smart-city-developments/. (Accessed: 27 January 2108)

Bradley, V. and Pratt, R. (2011) *Exploring the Relationships Among Corporate Entrepreneurship, IT Governance, and Risk Management,* Proceedings of the 44th Hawaii International Conference on System Sciences

Britt, P. (2017). Cyber security Risk Management: Finding and Fixing Your Security Vulnerabilities. Retrieved from https://www.esecurityplanet.com/network-security/cybersecurity-risk-management.html

Bucy, E. P., & Gregson, K.S. (2001). Media participation, A legitimize mechanism of mass democracy. New Media & Society, 3 (3), pp. 357-380

Business Dictionary accessed online. Read more: http://www.businessdictionary.com/definition/risk-management.html

Bouaziz, F. & Hachicha, Z. S. (2018). Strategic Human Resource Management Practices and Organizational Resilience, Journal of Management Development, 37(7), pp. 537–551.

Buliga, O., Christian, W. S., & Voigt, K. (2018). Business model innovation and organizational resilience: towards an integrated conceptual framework, Journal of Business Economics, 86, pp. 647-670.

Cardenas, A. A., Amin, S., Sinopoli, B., Giani, A., Perrig, A. & Sastry, S. (n. d). Challenges for securing physical systems. Available at: https://pdfs.semanticscholar.org/d514/97e5827cc00d9d00c26e27a769d42284cfba.pdf. Accessed: 25 January 2018.

Cavelty, M. D., Kaufmann, M. & Kristensen, K. S. (2015). Resilience and (in)security: practices, subjects, temporalities. *Security dialogue,* Vol. 46, No. 1, pp. 3-14.

Chandler, D. (2014). Resilience: The governance of complexity. Rutledge.

Chanopas, A., Krairit, D. & Khang, D.B. (2006) Managing information technology infrastructure: a new flexibility framework, *Management Research News, 29 (10),* 632-651.

Chertoff, M 2014, 'Managing Cyber Risk in Today's Security Landscape', Electric Perspectives, 39, 6, pp. 36-38, Business Source Complete, EBSCOhost, (viewed 21 December 2016).

Chirstou, G. (2016). Cybersecurity in European Union: resilience and adaptability in governance policy: Springer.

CISCO (2011). Cyber–security: build trust, visibility, and resilience. Available at: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/cybersecurity_bvr_wp.pdf. (Accessed: 27 January, 2018).

Cocchiara, R. (2005) *Beyond disaster recovery: becoming a resilient business. An object-oriented framework and methodology*, IBM Global Services

Cohen, B. & Kietzmann, J. (2014). Ride on! Mobility business models for the sharing economy. . Organization & Environment, 27 (3), 279-296.

Coleman, S. et al. (1999). Parliament in the age of the internet. Parliamentary Affairs, 52.

Collier, Z., Linkov, I. & Lambert, J. (2013), 'Four domains of cybersecurity: a risk-based systems approach to cyber decisions', Environment Systems & Decisions, 33, 4, pp. 469-470, Environment Complete, EBSCOhost, (viewed 21 December 2016).

Conteh, N. & Schmick, P. (2016), 'Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks', International Journal Of Advanced Computer Research, 6, 23, pp. 31-38, Computers & Applied Sciences Complete, EBSCOhost, viewed 21 December 2016.

'Cyber security skills for the next generation' 2014, Education Journal, 194, p. 6, British Education Index, EBSCOhost, (viewed 21 December 2016).

Campbell, K., Keating, A., Ianni, F., Szcoenyi, M., Etienne, E., Velev, S. & McQuistan, C. (2019). Lessons Learned from Measuring Flood Resilience.

Cyber-Security & Risk Management, an evolving ecosystem, (2016)

Bodeau, D. J. & Graubart, R. (2011), "Cyber resiliency engineering framework," The MITRE Corporation.

Devadoss, P., Pan, S. & Huang, J. (2002). Structurational analysis of Smart government initiatives: A case study of SCO. Decision Support Systems, vol. 34 (3), pp. 253-269.

Dolicanin, C. (2014). *Handbook of research on democratic strategies and citizen-centered e-government services*.

Douglas M. Lambert and A. Michael Knemeyer, "We're in This Together," Harvard Business Review, Vol. 82, No. 12 (2004), pp. 114-122.

Drabek, T.E. (1986) *Human System Responses to Disaster: An Inventory of Sociological Findings*, New York: Springer.

Drew, J. (2012), 'Managing Cybersecurity Risks', Journal Of Accountancy, 214, 2, pp. 44-48, Business Source Complete, EBSCOhost, (viewed 21 December 2016).

Dess, G. G., Peng, M. W. & Lei, D. (2013). Strategic Management: Current Issues and Future Directions, Journal of Leadership & Organizational Studies, 20(4), pp. 373–374.

Dess, G. G., Peng, M. W., & Lei, D. (2013). Strategic management: current issues and future directions, Journal of Leadership & Organizational Studies, 20(4), pp. 373-374.

Dubai Smart government Booklet (2008). Making life easier. A definitive booklet about Dubai Smart government project and services, 8-15.

Emirates 24/7 News (2017). Sheikh Mohammed launches 'Dubai Cyber Security Strategy'. Available at: http://www.emirates247.com/news/emirates/sheikh-mohammed-launches-dubai-cyber-security-strategy-2017-05-31-1.653840. (Accessed: 27 January 2018).

ENISA (2011). Measurement framework and metrics for resilient network and services: challenges and recommendations. Available at: https://www.enisa.europa.eu/publications/metrics-tech-report/at_download/fullReport. (Accessed: 17 January 2018).

Epper Hoffman, K. (2014), 'FOLLOWING THE FRAMEWORK', SC Magazine: For IT Security Professionals (15476693), 25, 6, pp. 22-25, Computers & Applied Sciences Complete, EBSCOhost, (viewed 21 December 2016).

Esterbay-Smith, M., Thorpe, R., & Jackson, P. R. (2015). 'MANAGEMENT AND BUSINESS RESEARCH' (5th ed). Pp 46-50. SAGE

Esteves J. and Joseph R. C. (2008) A comprehensive framework for the assessment of Smart government projects. *Government Information Quarterly, 25,* 118–132.

Featherman, M. and Pavlou, P. (2003) Predicting e-services adoption: a perceived risk facets perspective, *International Journal of Human -Computer Studies, 59,* 451–474.

Fretz, W. (ed). (1999). Electronic commerce and the transformation of marketing. Internet-Marketing, pp. 55-80, Stuttgart: Schaffer-Poeschel.

From the Editors, Managing Risk and resilience, Academy of Management Journal 2015, Vol. 58, No. 4, 971–980.

G. Klein, "Sources of Power: how people make decisions," MIT Press Cambridge, Massachusetts, (1998).

Gartner (n. d). The Internet of Things. Available at: https://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf. (Accessed: 20 January 2018)

Gerben, V., Peter, E., Margareta, W. & Gerard, G. (2015). Managing risk and resilience. Academy of Management Journal, 8(4), 971-980.

Gil-Garcia, R., and Pardo, T. (2005) Smart government success factors: Mapping practical tools to theoretical foundations. *Government Information Quarterly, 22,* 187–216.

Greenaway, K., Chan, Y. & Crossler, R. (2015), 'Company information privacy orientation: a conceptual framework', Information Systems Journal, 25, 6, pp. 579-606, Computers & Applied Sciences Complete, EBSCOhost, viewed 21 December 2016.

Guo Y., Fang D., and Chen, J. (2009) *Effect of IT Capability on IT Project Risk*, International Conference on Management and Service Science.

Guth, W. D. (1981). Strategic Management, Strategic Management Journal, 2(2).

Holtz, S. (1999). *Public Relation on the net: winning strategies to inform and influence the media, the investment community, the government, the public and more.* (1st ed), NEW YORK, NY: AMAKOM

Holtz, S. (2002). *Public Relation on the net: winning strategies to inform and influence the media, the investment community, the government, the public and more.* (2nd ed), NEW YORK, NY: AMAKOM

Hyslip, G. (2016), Cyber-Security and Risk Management, an evolving ecosystem. CISO, City of San Diego.

Hirani, S., Lasiuk, G., & Hegadoren, K. (2016). The intersection of gender and resilience. *Journal of psychiatric and mental health nursing*.

Holm, J. R., & Østergaard, C. R. (2015). Regional employment growth, shocks and regional industrial resilience: a quantitative analysis of the Danish ICT sector. *Regional Studies*, *49*(1), 95-112.

Harrington, R. J. & Ottenbacher, M. C. (2011). Strategic management – an analysis of its representation and focus in recent hospitality research, International Journal of Contemporary Hospitality Management, 23(4), pp. 439-462.

Iribarren, M., Concha, G., Valdes, G., Solar, M., Villarroel, M.T., Gutiérrez, P. and Vásquez, Á. (2008) Capability Maturity Framework for Smart government: A Multi-dimensional Model and Assessing Tool, *E-Governance LNCS, 5184*, 136–147.

Ishak, A. W. & Williams, E. A. (2018). A Dynamic Model of Organizational Resilience: Adaptive and Anchored Approaches, Corporate Communications: An International Journal, 23(2), pp. 180–196.

IT Governance. (2017). Cyber Resilience. Retrieved from https://www.itgovernance.co.uk/cyber-resilience.

Jarrow, R.A. (2011), 'Risk Management Models: Construction, Testing, Usage', Journal Of Derivatives, 18, 4, pp. 89-98, Business Source Complete, EBSCOhost, viewed 21 December 2016.

Jenab, K, & Moslehpour, S. (2016), 'Cyber Security Management: A Review', Business Management Dynamics, 5, 11, pp. 16-39, Business Source Complete, EBSCOhost, viewed 21 December 2016.

Johnson, B. (1994). Prove public relations affects the bottom line. *Public Relations Journal*, vol. 50 (4), pp. 31-40.

Kerr, H. (2016, July). Organizational resilience, Harnessing Experience, embracing opportunity, *Quality*, 40-43, Available at: www.qualitymag.com

Keys, B., Chhajer, A., Liu, Z., & Honer, D. (2016). A framework for assessing cyber resilience. World Economic Forum.

Keys, B., Chhajer, A., Liu, Z., & Horner, D. (2016). A framework for assessing cyber resilience: a report for the World Economic Forum. Available at: http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf. Accessed: 17 January, 2018.

Kim, H. J., Pan, G. and Pan, S. L. (2007) Managing IT-enabled transformation in the public sector: A case study on Smart government in South Korea, *Government Information Quarterly, 24*, 338–352.

Kwasinski, A. (2016). Quantitative model and metrics of electrical grids' resilience evaluated at a power distribution level. *Energies*, *9*(2), 93.

Kothari, C. (2004). Research methodology: Methods and techniques. New Age International.

Kumar, S., & Phrommathed, P. (2005). Research methodology. Springer US.

Kumari, L. and Kumar, R. (2015) *Impact of Cyber Security in different application of e-Governance: Case Study.* Proceedings of the 4th International Conference on System Modeling & Advancement in Research Trends (SMART) College of Computing Sciences and Information Technology (CCSIT), Teerthanker Mahaveer University, Moradabad

Kantur, D. & Iseri-Say, A. (2015). Measuring organizational resilience: a scale development, journal of business, economics, & Finance, 4(3), pp. 456-472.

Kerr, H. (2016). Organizational resilience: harnessing experience, embracing opportunity. Quality, July 2016, pp. 40-43.

Langfield-Smith, K. (2008). The relations between transactional characteristics, trust and risk in the start-up phase of a collaborative alliance, *Management Accounting Research, 19,* 344–364.

Lanz, J. (2016), 'Communicating Cybersecurity Risks to the Audit Committee', CPA Journal, pp. 6-10, Business Source Complete, EBSCOhost, viewed 21 December 2016.

Leck, H. (2014), 'THE IMPORTANCE OF RISK MANAGMENT FOR MANAGERS', Managerial Challenges Of The Contemporary Society, 7, 1, pp. 119-124, Business Source Complete, EBSCOhost, viewed 21 December 2016.

Leautier & Rochet (2014). On the strategic value of risk management, International Journal of Industrial Organization, 37, pp. 153-169.

Leyesdorff, L. & Deakin, M. (2011). The Triple-Helix Model of smart cities: a neo-evolutionary perspective, Journal of Urban Technology, Vol. 18, pp. 53-63.

Linkov, I., Iesenberg, D. A., Plourde, K., Seager, T. P., Allen, J. & Kott, A. (2013b). Resilience metrics for cyber systems, *Environment Systems and Decisions,* Vol. 33, No. 4, pp. 471-476.

Linkov, I., Senberg, D., Bates, M., Chang, D., Convertino, M., Flynn, S. & Seager, T. (2013). Measurable resilience for actionable policy, *Environmental Science and Technology,* Vol. 47, No, 18. Pp. 10108-10110.

Longstaff, P.H. (2005) *Security, Resilience and Communication in Unpredictable Environments such as Terrorism, Natural Disasters and Complex Technology*, Program on Information Resources Policy, Center for Information Policy Research, Harvard University, URL: http://www.pirp. harvard.edu.

Marvell, S. (2015), 'RISK MANAGEMENT', Itnow, 57, 4, pp. 26-27, Computers & Applied Sciences Complete, EBSCOhost, viewed 21 December 2016.

Matook, S., Lasch, R. & Tamaschke, R. (2009) Supplier development with benchmarking as part of a comprehensive supplier risk management framework, *International Journal of Operations & Production Management, 29(3),* 241-267

Maughan, D. (2010), 'Inside Risks The Need for a National Cybersecurity Research and Development Agenda', Communications Of The ACM, 53, 2, pp. 29-31, Business Source Complete, EBSCOhost, viewed 21 December 2016.

Montagna, J. M. (2005) A framework for the assessment and analysis of electronic government proposals. *Electronic Commerce Research and Applications, 4,* 204–219.

Mienipre, A., Nwuche, C. A. & Anyanwu, S. A. C. (2016). Talent management and organizational resilience in manufacturing firms in Port Harcourt, The International Journal of Business and Management, 4(3), pp. 135-145.

Morais-Storz, M., Platou, R.S. & Norheim, K.B. (2018). Innovation and metamorphosis towards strategic resilience, International Journal of Entrepreneurial Behavior & Research, 24(7), pp. 1181-1199.

Moller, K., Schaffer & Verbeeten, F. (2020). Digitalization in management accounting and control: an editorial. *Journal of Management Control,* **31**(1-2), pp. 1-8

Nag, R., Hambrick, D. C. & Chen, M. J. (2007). What is strategic management really? Inductive derivation of a consensus definition of the field, Strategic Management Journal, 28(9), pp. 935-955.

Leveson, N. (2002) "A new approach to system safety engineering," Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.

Nastasiu, C. (2016), 'CYBER SECURITY STRATEGIES IN THE INTERNET ERA', Proceedings Of The Scientific Conference AFASES, 2, pp. 619-624, Academic Search Complete, EBSCOhost, viewed 21 December 2016.

National Institute of Standards and Technology (2017). Framework for improving critical infrastructure Cyber security. Available at: https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf. Accessed: 21 January 2018.

Newman, S. (2007), 'Cyber Security--Are You Prepared?', Techniques: Connecting Education And Careers, 82, 4, pp. 22-25, ERIC, EBSCOhost, viewed 21 December 2016.

Newnham, C. & Crask, J. (2015) *Emerging Capability every business needs: the art and science of enterprise resilience*, available at: www.pwc.com/resilience

NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009, p. 1

North, J. N., Pascoe, R. & Westgarth, C. C. (2016). Cyber security and resilience – it's all about governance. Available at: file:///C:/Users/DELL2/Downloads/cyber_security_resilience_governance_april_2016.pdf. Accessed: 26 January 2018.

Öğüt, H., Raghunathan, S. & Menon, N. (2011), 'Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection', Risk Analysis: An International Journal, 31, 3, pp. 497-512, Environment Complete, EBSCOhost, viewed 21 December 2016.

Oliver, L. & Sanders, L. (2014). *E-governance reconsidered: Renewal of governance for the knowledge age*. Regina: Canadian Plain Research Centre, University of Regina.

Olson, A., Anderson, J. (2016). Resiliency Scoring for Business Continuity Plans. J Bus Contin Emer Plan. 2016;10(1):31-43.

Onwuldike, O., Lock, R. & Phillips, I. (2015). Measuring the Resilience of Smart governments Using an Ontology. International Journal of Humanities and Social Science, 9(12), 1-10.

Orlikowisky, W.J. & Robey, D. (1991). Information technology and the structuring of organizations. Information System Research, 2 (2), pp. 143-69.

Pan, S.L., Pan, G., & Devadoss, P. (2005). Smart government capabilities and crisis management: Lessons from combating SARS in in Singapore. MIS Quarterly Executive, 4 (4), 385-397.

Papa, R., Galderisi, A., Majello, M. C. V. & Saretta, E. (2015). Smart and resilient cities, Journal of Land use, mobility, and environment, 1, pp. 1-36.

Pauchant, T.C. & Mitroff, I.I. (1992) *Transforming the Crisis Prone Organization: Preventing Individual, Organizational and Environmental Tragedies*, San Francisco: Jossey-Bass.

Peffers, K., Tuunanen, T., Rothenberger, M. & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24 (3), 45-77.

Pennathur, A.K. (2001), "Clicks and bricks': e-Risk Management for banks in the age of the Internet', Journal Of Banking & Finance, 25, 11, pp. 2103-2123, Business Source Complete, EBSCOhost, viewed 17 December 2016.

Pico, Y., Alfarhan, A. & Barcelo, D. (2019). Nano-and microplastic analysis: Focus on their occurrence in freshwater ecosystems and remediation technologies. *Trends in analytical chemistry*.

Ratnasingham, P. (1999) Risks in Low Trust Among Trading Partners in Electronic Commerce, *Computers & Security, 18*, 587-592.

Rahman, M.H., Low, K.C.P., Almunawar, M.N., Mohiddin, F. & Sik-Leong, A. (2012). Egovernment policy implementation in Brunei: lessons learnt from Singapore. In Manoharan, A. and Holzer, M. (eds) *Active Citizen Participation in E-Government: A Global Perspective*, Hershey, USA: IGI Global, 359-377.

Rechtman, Y. & Rashbaum, K. (2015), 'Cybersecurity Risks to CPA Firms', CPA Journal, 85, 5, pp. 54-57, Business Source Complete, EBSCOhost, viewed 21 December 2016.

Ridley, J., & Channing, J. (1999), 'RISK MANAGEMNET', pp. 71-81, UK: Butter Worth Heinemann. ELSEIVER.

Rotchanakitumnuai, S. (2007) *The important risk factors of Smart government service adoption*, International Conference on Wireless Communications, Networking and Mobile Computing, 2007.

Ross, J. W., Beath, C. M. & Sebastian, I. M. (2017). How to develop a great digital strategy. *MIT Sloan Management Review*, *58*(2), 7

Ruggeri, R. (2016), 'Risks in Cybersecurity', *Public Relations Tactics*, 23, 12, p. 13, Business Source Complete, EBSCO*host*, viewed 17 December 2016.

Ruizhong, D., Xiaoxue, M. &Zixian, W. (2010) *Dynamic Trust Model based on Perceived Risk*, International Conference on E-Business and Smart government.

Scholl, H. J. & AlAwadhi, S. (2016). Creating smart governance: the key to radical ICT overhaul at the city of Munich, information Policy, Vol. 21, pp. 21-42.

Schroeder, H. (2014). An Art and Science Approach to Strategic Risk Management, Strategic Direction, 30(4), pp. 28–30.

Sonnet, M. T. (2016). Employee behavior, beliefs, and collective resilience: an exploratory study in organizational resilience capacity, Human and Organizational Systems, Fielding Graduate University.

Saunders, M., Lewis, P. & Thornhill, A. (2007). Research methods for business students (6th ed.). Harlow: Pearson Education.

Schipper, E. L. F. & Langston, L. (2015). A comparative overview of resilience measurement frameworks. *Analysing indicators and approaches. Overseas Development Institute*.

Schell, R.R. (2016), 'Cyber Defense Triad for Where Security Matters', Communications Of The ACM, 59, 11, pp. 20-23, Business Source Complete, EBSCOhost, viewed 21 December 2016.

Schneider, R. (2010) A Comparison of Information Security Risk Analysis in the Context of Smart government to Criminological Threat Assessment Techniques. *InfoSecCD' 10*, Kennesaw, GA, USA.

Sikula, N.R., Mancillas, J.W., Linkov, I. & McDonagh, J.A. (2015). Risk management is not enough: a conceptual model for resilience and adaptation-based vulnerability assessments. Environment Systems & Decisions, 35(2), pp. 219-228.

Smart Government in Dubai Booklet (2010).

Sussan, F. & Acs, Z. J. (2017). The digital entrepreneurial ecosystem. *Small Business Economics, 49*(1), 55-73.

Spalević, Ž. (2014), 'CYBER SECURITY AS A GLOBAL CHALLENGE TODAY', Singidunum Journal Of Applied Sciences, pp. 687-692, Business Source Complete, EBSCOhost, viewed 21 December 2016.

Stolfo, S. J., Frias-Martinez, V. & Keromytis, A. D. (2008). Behavior-based network access control: a proof-of-concept *Lectus Note sin Computer Science, No. 5222: Information Security* pp. 175-190. Springer-Verlag.

Tapscott, Lowy, A. & Ticoll, D. (Eds), (1989). Blueprint to the digital economy. New York, NY: McGraw-Hill.

Taylor, S., Bogdan, R. & DeVault, M. (2015). Introduction to qualitative research methods: A guidebook and resource. John Wiley & Sons.

Teece, D., Pisano, G. & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, vol. 18 (7), pp. 509-533

'The Cybersecurity Risk' 2012, Communications Of The ACM, 55, 6, pp. 29-32, Business Source Complete, EBSCOhost, viewed 21 December 2016.

Van Der Vegt, G. S., Essens, P., Wahlström, M. & George, G. (2015). Managing risk and resilience.

Vucina, D. & Fabac, R. (2017). Organizational resilience and risk management improvement – how to reduce and prevent fire hazard using simulation scenarios. International Scientific Conference on economic and Social Development, Madrid, 15-16 September.

Wilson, R. L. (2010). Organizational resilience models applied to companies in bankruptcy, university of Maryland university College.

Walser, K., Kühn, A. & Riedl, R. (2009) *Risk management in Smart government from the perspective of IT governance.* The Proceedings of the 10th International Digital Government Research Conference.

Widmer, L. (2013), 'IS RISK MANAGMENT OBSOLETE', Risk Management (00355593), 60, 3, pp. 35-38, Computers & Applied Sciences Complete, EBSCOhost, viewed 17 December 2016.

Woods, M. (2009) A contingency theory perspective on the risk management control system within Birmingham City Council, *Management Accounting Research, 20,* 69–81.

Yan Pillitteri, V. (2014), 'NIST Cybersecurity Framework Addresses Risks to Critical Infrastructure', Electroindustry, 19, 6, pp. 20-21, Energy & Power Source, EBSCOhost, viewed 21 December 2016.

Yaich, A. (2016). La resilience pour s'adapter dans un environemtn difficile, La Revue Comptable et Financiere, No. 112, pp. 1-2.

Yoon, D. K., Kang, J. E. & Brody, S. D. (2016). A measurement of community disaster resilience in Korea. *Journal of Environmental Planning and Management*, *59*(3), 436-460.

Zamoum, K. (2007), '*Dubai Smart government website evaluation'* pp.13-17

Appendix 1:

"Smart Government Resilience & Cyber Security Risk management"

Survey Questionnaire

Section 1 (a) - Demographic information s

1. Gender: Male [1] Female [2]
2. Age: 18-30 [1] 31-40 [2] 41-50 [3] over 50 years [4]
3. Education Level: Secondary [1] Diploma [2] Bachelor's degree [3] Master's Degree [4] PhD [5]
4. Employment Status: Casual [1] Permanent [2] Contract [3]
5. Duration of Employment: Less than 5 Years [1] 5-10 Years [2] 11-15 Years [3] Over 15 years [4]
6. Department: Administration [1] Finance [2] IT [3] Other [4]

Section 1 (b) – General Questions

In the table below, using the scale provided, please tick if you agree or disagree, with (1-Strongly agree; 2-Agree; 3-Not Sure; 4-Disagree; 5-Strongly Disagree)

	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
1. Risk Management in Information Communication Technology Applications will bring about a lot of benefits to the Institution	5	4	3	2	1
2. Smart governance organizations are need better resilience and risk management policies					

3. The resilience management in smart government organizations will bring flexibility in cyberspace, and continuity of organizational functions despite the cyber attack					
4. There are more risks than benefits attributed to the whole process of Smart Governance					
5. The changing environment and relations in society require smart government organizations in the UAE to focus on better resilience policies					
6. Smart Governance introduces improved techniques and processes to the organization					
7. Smart governance organizations should consider implementation of effective resilience					
8. Better management control in smart governance organizations can create capabilities and resilience against cyber attacks					
9. Multiple layers to foster resilience will result in shorter network and system downtimes.					

10. The government is focusing on cyber resilience to avoid threats in changing cyber environment					
11. Smart Governance Platforms is generally vulnerable to common attacks such as Denial of Service Attacks.					
12. Smart Governance Platforms will result in a greater uptake of cloud based resources by the average person.					
13. Smart Governance Platforms will be able to accurately predict the unique needs of individual students, instead of providing generic answers.					
14. The current ICT policies and frameworks that guide the system are inadequate due to lack of resilience polices and risk management strategy					
15. Smart governance organizations of the UAE need effective policies and frameworks for the system					

Section 2 – Importance of Resilience and Risk Management

1. The smart Governance Platform will enable the institution to maintain its competitive advantage across all spheres of service provision.	5	4	3	2	1

2. The smart Governance Platform will improve service consistency, continuity and overall quality at a minimal cost.					
3. Risk Management interventions will prevent the institution from being exposed to costly legal proceedings in case of data breaches.					
4. The smart Governance Platform will offer real time feedback and 24/7 access and resource provision.					
5. Improved risk management and resilience will enhance performance of employees					
6. Risk management will be beneficial for all stakeholders					

Section 3 – Benefits of Resilience and Risk Management

	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
7. Resilience and Risk Management will result in better mitigation, reduction or elimination of cyber related attacks	5	4	3	2	1
8. Better policies for Cyber resilience will help smart government					

organizations to recover quickly from any cyber attack					
9. The regularity authorities of the country should pay attention enhance infrastructure resilience in smart government organizations					
10. The federal government of the UAE is aware of the importance of resilience and cyber security management in smart government organizations					
11. The purpose of cyber security domain in smart government organizations is to build control for making cyberspace secure					
12. Smart Governance will introduce a high rate of resilience in institutional platforms and virtual services provided.					
13. The smart Platform will result in faster and more specific responses to stakeholders					
14. Smart Governance Platforms will introduce more secure data storage and data management to this facility.					
15. The smart Governance Platform will enable the institution to focus its					

resources and energy on core activities rather than peripheral ones.					
16. The smart Governance Platform will result in capacity building, better knowledge transfer and the creation of new skill sets for the stakeholders.					

Section 4 – Risks due to lack of resilience and risk management

	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
1. Existing and evolving Cyber Security Threats will make the smart government organizations vulnerable	5	4	3	2	1
2. The smart Platform may cause the institution will to lose reliable and more talented staff who may not be that tech savvy, and introduce untrusted third parties.					
3. External Service Providers for the smart Governance Platform cannot always reliable and consistent services.					
4. The introduction of the smart Governance platform may result in a dearth of interpersonal skills from minimal staff recruitment.					

5. In the event of a data breach, massive volumes of sensitive data could be get exposed to the public domain.					
6. Resilience and risk management in smart government organization will enhance the capacity of the system to perform better even if there are issue in cyber environment					
7. Resilience in smart government organizations will improve performance and output					
8. The safe environment created by risk management will enhance technical competence in smart government organizations					

Section 5 – Performance of smart government organizations after resilience and risk management

	Strongly Agree	Agree	Not Sure	Disagree	Strongly disagree
1. The overall performance of my organization will improve with the introduction or smart Governance resilience and risk management interventions	5	4	3	2	1
2. I think the organization will perform extremely well in the core functions because of the introduction of an					

smart Governance resilience and risk management policies					
3. The institution will greatly benefit from the new knowlege base and new skill requirements, occasioned by the introduction of an smart Governance risk management strategy					
4. The smart governance Platform and associated Risk Management interventions will improve the overall satisfaction of the students and staff to the institution's service provision.					
5. The introduction of the smart Governance risk management will result in higher profit margins and reduced operational costs.					

Section 6 - Framework and Hypothesis Testing

	Strongly Agree	Agree	Not Sure	Disagree	Strongly disagree
1. There are differences between smart government organizations in terms of using resilience and cyber security risk management	5	4	3	2	1
2. The capability factors affect resilience in smart government organizations					

3. The change factors effect resilience in smart government organizations					
4. The management control factors effect resilience in smart government organizations					
5. The vulnerability factors effect resilience in smart government organizations					
6. The resilience framework is about detecting, preventing, and recovering from a cyber-attack					
7. The forces of change cause vulnerabilities that provoke the need for resilience in organizations					
8. The implementation of balanced resilience can result in improved performance					
9. Unbalanced resilience in organizations can impose excessive frisks and erode profitability					
10. The resilience can help organizations in evaluating risks and challenges involved at multiple levels					

Appendix 2

"Smart Government Resilience & Cyber Security Risk management"

Descriptive Statistics

Demographics of Participants
Gender of participant

Gender

		Frequency	Percent
Valid	Male	197	45.6
	Female	231	53.5
	Total	428	99.1
Missing	System	4	.9
Total		432	100.0

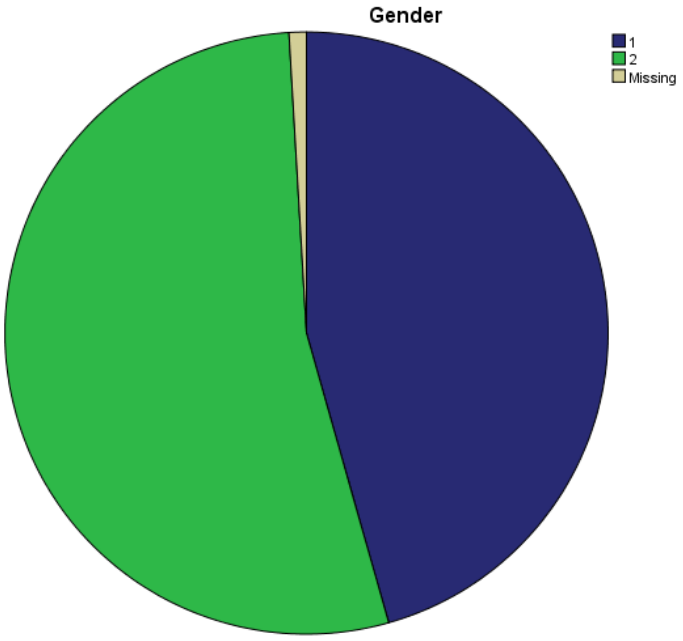

Figure 2: Gender

As per the figure given above, there were 432 participants in total in the survey. 45% of the participants were males, whereas 53% of the participants were females. As per given data in both chart and table, it is demonstrated that the majority of participants were females.

Age of Participants

Age

		Frequency	Percent
Valid	25-30	202	46.8
	31-40	138	31.9

	41-50		60	13.9
	Over 50 years		25	5.8
	Total		425	98.4
Missing	System		7	1.6
Total			432	100.0

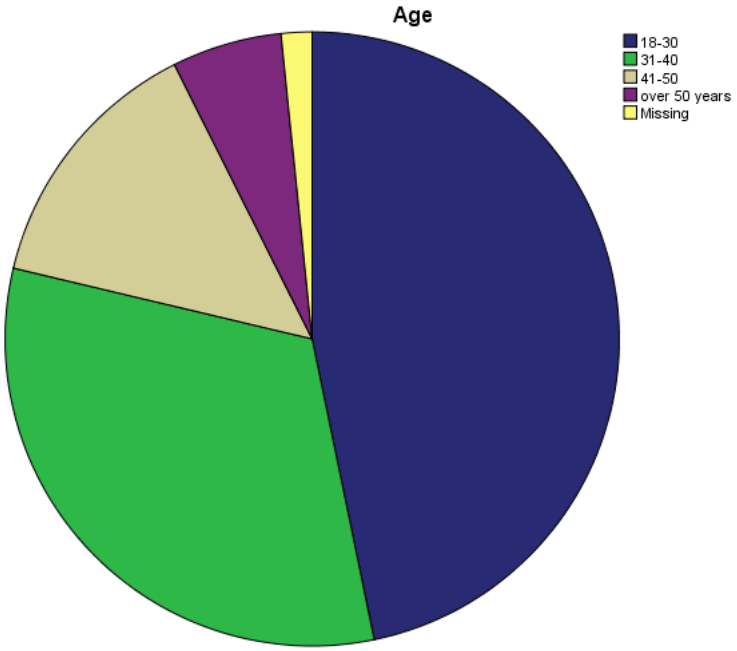

Figure 3: Age

As per the data given above, there were 432 participants in total in the survey. 46% of the participants were between 25-30 years of their age, 31% were 31-40, 13% were in 41-50 and 5.8% were above 50 years. As per the given data in both chart and table, it is demonstrated that the majority of participants were in the age bracket of 25-30.

Education Level of Participant

Education Level

		Frequency	Percent
Valid	Secondary	94	21.8
	Diploma	75	17.4
	Bachelor's degree	183	42.4
	Master's Degree	55	12.7
	PhD	21	4.9
	Total	428	99.1
Missing	System	4	.9
Total		432	100.0

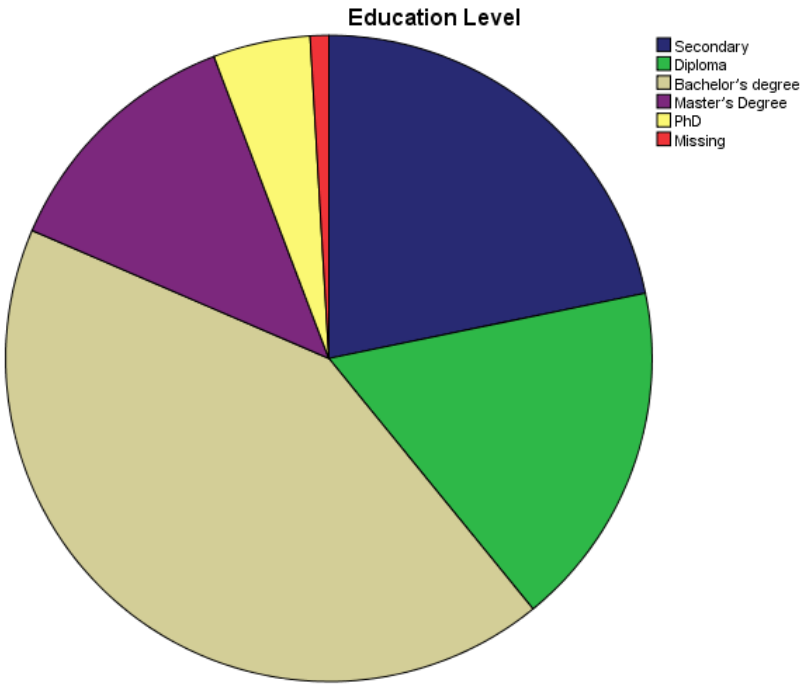

Figure 4: Educational Level

As per the data given above, there were 432 participants in total in the survey. 21.8% of the participants were secondarily educated, 17% were diploma, 42% were bachelors, 12% were in masters, and 4.9% were Ph.D. As per the given data in both chart and table, it is demonstrated that the majority of participants were in the bachelor degree.

Employment Status of Participants

Employment Status

		Frequency	Percent
Valid	Casual	160	37.0
	Permanent	164	38.0
	Contract	100	23.1

	Total	424	98.1
Missing	System	8	1.9
Total		432	100.0

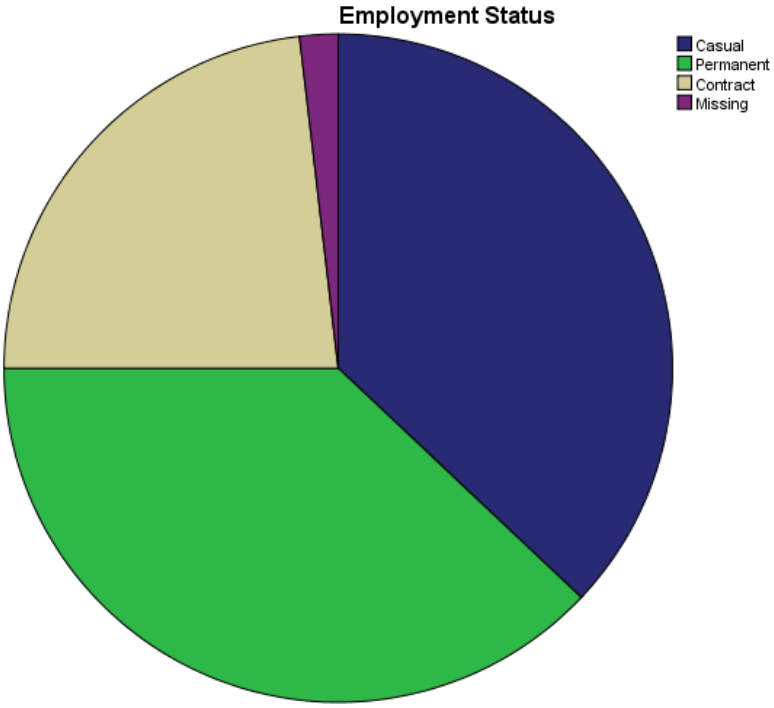

Figure 5: Employment Status

As per the data given above, there were 432 participants in total in the survey. 37.% of the participants were casual employees, 38% were permanent employees, 42% were contract-base employees. As per the given data in both chart and table, it is demonstrated that the majority of participants were in the permanent employment.

Duration of Employment of Participant

Duration of Employment

		Frequency	Percent
Valid	Less than 5 Years	191	44.2
	5-10 Years	100	23.1
	11-15 Years	64	14.8
	Over 15 years	72	16.7
	Total	427	98.8
Missing	System	5	1.2
Total		432	100.0

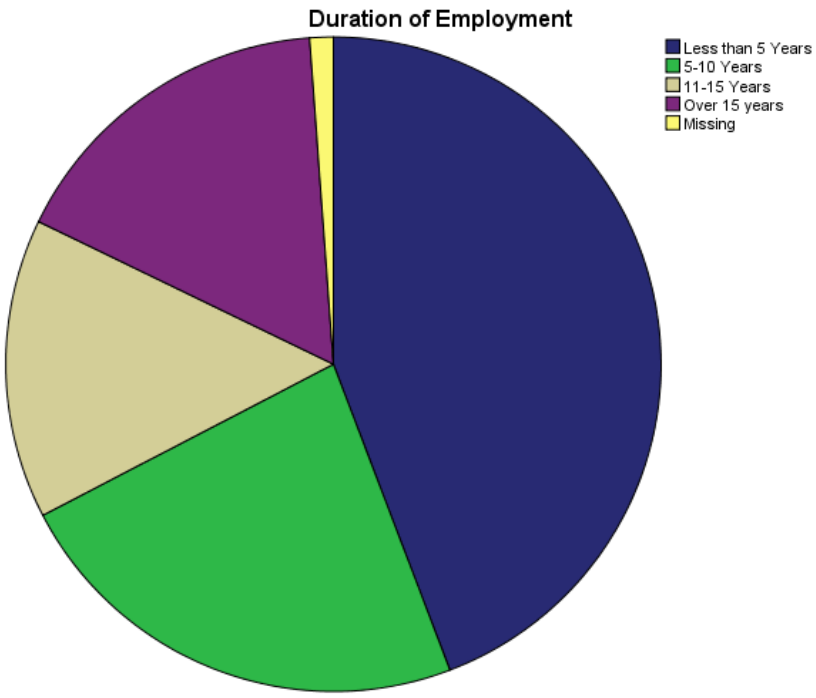

Figure 6: Duration of Employment

As per the data given above, there were 432 participants in total in the survey. 44.% of the participants were less than 5, 23% were in between 5-10, 14% were between 11-15, 16% were over 15 years, in terms of the period of their employment. As per the given data in both chart and table, it is demonstrated that the majority of participants were in the less than 5 years of the period in terms of their employment.

Department of Participants

Department

		Frequency	Percent
Valid	Administration	83	19.2
	Finance	46	10.6
	IT	59	13.7
	Other	238	55.1
	Total	426	98.6
Missing	System	6	1.4
Total		432	100.0

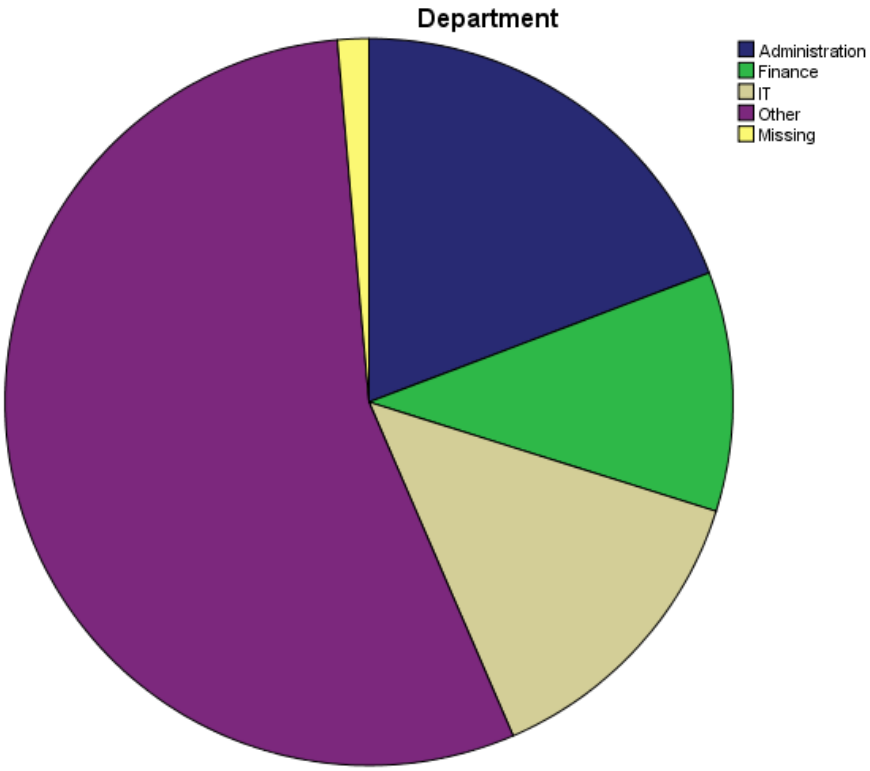

Figure 7: Department of Participants

As per the data given above, there were 432 participants in total in the survey. 19% of the participants were from Administration, 10% were in Finance, 13% were in IT, 1.4% were from other departments. As per the given data in both chart and table, it is demonstrated that the majority of participants were in Finance department.

Risk Management in Information Communication Technology Applications will bring about a lot of benefits to the Institution

Risk Management in Information Communication Technology Applications	

will bring about a lot of benefits to the Institution

		Frequency	Percent
Valid	Strongly Agree	129	29.9
	Agree	214	49.5
	Not Sure	68	15.7
	Disagree	6	1.4
	Strongly Disagree	12	2.8
	Total	429	99.3
Missing	System	3	.7
Total		432	100.0

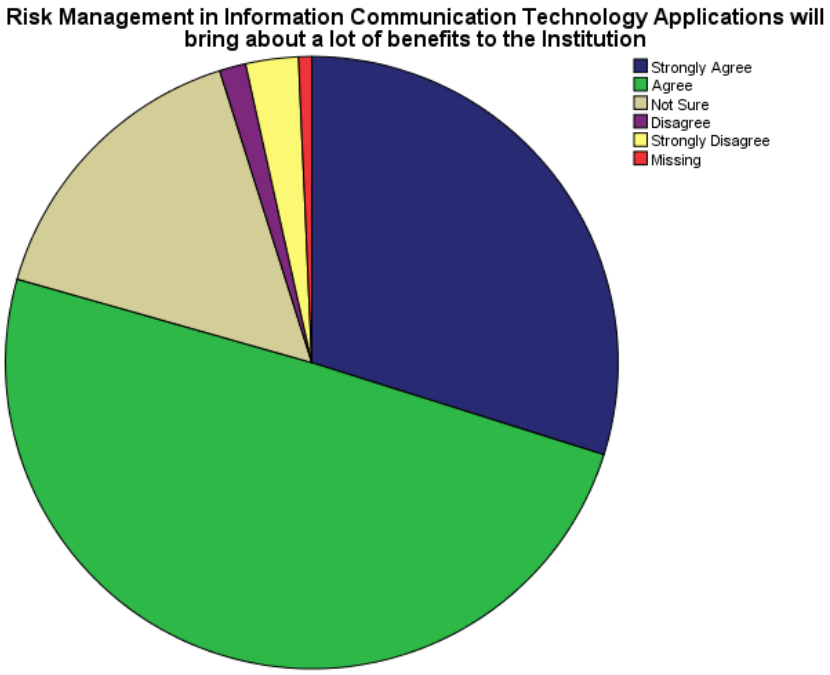

Figure 8: Risk Management in Information Communication Technology Applications will bring about a lot of benefits to the Institution

As per the data given above, there were 432 participants in total in the survey. 29% of them strongly agreed, 49% agreed, 15% were not sure, 1.4% disagreed, and the remaining 2.8% were disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Risk Management in Information Communication Technology Applications will bring about a lot of benefits to the Institution.

Smart governance organizations are need better resilience and risk management policies

Smart governance organizations are need better resilience and risk management policies

		Frequency	Percent
Valid	Strongly Agree	127	29.4
	Agree	220	50.9
	Not Sure	59	13.7
	Disagree	13	3.0
	Strongly Disagree	8	1.9
	Total	427	98.8
Missing	System	5	1.2
Total		432	100.0

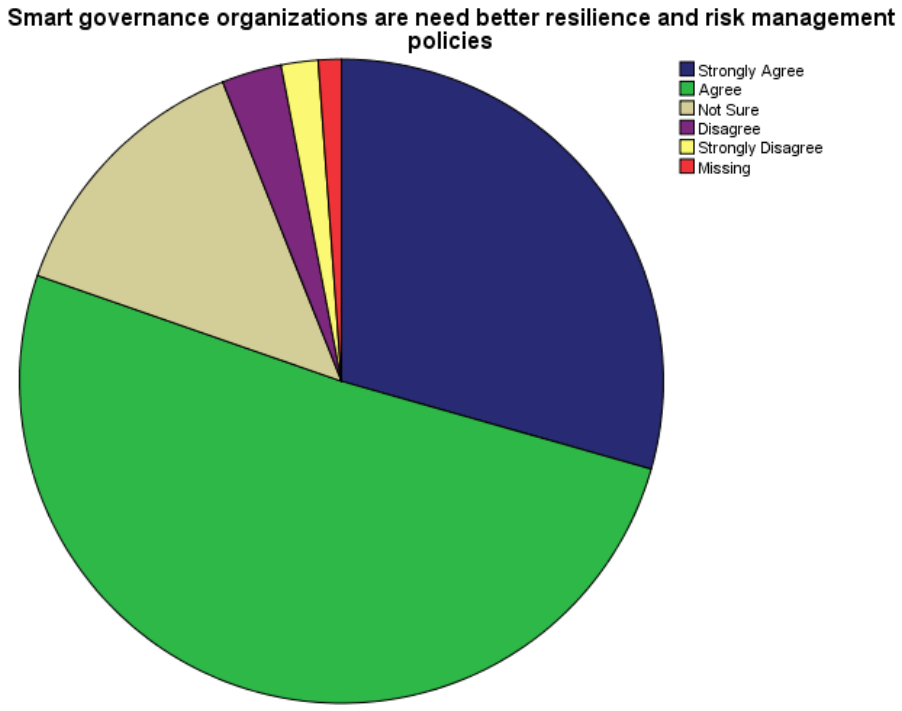

Figure 9: Smart governance organizations are need better resilience and risk management policies

As per the data given above, there were 432 participants in total in the survey. 29% of them strongly agreed, 50% agreed, 13% were not sure, 3% were disagreed, and the remaining 1.9% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that smart governance organizations are need better resilience and risk management policies.

The resilience management in smart government organizations will bring flexibility in cyberspace, and continuity of organizational functions despite the cyber

The resilience management in smart government organizations will bring

flexibility in cyberspace, and continuity of organizational functions despite the cyber attack

		Frequency	Percent
Valid	Strongly Agree	96	22.2
	Agree	204	47.2
	Not Sure	102	23.6
	Disagree	17	3.9
	Strongly Disagree	6	1.4
	Total	425	98.4
Missing	System	7	1.6
Total		432	100.0

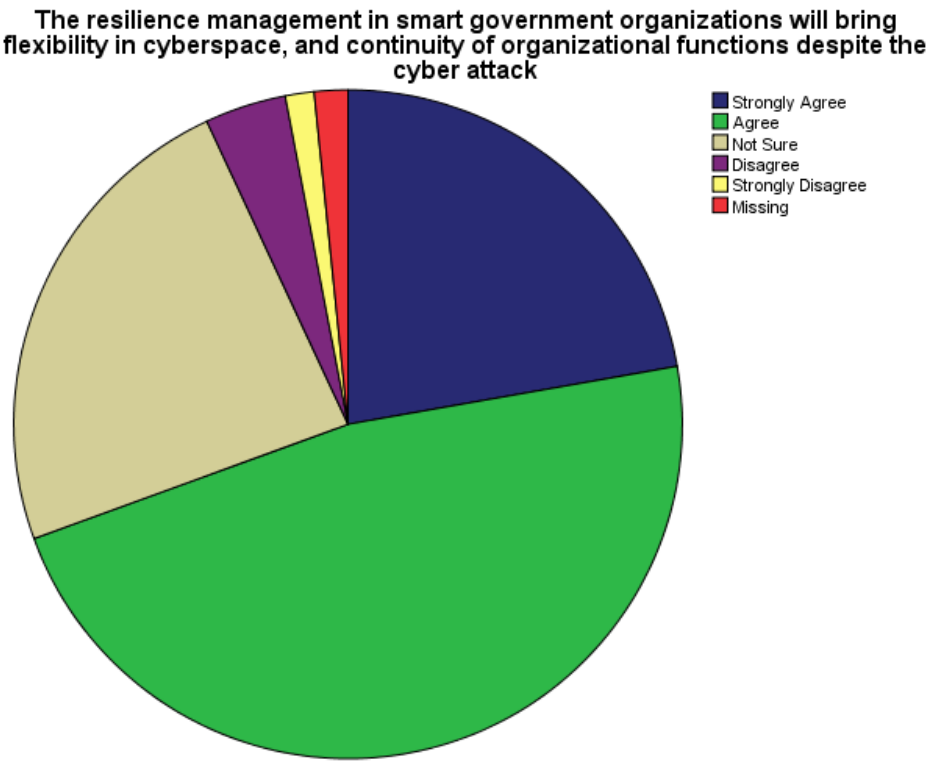

Figure 10: The resilience management in smart government organizations will bring flexibility in cyberspace, and continuity of organizational functions despite the cyber

As per the data given above, there were 432 participants in total in the survey. 22% of them strongly agreed, 47% agreed, 23.9% were not sure, 3.9% were disagreed, and the remaining 1.4% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the resilience management in smart government organizations will bring flexibility in cyberspace, and continuity of organizational functions despite the cyber attack.

There are more risks than benefits attributed to the whole process of Smart Governance

There are more risks than benefits attributed to the whole process of Smart Governance

		Frequency	Percent
Valid	Strongly Agree	60	13.9
	Agree	140	32.4
	Not Sure	125	28.9
	Disagree	83	19.2
	Strongly Disagree	18	4.2
	Total	426	98.6
Missing	System	6	1.4
Total		432	100.0

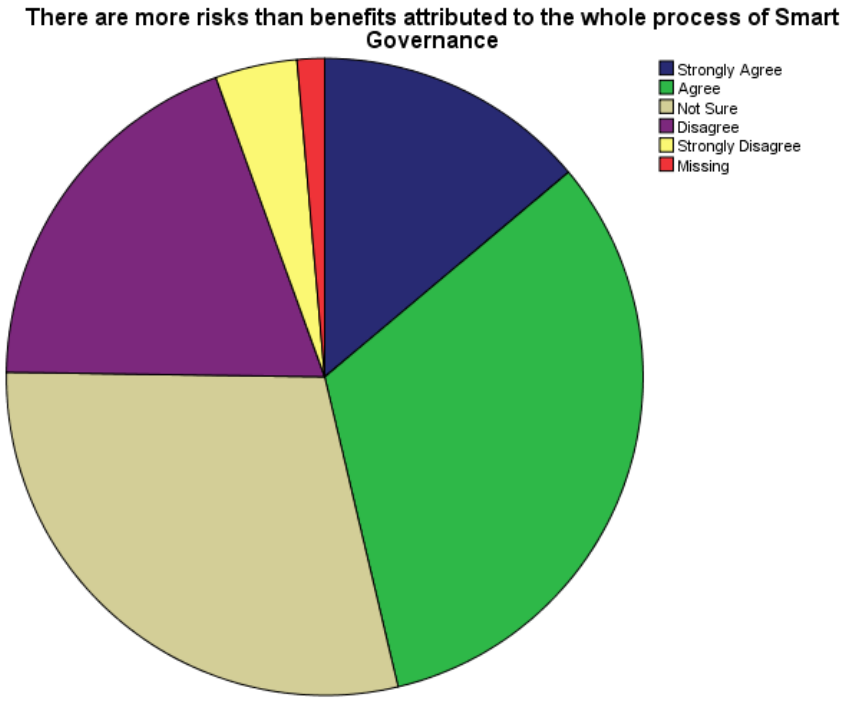

Figure 11: There are more risks than benefits attributed to the whole process of Smart Governance

As per the data given above, there were 432 participants in total in the survey. 13% of them strongly agreed, 32% agreed, 28% were not sure, 19% were disagreed, and the remaining 4.2% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that there are more risks than benefits attributed to the whole process of Smart Governance.

The changing environment and relations in society require smart government organizations in the UAE to focus on better resilience policies

The changing environment and relations in society require smart government organizations in the UAE to focus on better resilience policies

		Frequency	Percent
Valid	Strongly Agree	110	25.5
	Agree	198	45.8
	Not Sure	90	20.8
	Disagree	20	4.6
	Strongly Disagree	7	1.6
	Total	425	98.4
Missing	System	7	1.6
Total		432	100.0

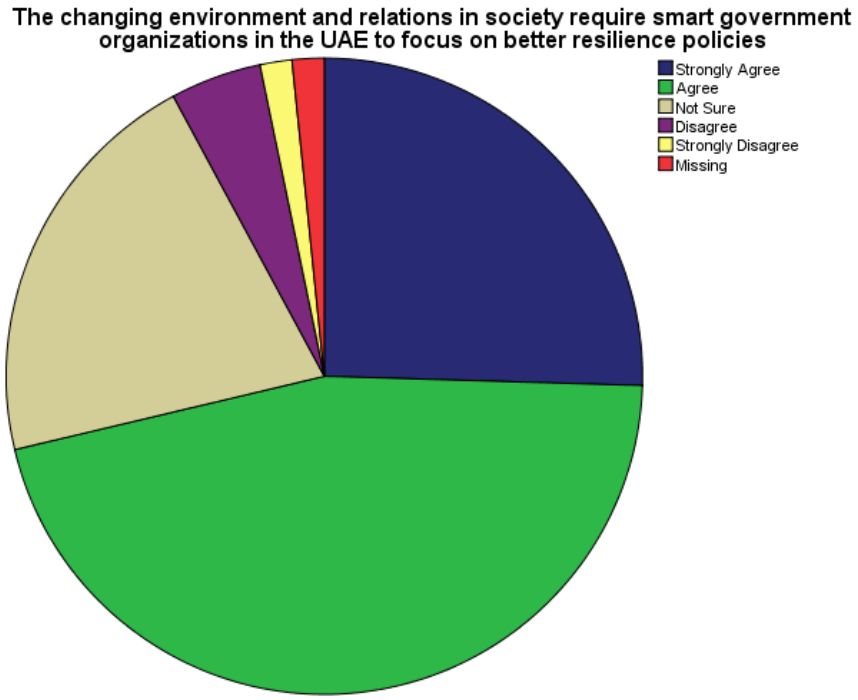

Figure 12: The changing environment and relations in society require smart government organizations in the UAE to focus on better resilience policies

As per the data given above, there were 432 participants in total in the survey. 22% of them strongly agreed, 25% agreed, 45.% were not sure, 20% were disagreed, and the remaining 4.6% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the changing environment and relations in society require smart government organizations in the UAE to focus on better resilience policies.

Smart Governance introduces improved techniques and processes to the organization

Smart Governance introduces improved techniques and processes to the organization

		Frequency	Percent
Valid	Strongly Agree	115	26.6
	Agree	217	50.2
	Not Sure	63	14.6
	Disagree	21	4.9
	Strongly Disagree	9	2.1
	Total	425	98.4
Missing	System	7	1.6
Total		432	100.0

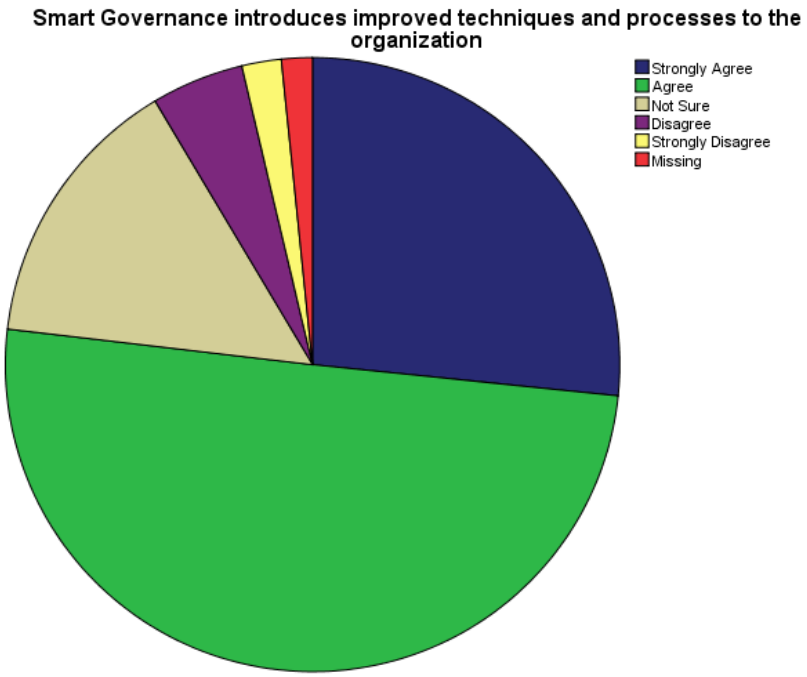

Figure 13: Smart Governance introduces improved techniques and processes to the organization

As per the data given above, there were 432 participants in total in the survey. 26% of them strongly agreed, 50% agreed, 14.6% were not sure, 4.9% were disagreed, and the remaining 2.1% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Smart Governance introduces improved techniques and processes to the organization.

Smart governance organizations should consider implementation of effective resilience

Smart governance organizations should consider implementation of effective resilience

		Frequency	Percent
Valid	Strongly Agree	96	22.2
	Agree	218	50.5
	Not Sure	80	18.5
	Disagree	18	4.2
	Strongly Disagree	12	2.8
	Total	424	98.1
Missing	System	8	1.9
Total		432	100.0

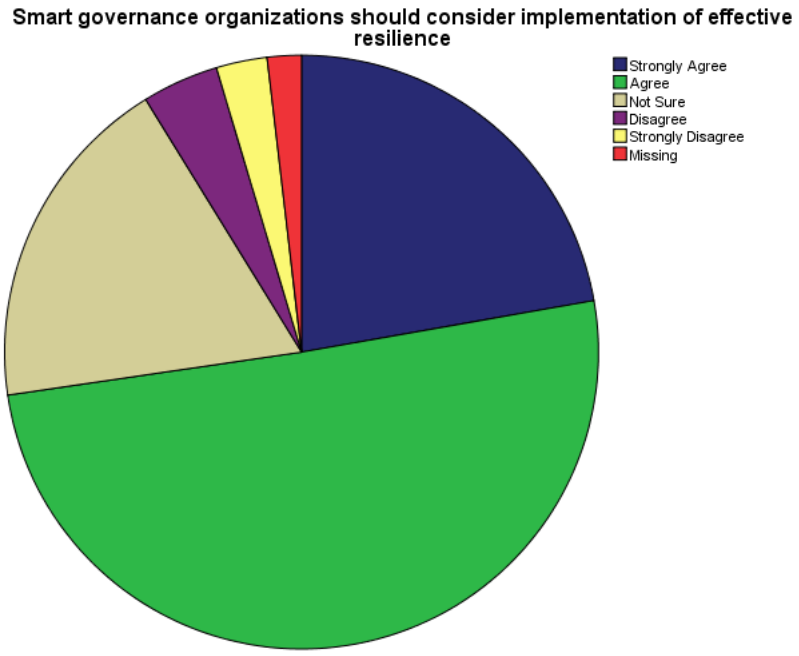

Figure 14: Smart governance organizations should consider implementation of effective resilience

As per the data given above, there were 432 participants in total in the survey. 22% of them strongly agreed, 50% agreed, 18% were not sure, 4% were disagreed, and the remaining 2.8% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Smart governance organizations should consider implementation of effective resilience.

Better management control in smart governance organizations can create capabilities and resilience against cyber attacks

Better management control in smart governance organizations can create

capabilities and resilience against cyber attacks

		Frequency	Percent
Valid	Strongly Agree	104	24.1
	Agree	211	48.8
	Not Sure	82	19.0
	Disagree	15	3.5
	Strongly Disagree	9	2.1
	Total	421	97.5
Missing	System	11	2.5
Total		432	100.0

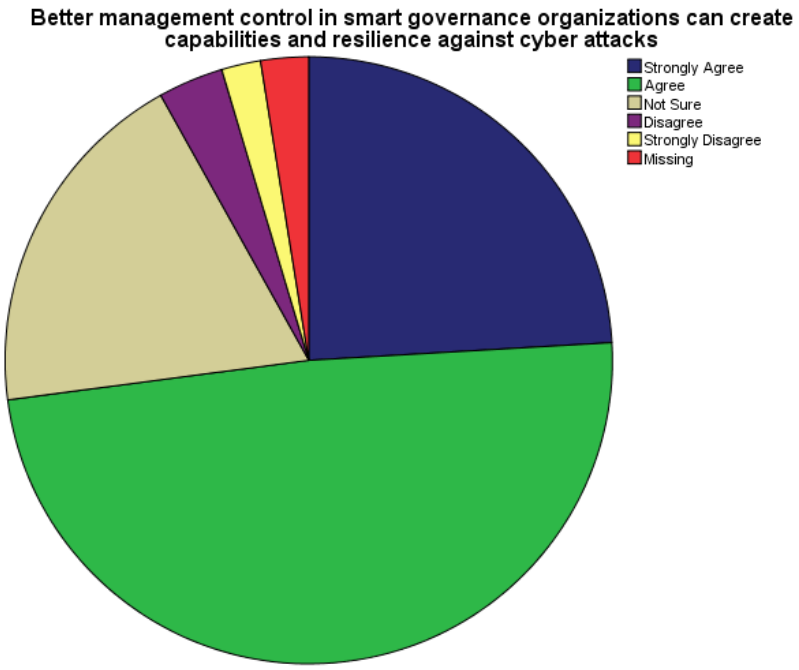

Figure 15: Better management control in smart governance organizations can create capabilities and resilience against cyber attacks

As per the data given above, there were 432 participants in total in the survey 19% of them strongly agreed, 39% agreed, 29.% were not sure, 3.5% were disagreed, and the remaining 4.% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that better management control in smart governance organizations can create capabilities and resilience against cyber attacks.

Multiple layers to foster resilience will result in shorter network and system downtimes

Multiple layers to foster resilience will result

in shorter network and system downtimes

		Frequency	Percent
Valid	Strongly Agree	84	19.4
	Agree	171	39.6
	Not Sure	129	29.9
	Disagree	25	5.8
	Strongly Disagree	15	3.5
	Total	424	98.1
Missing	System	8	1.9
Total		432	100.0

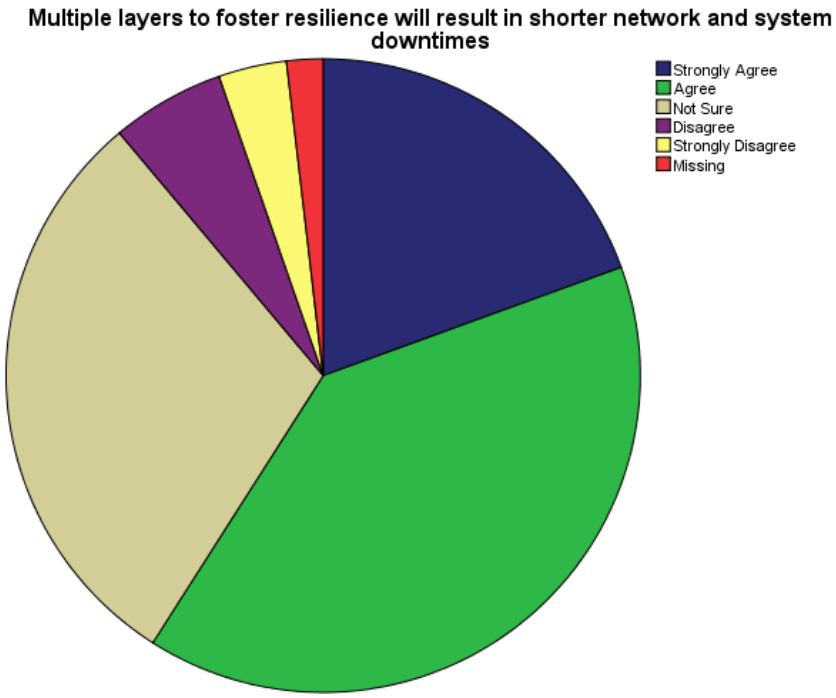

Figure 16: Multiple layers to foster resilience will result in shorter network and system downtimes

As per the data given above, there were 432 participants in total in the survey 19% of them strongly agreed, 39% agreed, 29% were not sure, 5.8% were disagreed, and the remaining 3.5% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that multiple layers to foster resilience will result in shorter network and system downtimes.

The government is focusing on cyber resilience to avoid threats in changing cyber environment

The government is focusing on cyber resilience to avoid threats in changing cyber environment

		Frequency	Percent
Valid	Strongly Agree	76	17.6
	Agree	195	45.1
	Not Sure	120	27.8
	Disagree	19	4.4
	Strongly Disagree	15	3.5
	Total	425	98.4
Missing	System	7	1.6
Total		432	100.0

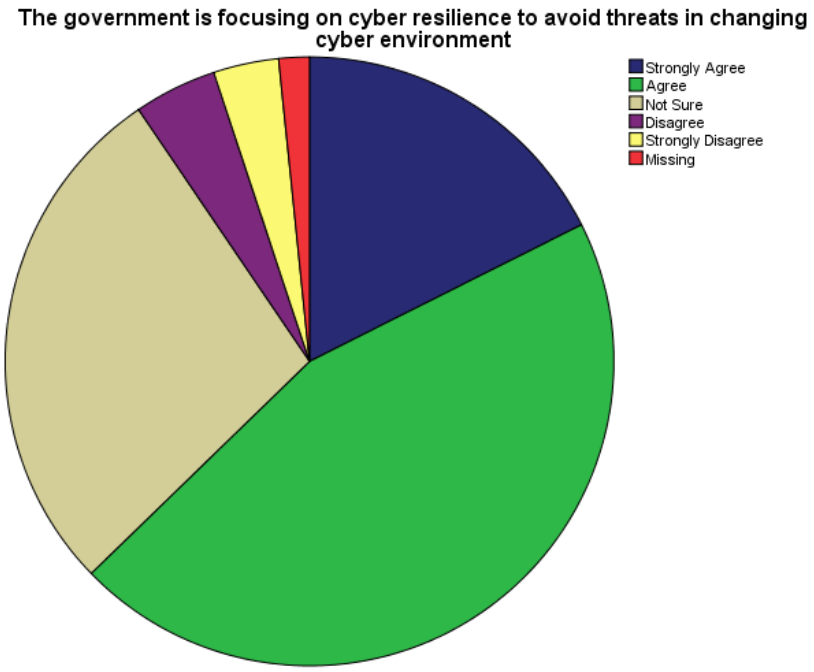

Figure 17: The government is focusing on cyber resilience to avoid threats in changing cyber environment

As per the data given above, there were 432 participants in total in the survey 17% of them strongly agreed, 45% agreed, 27% were not sure, 4.4% were disagreed, and the remaining 3.5% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the government is focusing on cyber resilience to avoid threats in changing cyber environment.

Smart Governance Platforms is generally vulnerable to common attacks such as Denial of Service Attacks.

Smart Governance Platforms is generally vulnerable to common attacks such as Denial of Service Attacks.

		Frequency	Percent
Valid	Strongly Agree	68	15.7
	Agree	153	35.4
	Not Sure	153	35.4
	Disagree	43	10.0
	Strongly Disagree	5	1.2
	Total	422	97.7
Missing	System	10	2.3
Total		432	100.0

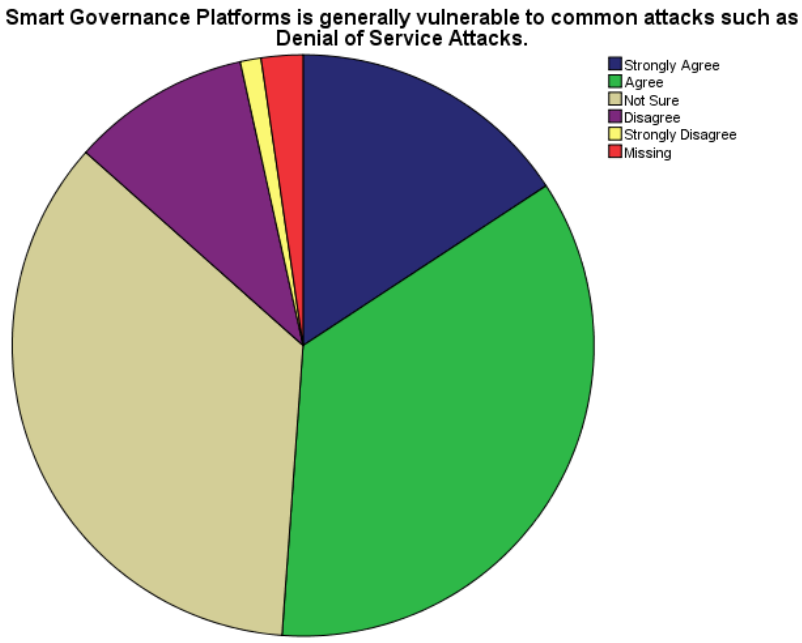

Figure 18: Smart Governance Platforms is generally vulnerable to common attacks such as Denial of Service Attacks.

As per the data given above, there were 432 participants in total in the survey 15.7% of them strongly agreed, 35% agreed, 35% were not sure, 10% were disagreed, and the remaining 1.2% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Smart Governance Platforms is generally vulnerable to common attacks such as Denial of Service Attacks.

Smart Governance Platforms will result in a greater uptake of cloud based resources by the average person

Smart Governance Platforms will result in a greater uptake of cloud based resources by the average person

		Frequency	Percent
Valid	Strongly Agree	81	18.8
	Agree	189	43.8
	Not Sure	121	28.0
	Disagree	17	3.9
	Strongly Disagree	17	3.9
	Total	425	98.4
Missing	System	7	1.6
Total		432	100.0

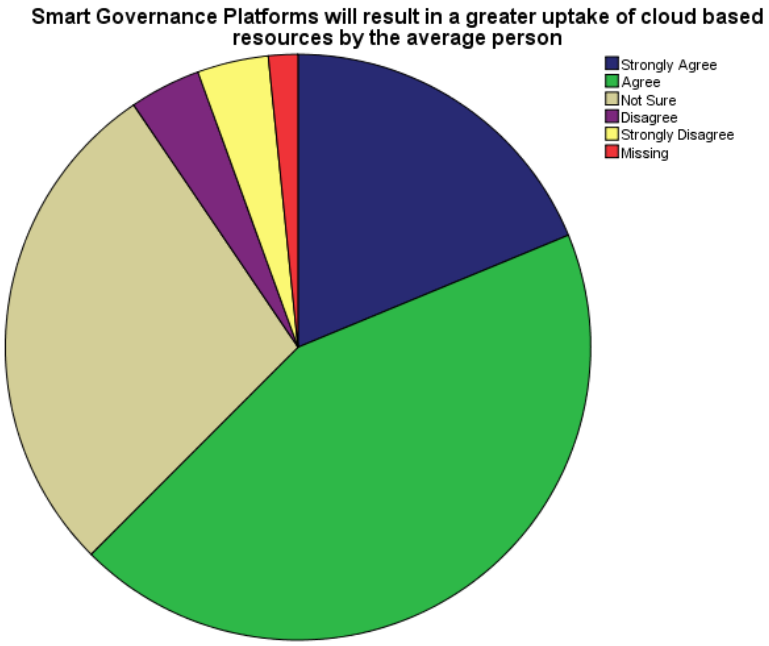

Figure 19: Smart Governance Platforms will result in a greater uptake of cloud based resources by the average person

As per the data given above, there were 432 participants in total in the survey. 18.7% of them strongly agreed, 43% agreed, 28% were not sure, 3.9% were disagreed, and the remaining 3.9% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Smart Governance Platforms will result in a greater uptake of cloud based resources by the average person.

Smart Governance Platforms will be able to accurately predict the unique needs of individual students, instead of providing generic answers.

Smart Governance Platforms will be able to accurately predict the unique needs of

individual students, instead of providing generic answers.

		Frequency	Percent
Valid	Strongly Agree	83	19.2
	Agree	191	44.2
	Not Sure	108	25.0
	Disagree	30	6.9
	Strongly Disagree	12	2.8
	Total	424	98.1
Missing	System	8	1.9
Total		432	100.0

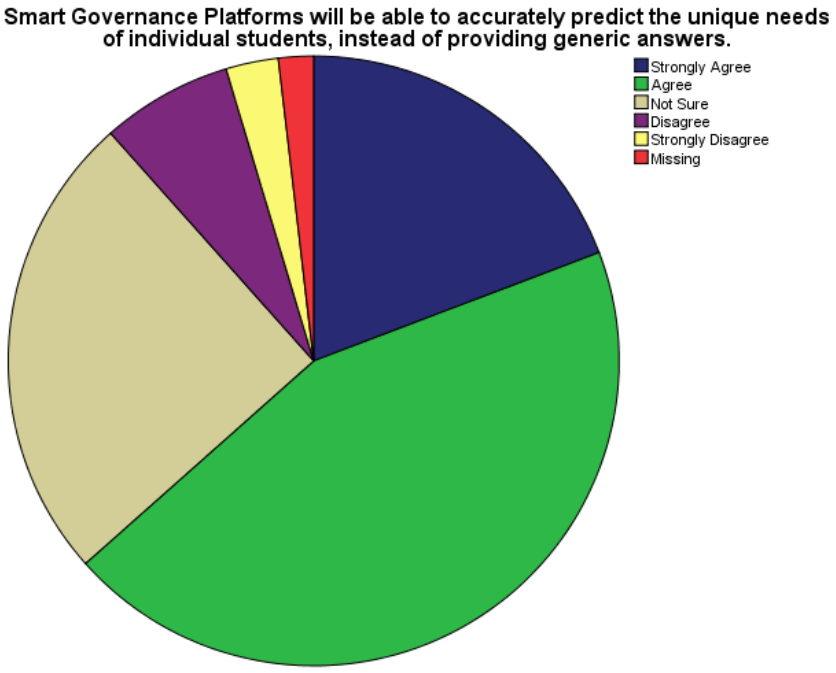

Figure 20: Smart Governance Platforms will be able to accurately predict the unique needs of individual students, instead of providing generic answers.

As per the data given above, there were 432 participants in total in the survey 19% of them strongly agreed, 44% agreed, 25% were not sure, 2.8% were disagreed, and the remaining 2.1% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Smart Governance Platforms will be able to accurately predict the unique needs of individual students, instead of providing generic answers.

The current ICT policies and frameworks that guide the system are inadequate due to lack of resilience polices and risk management strategy

The current ICT policies and frameworks
that guide the system are inadequate due to

lack of resilience polices and risk management strategy

		Frequency	Percent
Valid	Strongly Agree	61	14.1
	Agree	180	41.7
	Not Sure	138	31.9
	Disagree	31	7.2
	Strongly Disagree	13	3.0
	Total	423	97.9
Missing	System	9	2.1
Total		432	100.0

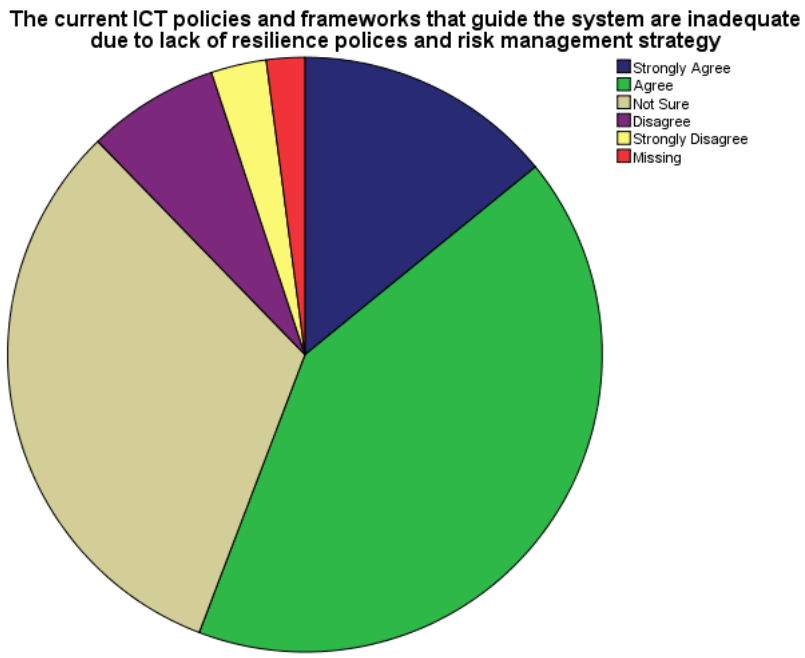

Figure 21: The current ICT policies and frameworks that guide the system are inadequate due to lack of resilience polices and risk management strategy

As per the data given above, there were 432 participants in total in the survey 14.1% of them strongly agreed, 41% agreed, 31% were not sure, 7% were disagreed, and the remaining 3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the current ICT policies and frameworks that guide the system are inadequate due to lack of resilience polices and risk management strategy.

Smart governance organizations of the UAE need effective policies and frameworks for the system

Smart governance organizations of the UAE need effective policies and frameworks for the system

		Frequency	Percent
Valid	Strongly Agree	83	19.2
	Agree	207	47.9
	Not Sure	96	22.2
	Disagree	24	5.6
	Strongly Disagree	13	3.0
	Total	423	97.9
Missing	System	9	2.1
Total		432	100.0

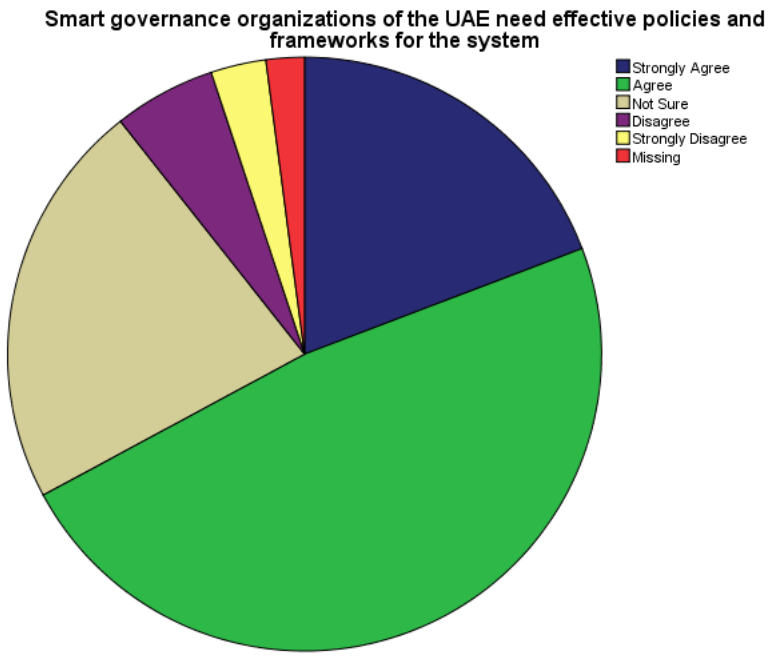

Figure 22: Smart governance organizations of the UAE need effective policies and frameworks for the system

As per the data given above, there were 432 participants in total in the survey 19% of them strongly agreed, 47% agreed, 22% were not sure, 5% were disagreed, and the remaining 3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Smart governance organizations of the UAE need effective policies and frameworks for the system.

The smart Governance Platform will enable the institution to maintain its competitive advantage across all spheres of service provision.

The smart Governance Platform will enable the institution to maintain its

competitive advantage across all spheres of service provision.

		Frequency	Percent
Valid	Strongly Agree	78	18.1
	Agree	203	47.0
	Not Sure	110	25.5
	Disagree	21	4.9
	Strongly Disagree	10	2.3
	Total	422	97.7
Missing	System	10	2.3
Total		432	100.0

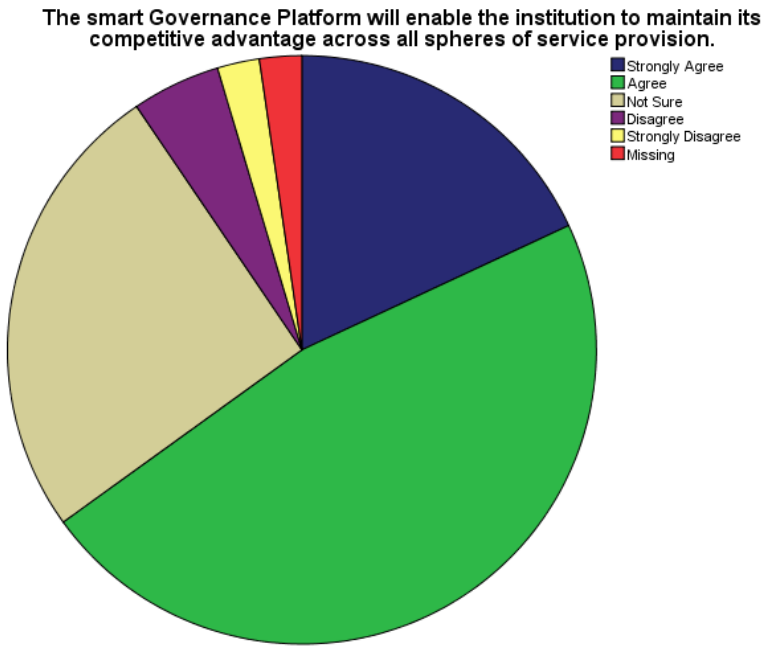

Figure 23: The smart Governance Platform will enable the institution to maintain its competitive advantage across all spheres of service provision.

As per the data given above, there were 432 participants in total in the survey 18.1% of them strongly agreed, 47% agreed, 25% were not sure, 4.9% were disagreed, and the remaining 2.3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the smart Governance Platform will enable the institution to maintain its competitive advantage across all spheres of service provision.

The smart Governance Platform will improve service consistency, continuity and overall quality at a minimal cost.

The smart Governance Platform will improve service consistency, continuity and overall quality at a minimal cost.

		Frequency	Percent
Valid	Strongly Agree	88	20.4
	Agree	189	43.8
	Not Sure	105	24.3
	Disagree	30	6.9
	Strongly Disagree	10	2.3
	Total	422	97.7
Missing	System	10	2.3
Total		432	100.0

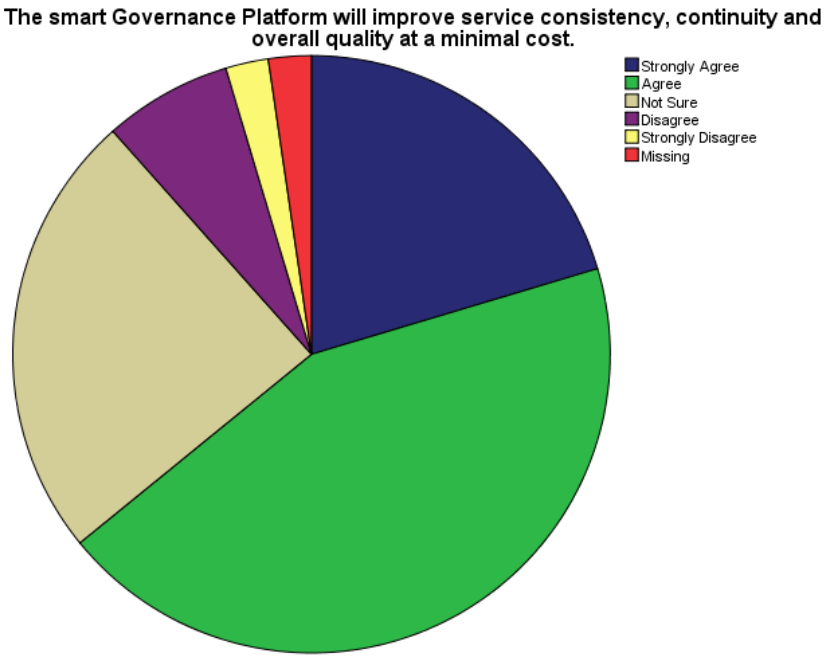

Figure 24: The smart Governance Platform will improve service consistency, continuity and overall quality at a minimal cost.

As per the data given above, there were 432 participants in total in the survey 20% of them strongly agreed, 43% agreed, 24% were not sure, 6.9% were disagreed, and the remaining 2.3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the smart Governance Platform will improve service consistency, continuity and overall quality at a minimal cost.

Risk Management interventions will prevent the institution from being exposed to costly legal proceedings in case of data breaches

Risk Management interventions will prevent the institution from being exposed	

to costly legal proceedings in case of data breaches

		Frequency	Percent
Valid	Strongly Agree	79	18.3
	Agree	201	46.5
	Not Sure	97	22.5
	Disagree	31	7.2
	Strongly Disagree	17	3.9
	Total	425	98.4
Missing	System	7	1.6
Total		432	100.0

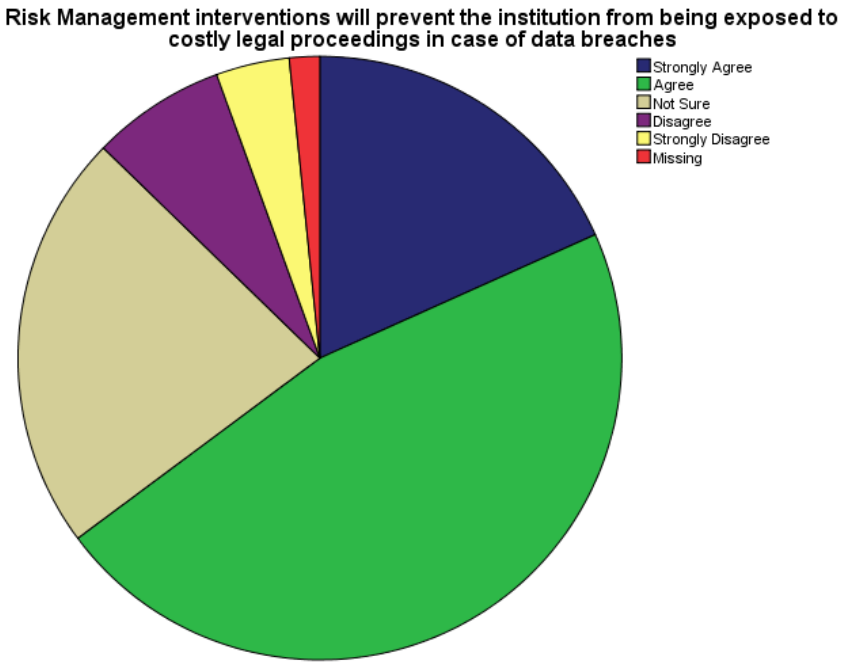

Figure 25: Risk Management interventions will prevent the institution from being exposed to costly legal proceedings in case of data breaches

As per the data given above, there were 432 participants in total in the survey 18.1% of them strongly agreed, 46.5% agreed, 22.6% were not sure, 7% were disagreed, and the remaining 4% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Risk Management interventions will prevent the institution from being exposed to costly legal proceedings in case of data breaches.

The smart Governance Platform will offer real time feedback and 24/7 access and resource provision.

The smart Governance Platform will offer real time feedback and 24/7 access and resource provision.

		Frequency	Percent
Valid	Strongly Agree	88	20.4
	Agree	182	42.1
	Not Sure	103	23.8
	Disagree	24	5.6
	Strongly Disagree	17	3.9
	Total	414	95.8
Missing	System	18	4.2
Total		432	100.0

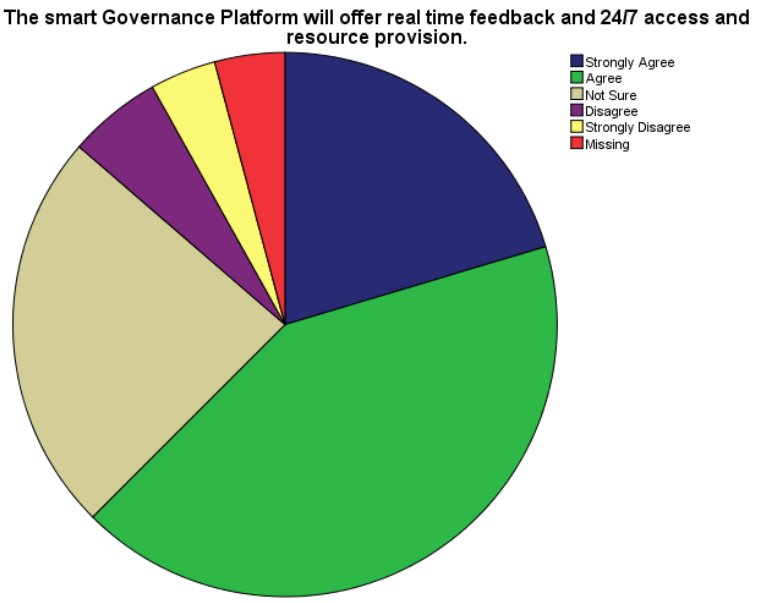

Figure 26: The smart Governance Platform will offer real time feedback and 24/7 access and resource provision.

As per the data given above, there were 432 participants in total in the survey 20% of them strongly agreed, 42% agreed, 23% were not sure, 5% were disagreed, and the remaining 3.9% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the smart Governance Platform will offer real time feedback and 24/7 access and resource provision.

Improved risk management and resilience will enhance performance of employees

Improved risk management and resilience will enhance performance of employees

		Frequency	Percent
Valid	Strongly Agree	87	20.1
	Agree	201	46.5
	Not Sure	98	22.7
	Disagree	24	5.6
	Strongly Disagree	11	2.5
	Total	421	97.5
Missing	System	11	2.5
Total		432	100.0

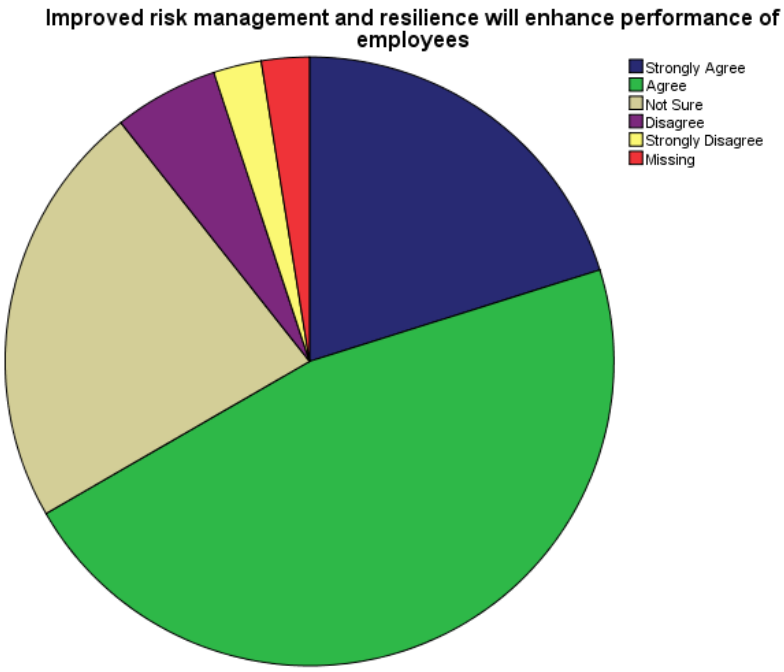

Figure 27: Improved risk management and resilience will enhance performance of employees

As per the data given above, there were 432 participants in total in the survey 20% of them strongly agreed, 46% agreed, 22% were not sure, 5.6% were disagreed, and the remaining 2.5% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that improved risk management and resilience will enhance performance of employees.

Risk management will be beneficial for all stakeholders

Risk management will be beneficial for all stakeholders

		Frequency	Percent
Valid	Strongly Agree	93	21.5
	Agree	184	42.6
	Not Sure	104	24.1
	Disagree	33	7.6
	Strongly Disagree	8	1.9
	Total	422	97.7
Missing	System	10	2.3
Total		432	100.0

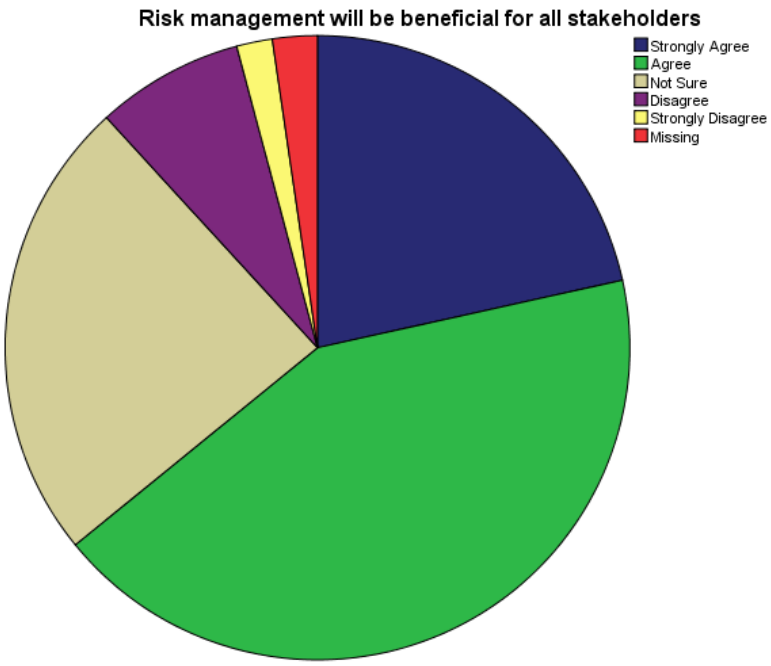

Figure 28: Risk management will be beneficial for all stakeholders

As per the data given above, there were 432 participants in total in the survey 21% of them strongly agreed, 42% agreed, 24% were not sure, 7.6% were disagreed, and the remaining 1.9% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that risk management will be beneficial for all stakeholders.

Resilience and Risk Management will result in better mitigation, reduction or elimination of cyber related attacks

Resilience and Risk Management will result in better mitigation, reduction or elimination of cyber related attacks

		Frequency	Percent
Valid	Strongly Agree	86	19.9
	Agree	202	46.8
	Not Sure	107	24.8
	Disagree	19	4.4
	Strongly Disagree	9	2.1
	Total	423	97.9
Missing	System	9	2.1
Total		432	100.0

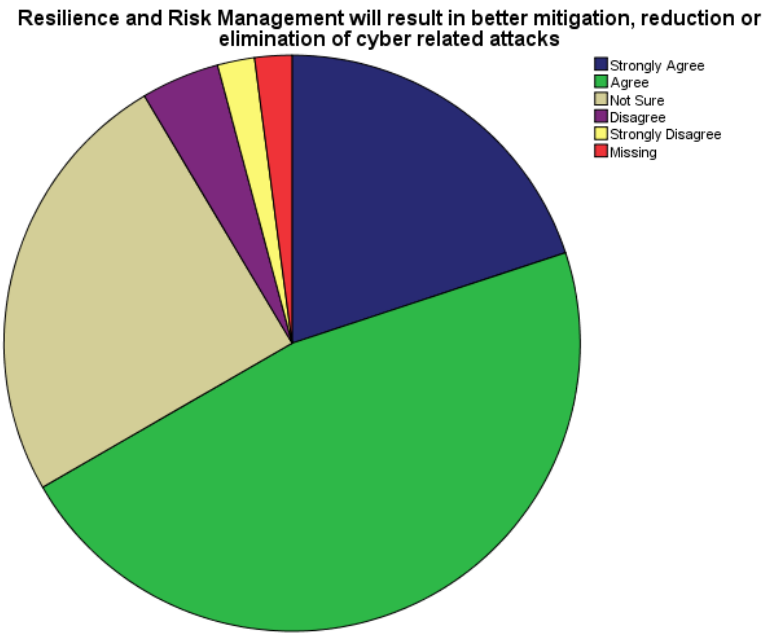

Figure 29: Resilience and Risk Management will result in better mitigation, reduction or elimination of cyber related attacks

As per the data given above, there were 432 participants in total in the survey 19.9% of them strongly agreed, 46% agreed, 24% were not sure, 4.4% were disagreed, and the remaining 2.1% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Resilience and Risk Management will result in better mitigation, reduction or elimination of cyber related attacks.

Better policies for Cyber resilience will help smart government organizations to recover quickly from any cyber attack

Better policies for Cyber resilience will help smart government organizations to recover quickly from any cyber attack

		Frequency	Percent
Valid	Strongly Agree	99	22.9
	Agree	199	46.1
	Not Sure	94	21.8
	Disagree	21	4.9
	Strongly Disagree	10	2.3
	Total	423	97.9
Missing	System	9	2.1
Total		432	100.0

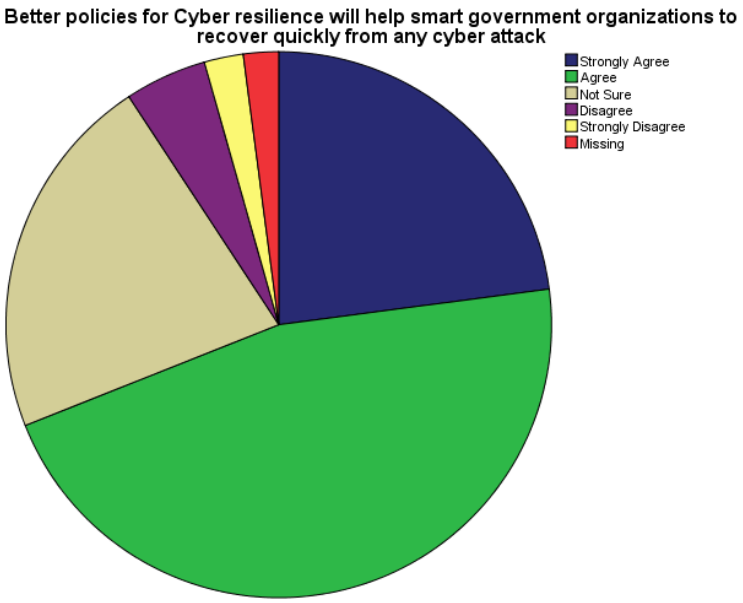

Figure 30: Better policies for Cyber resilience will help smart government organizations to recover quickly from any cyber attack

As per the data given above, there were 432 participants in total in the survey 22% of them strongly agreed, 46% agreed, 21% were not sure, 4.9% were disagreed, and the remaining 2.3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that better policies for Cyber resilience will help smart government organizations to recover quickly from any cyber attack.

The regularity authorities of the country should pay attention enhance infrastructure resilience in smart government organizations

The regularity authorities of the country should pay attention enhance	

infrastructure resilience in smart government organizations

		Frequency	Percent
Valid	Strongly Agree	93	21.5
	Agree	204	47.2
	Not Sure	98	22.7
	Disagree	23	5.3
	Strongly Disagree	4	.9
	Total	422	97.7
Missing	System	10	2.3
Total		432	100.0

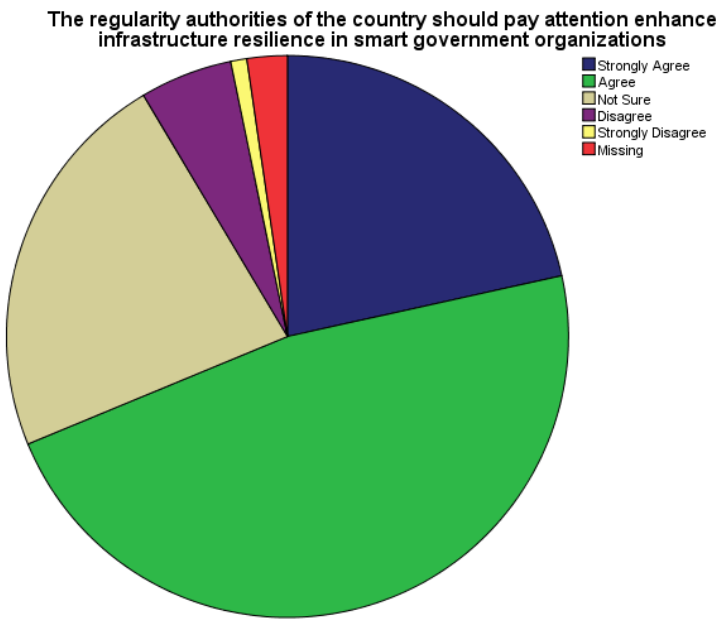

Figure 31: The regularity authorities of the country should pay attention enhance infrastructure resilience in smart government organizations

As per the data given above, there were 432 participants in total in the survey 21% of them strongly agreed, 47% agreed, 22% were not sure, 5.3% were disagreed, and the remaining .9% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the regularity authorities of the country should pay attention enhance infrastructure resilience in smart government organizations.

The federal government of the UAE is aware of the importance of resilience and cyber security management in smart government organizations

The federal government of the UAE is aware of the importance of resilience and

cyber security management in smart government organizations

		Frequency	Percent
Valid	Strongly Agree	98	22.7
	Agree	175	40.5
	Not Sure	119	27.5
	Disagree	24	5.6
	Strongly Disagree	6	1.4
	Total	422	97.7
Missing	System	10	2.3
Total		432	100.0

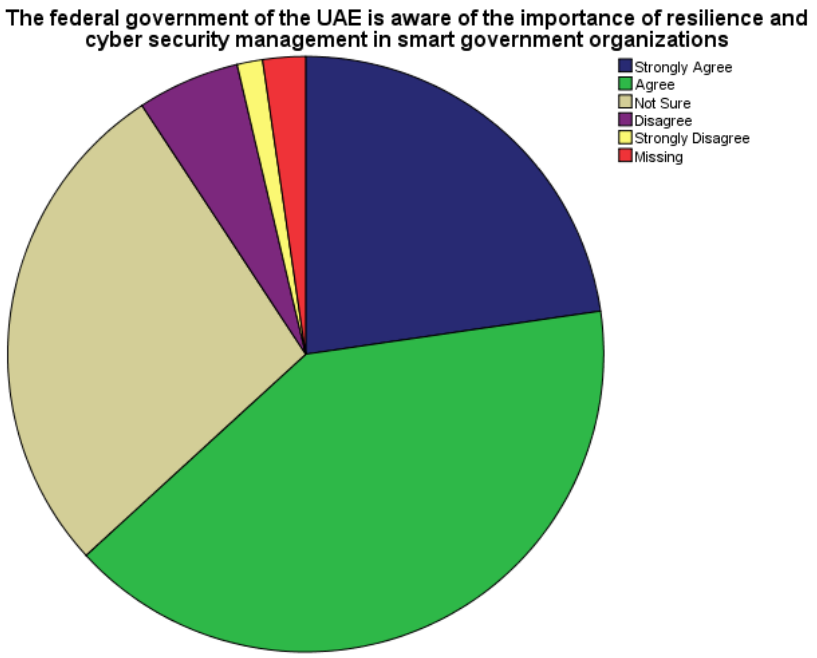

Figure 32 :The federal government of the UAE is aware of the importance of resilience and cyber security management in smart government organizations

As per the data given above, there were 432 participants in total in the survey 22% of them strongly agreed, 40.5% agreed, 27.5% were not sure, 5.6% were disagreed, and the remaining 1.4% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the federal government of the UAE is aware of the importance of resilience and cyber security management in smart government organizations.

The purpose of cyber security domain in smart government organizations is to build control for making cyberspace secure

The purpose of cyber security domain in smart government organizations is to build control for making cyberspace secure

		Frequency	Percent
Valid	Strongly Agree	90	20.8
	Agree	203	47.0
	Not Sure	86	19.9
	Disagree	27	6.3
	Strongly Disagree	17	3.9
	Total	423	97.9
Missing	System	9	2.1
Total		432	100.0

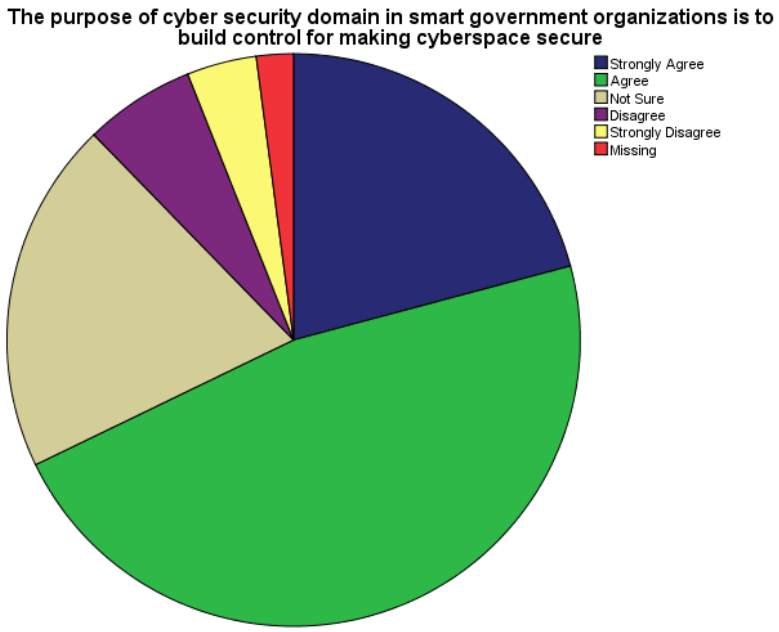

Figure 33: The purpose of cyber security domain in smart government organizations is to build control for making cyberspace secure

As per the data given above, there were 432 participants in total in the survey 20% of them strongly agreed, 47% agreed, 19% were not sure, 6.3% were disagreed, and the remaining 3.9% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the purpose of cyber security domain in smart government organizations is to build control for making cyberspace secure.

Smart Governance will introduce a high rate of resilience in institutional platforms and virtual services provided.

Smart Governance will introduce a high rate of resilience in institutional platforms and virtual services provided.

		Frequency	Percent
Valid	Strongly Agree	86	19.9
	Agree	194	44.9
	Not Sure	110	25.5
	Disagree	17	3.9
	Strongly Disagree	13	3.0
	Total	420	97.2
Missing	System	12	2.8
Total		432	100.0

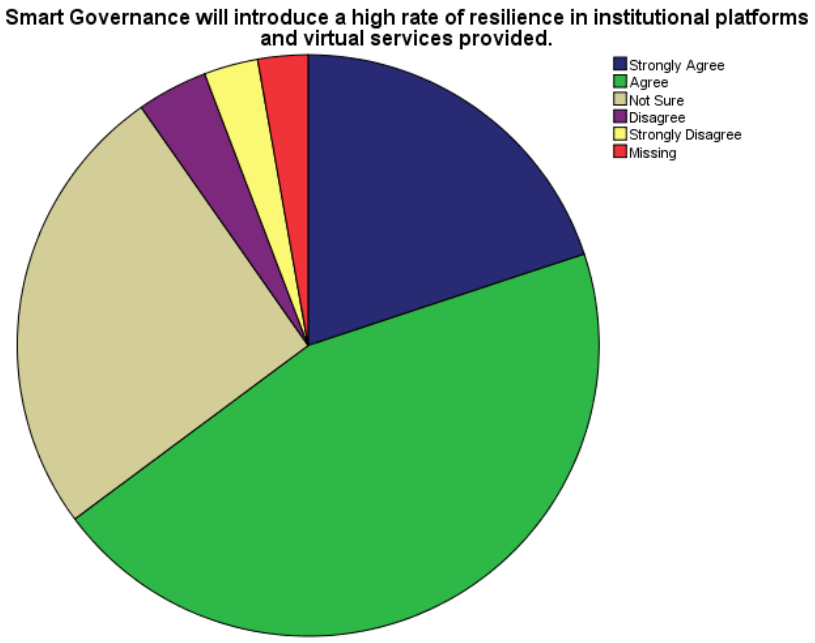

Figure 34: Smart Governance will introduce a high rate of resilience in institutional platforms and virtual services provided.

As per the data given above, there were 432 participants in total in the survey 19% of them strongly agreed, 44% agreed, 25.% were not sure, 3.9% were disagreed, and the remaining 3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Smart Governance will introduce a high rate of resilience in institutional platforms and virtual services provided.

The smart Platform will result in faster and more specific responses to stakeholders

The smart Platform will result in faster and more specific responses to stakeholders

	Frequency	Percent

Valid	Strongly Agree	101	23.4
	Agree	173	40.0
	Not Sure	110	25.5
	Disagree	26	6.0
	Strongly Disagree	9	2.1
	Total	419	97.0
Missing	System	13	3.0
Total		432	100.0

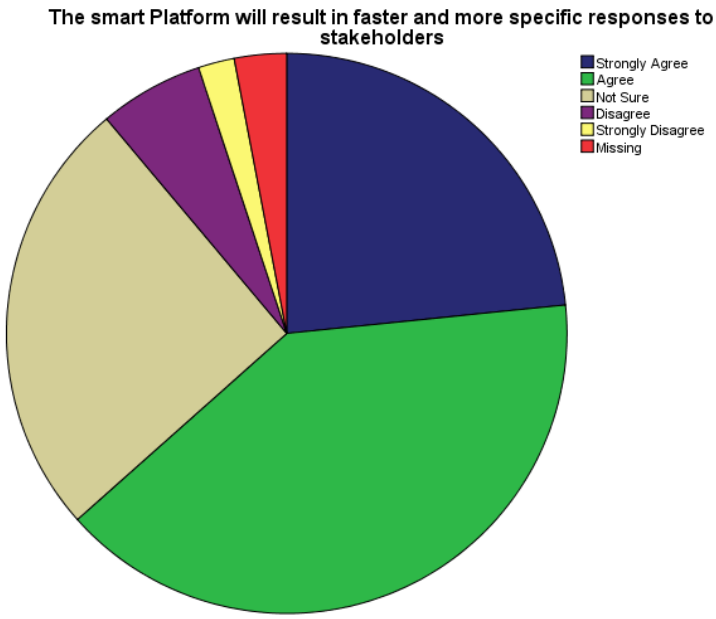

Figure 35: The smart Platform will result in faster and more specific responses to stakeholders

As per the data given above, there were 432 participants in total in the survey 24% of them strongly agreed, 40% agreed, 25 % were not sure, 6% were disagreed, and the remaining 2.1% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the smart Platform will result in faster and more specific responses to stakeholders.

Smart Governance Platforms will introduce more secure data storage and data management to this facility

Smart Governance Platforms will introduce more secure data storage and data management to this facility

		Frequency	Percent
Valid	Strongly Agree	96	22.2
	Agree	190	44.0
	Not Sure	96	22.2
	Disagree	21	4.9
	Strongly Disagree	15	3.5
	Total	418	96.8
Missing	System	14	3.2
Total		432	100.0

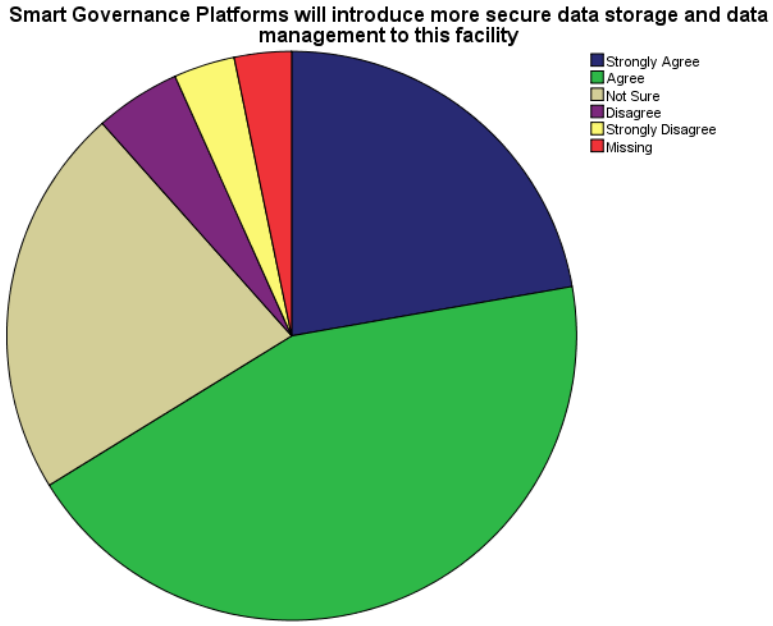

Figure 36: Smart Governance Platforms will introduce more secure data storage and data management to this facility

As per the data given above, there were 432 participants in total in the survey 22% of them strongly agreed, 44% agreed, 22% were not sure, 4.9% were disagreed, and the remaining 3.5% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Smart Governance Platforms will introduce more secure data storage and data management to this facility.

The smart Governance Platform will enable the institution to focus its resources and energy on core activities rather than peripheral ones.

The smart Governance Platform will enable the institution to focus its resources	

and energy on core activities rather than peripheral ones.

		Frequency	Percent
Valid	Strongly Agree	94	21.8
	Agree	172	39.8
	Not Sure	124	28.7
	Disagree	25	5.8
	Strongly Disagree	7	1.6
	Total	422	97.7
Missing	System	10	2.3
Total		432	100.0

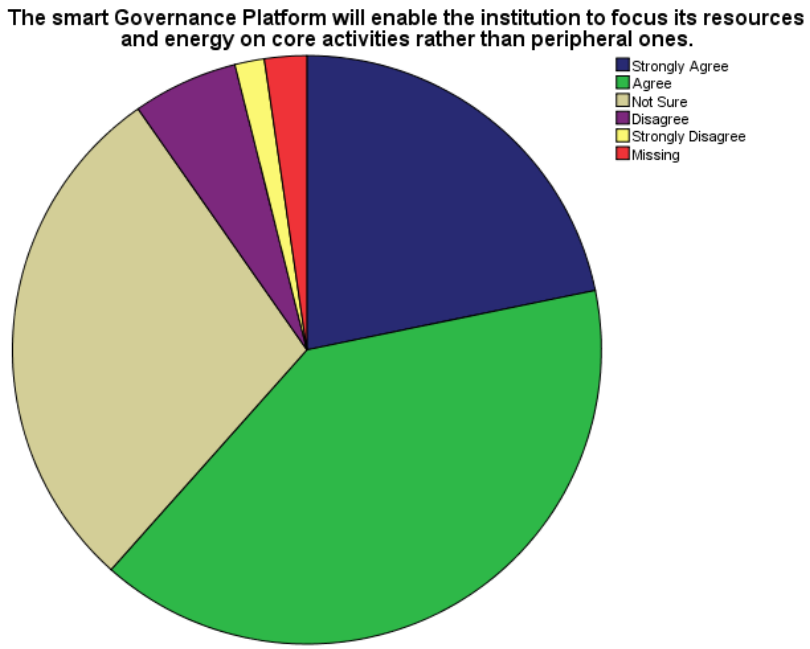

Figure 37: The smart Governance Platform will enable the institution to focus its resources and energy on core activities rather than peripheral ones.

As per the data given above, there were 432 participants in total in the survey 21% of them strongly agreed, 39% agreed, 28% were not sure, 5.8% were disagreed, and the remaining 1.6% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the smart Governance Platform will enable the institution to focus its resources and energy on core activities rather than peripheral ones.

The smart Governance Platform will result in capacity building, better knowlege transfer and the creation of new skill sets for the stakeholders.

	Frequency	Percent

Valid	Strongly Agree	99	22.9
	Agree	184	42.6
	Not Sure	100	23.1
	Disagree	26	6.0
	Strongly Disagree	12	2.8
	Total	421	97.5
Missing	System	11	2.5
Total		432	100.0

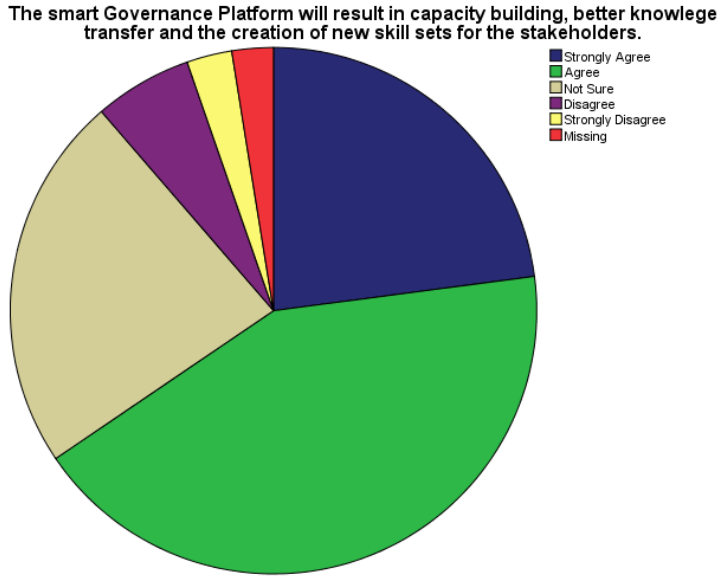

Figure 38: The smart Governance Platform will result in capacity building, better knowlege transfer and the creation of new skill sets for the stakeholders.

As per the data given above, there were 432 participants in total in the survey 23% of them strongly agreed, 42% agreed, 23% were not sure, 6% were disagreed, and the remaining 2.8% were

strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the smart Governance Platform will result in capacity building, better knowledge transfer and the creation of new skill sets for the stakeholders.

Existing and evolving Cyber Security Threats will make the smart government organizations vulnerable

Existing and evolving Cyber Security Threats will make the smart government organizations vulnerable

		Frequency	Percent
Valid	Strongly Agree	79	18.3
	Agree	158	36.6
	Not Sure	121	28.0
	Disagree	44	10.2
	Strongly Disagree	17	3.9
	Total	419	97.0
Missing	System	13	3.0
Total		432	100.0

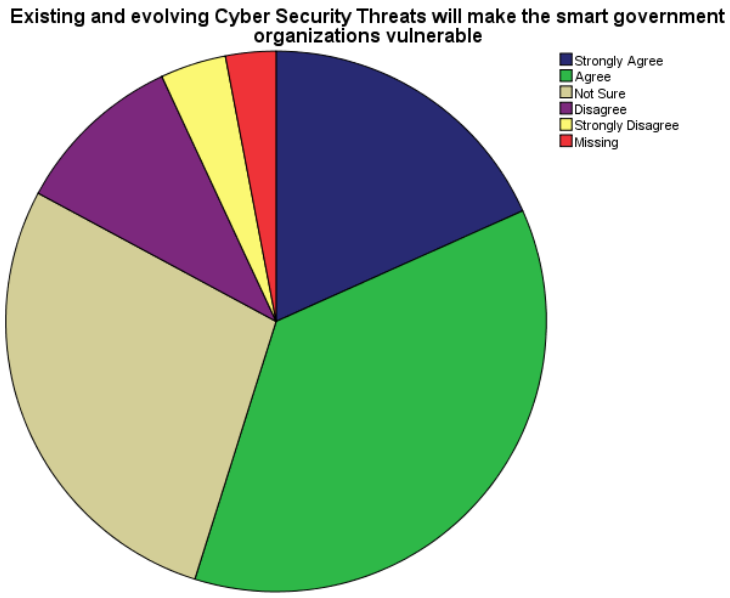

Figure 39: Existing and evolving Cyber Security Threats will make the smart government organizations vulnerable

As per the data given above, there were 432 participants in total in the survey 18% of them strongly agreed, 36% agreed, 28% were not sure, 10% were disagreed, and the remaining 3.9% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Existing and evolving Cyber Security Threats will make the smart government organizations vulnerable.

The smart Platform may cause the institution will to lose reliable and more talented staff who may not be that tech savvy, and introduce untrusted third parties.

The smart Platform may cause the institution will to lose reliable and more talented staff who may not be that tech

savvy, and introduce untrusted third parties.

		Frequency	Percent
Valid	Strongly Agree	88	20.4
	Agree	168	38.9
	Not Sure	113	26.2
	Disagree	38	8.8
	Strongly Disagree	13	3.0
	Total	420	97.2
Missing	System	12	2.8
Total		432	100.0

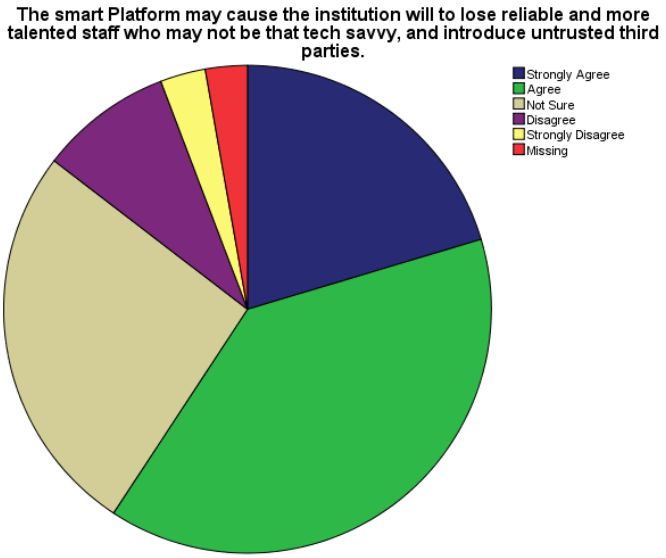

Figure 40: The smart Platform may cause the institution will to lose reliable and more talented staff who may not be that tech savvy, and introduce untrusted third parties.

As per the data given above, there were 432 participants in total in the survey 20% of them strongly agreed, 38.9% agreed, 26% were not sure, 8.8% were disagreed, and the remaining 3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the smart Platform may cause the institution will to lose reliable and more talented staff who may not be that tech savvy, and introduce untrusted third parties.

External Service Providers for the smart Governance Platform cannot always reliable and consistent services

External Service Providers for the smart Governance Platform cannot always reliable and consistent services

		Frequency	Percent
Valid	Strongly Agree	76	17.6
	Agree	172	39.8
	Not Sure	129	29.9
	Disagree	32	7.4
	Strongly Disagree	8	1.9
	Total	417	96.5
Missing	System	15	3.5
Total		432	100.0

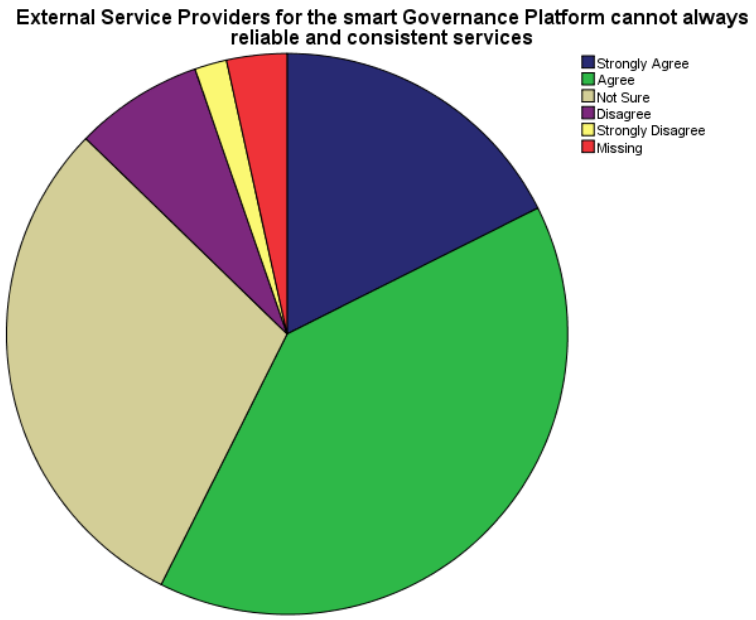

Figure 41: External Service Providers for the smart Governance Platform cannot always reliable and consistent services

As per the data given above, there were 432 participants in total in the survey 17.6% of them strongly agreed, 39% agreed, 29% were not sure, 7% were disagreed, and the remaining 1.9% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that External Service Providers for the smart Governance Platform cannot always reliable and consistent services.

The introduction of the smart Governance platform may result in a dearth of interpersonal skills from minimal staff recruitment.

The introduction of the smart Governance platform may result in a dearth of

interpersonal skills from minimal staff recruitment.

		Frequency	Percent
Valid	Strongly Agree	62	14.4
	Agree	177	41.0
	Not Sure	130	30.1
	Disagree	33	7.6
	Strongly Disagree	19	4.4
	Total	421	97.5
Missing	System	11	2.5
Total		432	100.0

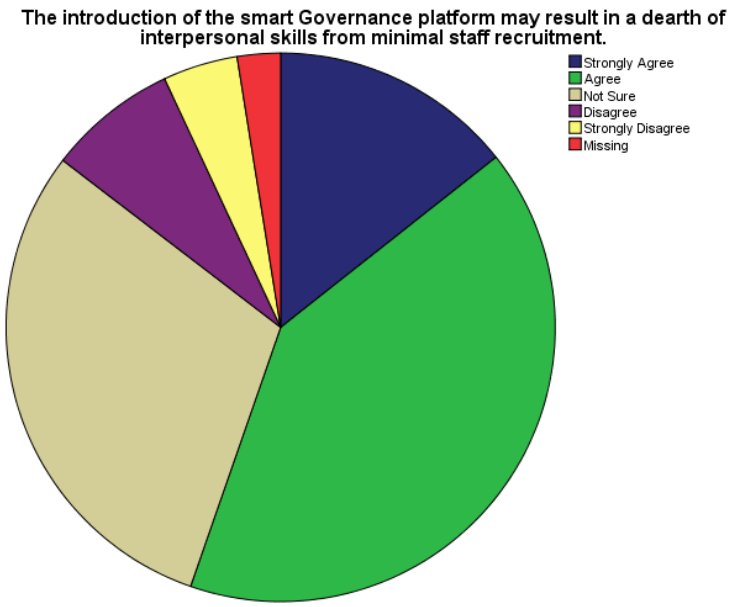

Figure 42: The introduction of the smart Governance platform may result in a dearth of interpersonal skills from minimal staff recruitment.

As per the data given above, there were 432 participants in total in the survey 14.4% of them strongly agreed, 41% agreed, 30% were not sure, 7% were disagreed, and the remaining 4.4% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the introduction of the smart Governance platform may result in a dearth of interpersonal skills from minimal staff recruitment.

In the event of a data breach, massive volumes of sensitive data could be get exposed to the public domain.

In the event of a data breach, massive volumes of sensitive data could be get exposed to the public domain.

		Frequency	Percent
Valid	Strongly Agree	74	17.1
	Agree	182	42.1
	Not Sure	122	28.2
	Disagree	32	7.4
	Strongly Disagree	9	2.1
	Total	419	97.0
Missing	System	13	3.0
Total		432	100.0

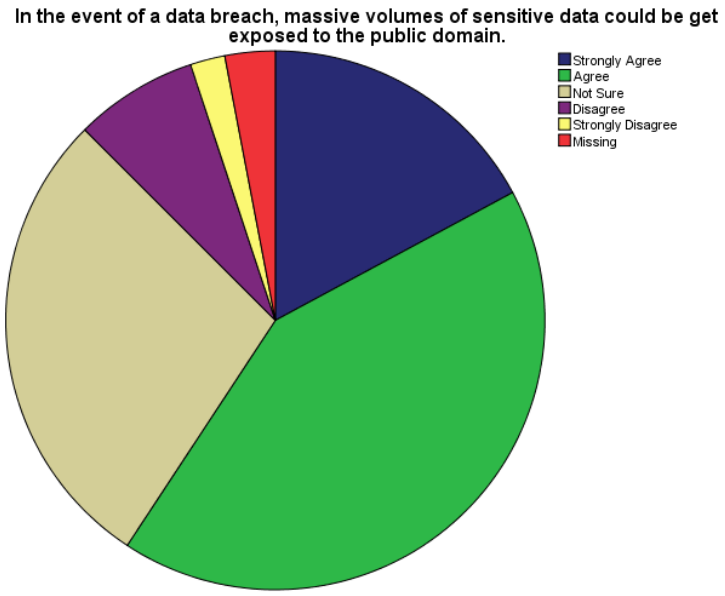

Figure 43: In the event of a data breach, massive volumes of sensitive data could be get exposed to the public domain.

As per the data given above, there were 432 participants in total in the survey 17.1% of them strongly agreed, 42% agreed, 28% were not sure, 7.4% were disagreed, and the remaining 2.1% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that in the event of a data breach, massive volumes of sensitive data could be get exposed to the public domain.

Resilience and risk management in smart government organization will enhance the capacity of the system to perform better even if there are issue in cyber environment

Resilience and risk management in smart government organization will enhance the	

capacity of the system to perform better even if there are issue in cyber environment

		Frequency	Percent
Valid	Strongly Agree	84	19.4
	Agree	183	42.4
	Not Sure	107	24.8
	Disagree	33	7.6
	Strongly Disagree	11	2.5
	Total	418	96.8
Missing	System	14	3.2
Total		432	100.0

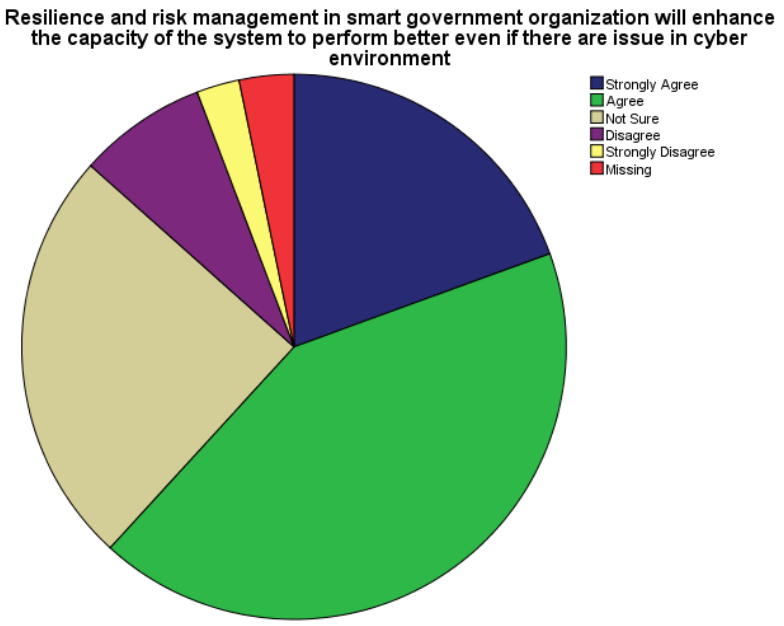

Figure 44: Resilience and risk management in smart government organization will enhance the capacity of the system to perform better even if there are issue in cyber environment

As per the data given above, there were 432 participants in total in the survey 19% of them strongly agreed, 42% agreed, 24% were not sure, 7% were disagreed, and the remaining 2.5% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Resilience and risk management in smart government organization will enhance the capacity of the system to perform better even if there are issue in cyber environment.

Resilience in smart government organizations will improve performance and output

Resilience in smart government organizations will improve performance and output

		Frequency	Percent
Valid	Strongly Agree	83	19.2
	Agree	186	43.1
	Not Sure	106	24.5
	Disagree	30	6.9
	Strongly Disagree	14	3.2
	Total	419	97.0
Missing	System	13	3.0
Total		432	100.0

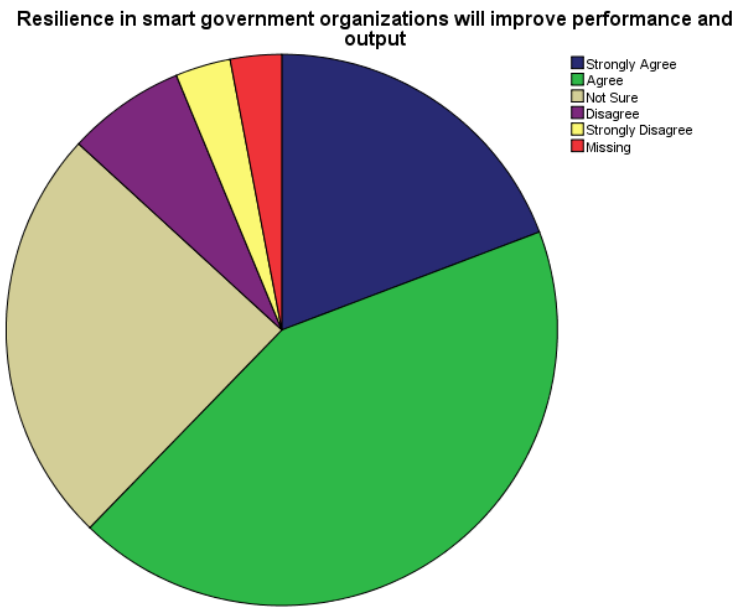

Figure 45: Resilience in smart government organizations will improve performance and output

As per the data given above, there were 432 participants in total in the survey 19.2% of them strongly agreed, 43% agreed, 24% were not sure, 6.9% were disagreed, and the remaining 3.2% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that Resilience in smart government organizations will improve performance and output.

The management control factors effect resilience in smart government organizations

The management control factors effect resilience in smart government organizations

		Frequency	Percent
Valid	Strongly Agree	81	18.8
	Agree	191	44.2
	Not Sure	117	27.1
	Disagree	18	4.2
	Strongly Disagree	13	3.0
	Total	420	97.2
Missing	System	12	2.8
Total		432	100.0

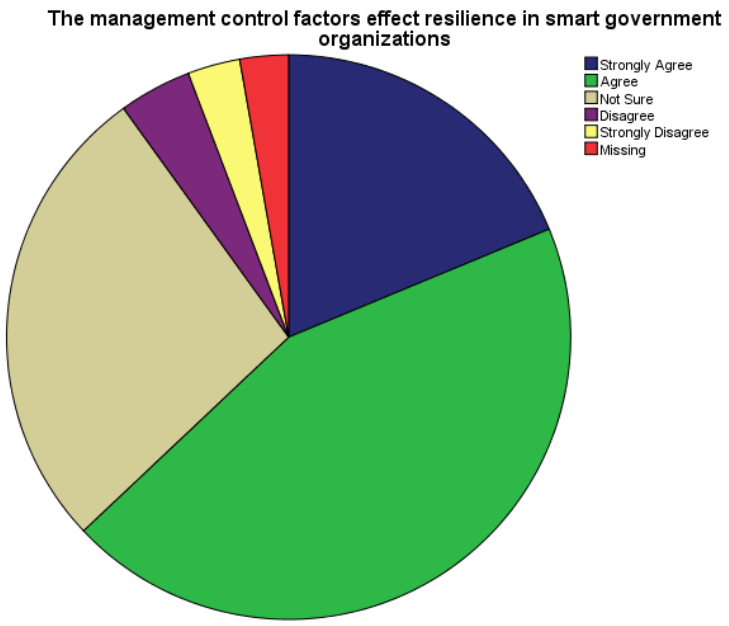

Figure 46: The management control factors effect resilience in smart government organizations

As per the data given above, there were 432 participants in total in the survey 18.8% of them strongly agreed, 44% agreed, 27% were not sure, 4.2% were disagreed, and the remaining 3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the management control factors effect resilience in smart government organizations.

The safe environment created by risk management will enhance technical competence in smart government organizations

The safe environment created by risk management will enhance technical competence in smart government organizations

		Frequency	Percent
Valid	Strongly Agree	96	22.2
	Agree	196	45.4
	Not Sure	90	20.8
	Disagree	27	6.3
	Strongly Disagree	11	2.5
	Total	420	97.2
Missing	System	12	2.8

Total	432	100.0

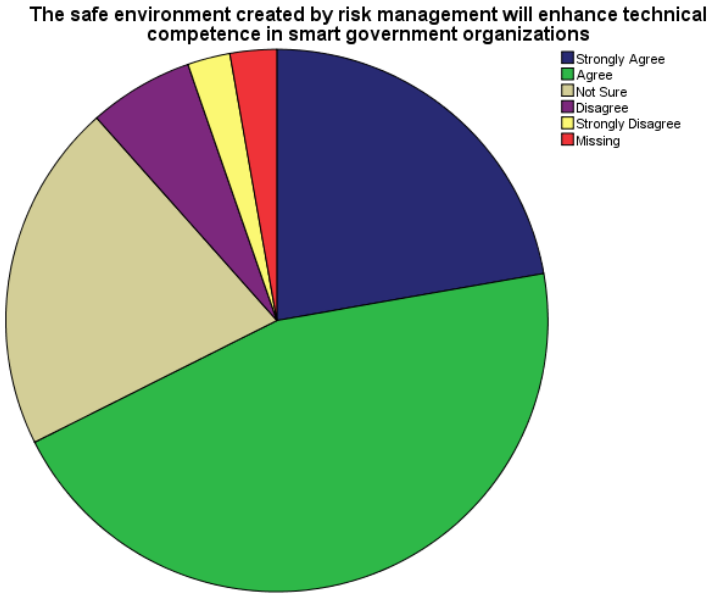

Figure 47: The safe environment created by risk management will enhance technical competence in smart government organizations

As per the data given above, there were 432 participants in total in the survey 22% of them strongly agreed, 45% agreed, 20% were not sure, 6.3% were disagreed, and the remaining 2.5% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the safe environment created by risk management will enhance technical competence in smart government organizations.

The overall performance of my organization will improve with the introduction or smart Governance resilience and risk management interventions

The overall performance of my organization will improve with the introduction or smart Governance resilience and risk management interventions

		Frequency	Percent
Valid	Strongly Agree	88	20.4
	Agree	201	46.5
	Not Sure	106	24.5
	Disagree	17	3.9
	Strongly Disagree	8	1.9
	Total	420	97.2
Missing	System	12	2.8
Total		432	100.0

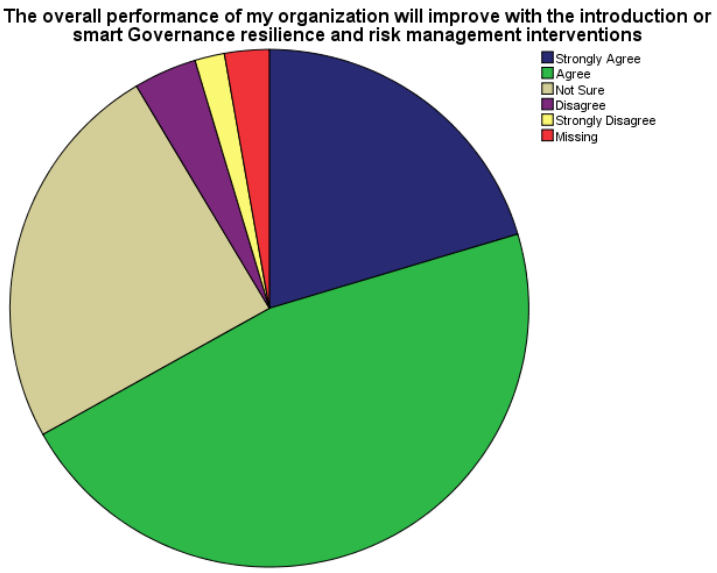

Figure 48: The overall performance of my organization will improve with the introduction or smart Governance resilience and risk management interventions

As per the data given above, there were 432 participants in total in the survey 20% of them strongly agreed, 46% agreed, 24% were not sure, 3.9% were disagreed, and the remaining 1.9% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the overall performance of my organization will improve with the introduction or smart Governance resilience and risk management interventions.

I think the organization will perform extremely well in the core functions because of the introduction of an smart Governance resilience and risk management policies

I think the organization will perform extremely well in the core functions because of the introduction of an smart	

Governance resilience and risk management policies

		Frequency	Percent
Valid	Strongly Agree	89	20.6
	Agree	196	45.4
	Not Sure	102	23.6
	Disagree	21	4.9
	Strongly Disagree	12	2.8
	Total	420	97.2
Missing	System	12	2.8
Total		432	100.0

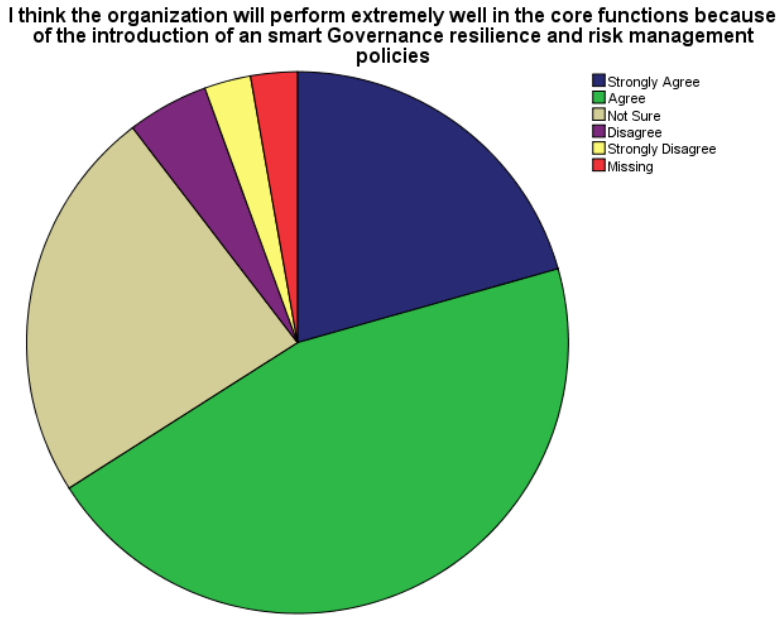

Figure 49: I think the organization will perform extremely well in the core functions because of the introduction of an smart Governance resilience and risk management policies

As per the data given above, there were 432 participants in total in the survey 20% of them strongly agreed, 45% agreed, 23.6% were not sure, 4.9% were disagreed, and the remaining 2.8% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that respondents think the organization will perform extremely well in the core functions because of the introduction of a smart Governance resilience and risk management policies.

The institution will greatly benefit from the new knowledge base and new skill requirements, occasioned by the introduction of a smart Governance risk management strategy

The institution will greatly benefit from the new knowledge base and new skill requirements, occasioned by the introduction of an smart Governance risk management strategy

		Frequency	Percent
Valid	Strongly Agree	94	21.8
	Agree	200	46.3
	Not Sure	93	21.5
	Disagree	22	5.1
	Strongly Disagree	12	2.8
	Total	421	97.5
Missing	System	11	2.5
Total		432	100.0

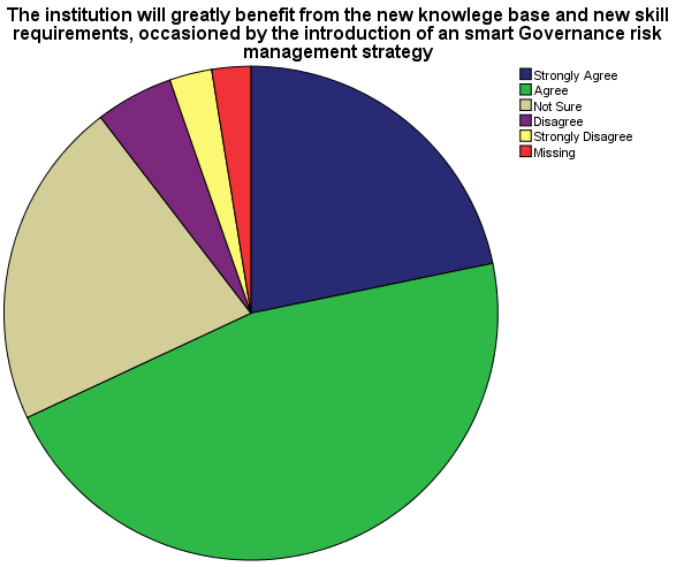

Figure 50: The institution will greatly benefit from the new knowledge base and new skill requirements, occasioned by the introduction of a smart Governance risk management strategy

As per the data given above, there were 432 participants in total in the survey 21% of them strongly agreed, 46% agreed, 5.1% were not sure, 4.9% were disagreed, and the remaining 2.8% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the institution will greatly benefit from the new knowledge base and new skill requirements, occasioned by the introduction of an smart Governance risk management strategy.

The smart governance Platform and associated Risk Management interventions will improve the overall satisfaction of the students and staff to the institution's service provision.

The smart governance Platform and associated Risk Management interventions

will improve the overall satisfaction of the students and staff to the institution's service provision.

		Frequency	Percent
Valid	Strongly Agree	74	17.1
	Agree	217	50.2
	Not Sure	106	24.5
	Disagree	15	3.5
	Strongly Disagree	10	2.3
	Total	422	97.7
Missing	System	10	2.3
Total		432	100.0

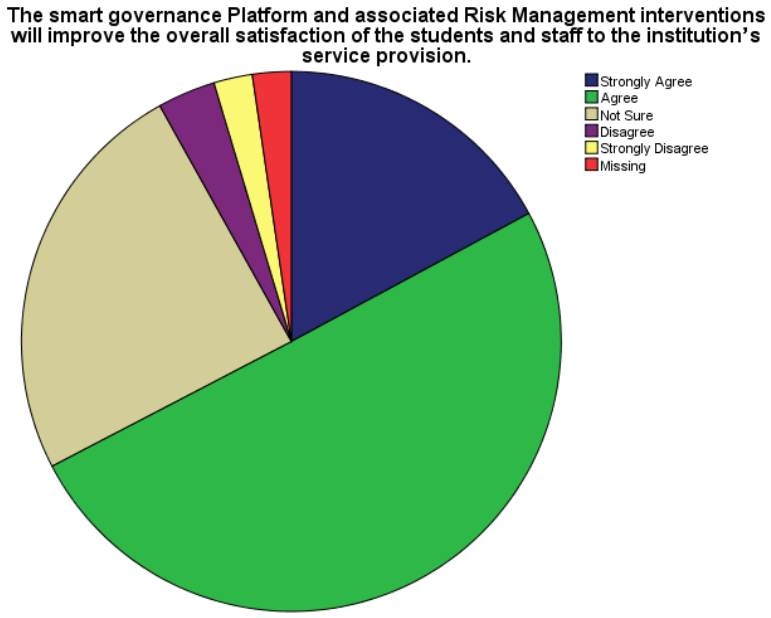

Figure 51: The smart governance Platform and associated Risk Management interventions will improve the overall satisfaction of the students and staff to the institution's service provision.

As per the data given above, there were 432 participants in total in the survey 17% of them strongly agreed, 50% agreed, 24.5% were not sure, 3.5% were disagreed, and the remaining 2.3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the smart governance Platform and associated Risk Management interventions will improve the overall satisfaction of the students and staff to the institution's service provision.

The introduction of the smart Governance risk management will result in higher profit margins and reduced operational costs.

The introduction of the smart Governance risk management will result in higher profit margins and reduced operational costs.

		Frequency	Percent
Valid	Strongly Agree	71	16.4
	Agree	182	42.1
	Not Sure	119	27.5
	Disagree	37	8.6
	Strongly Disagree	10	2.3
	Total	419	97.0
Missing	System	13	3.0
Total		432	100.0

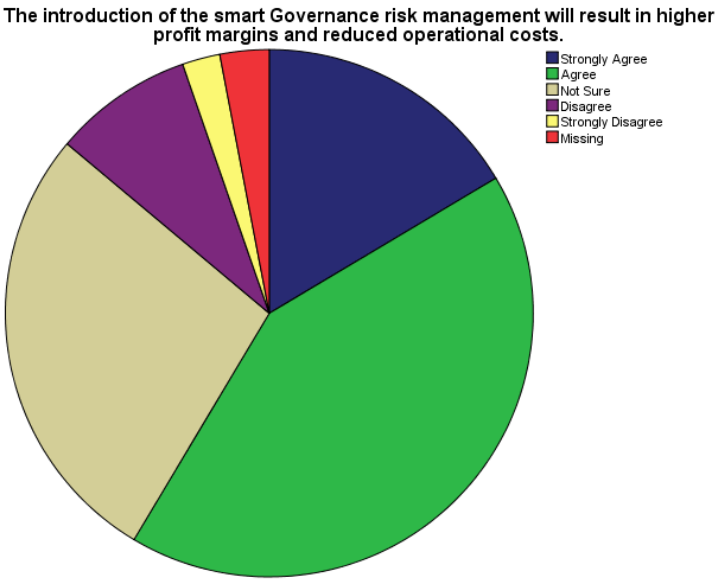

Figure 52: The introduction of the smart Governance risk management will result in higher profit margins and reduced operational costs.

As per the data given above, there were 432 participants in total in the survey 16.4% of them strongly agreed, 42% agreed, 27.1% were not sure, 8.6% were disagreed, and the remaining 2.3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the introduction of the smart Governance risk management will result in higher profit margins and reduced operational costs.

There are differences between smart government organizations in terms of using resilience and cyber security risk management

There are differences between smart government organizations in terms of using

resilience and cyber security risk management

		Frequency	Percent
Valid	Strongly Agree	79	18.3
	Agree	198	45.8
	Not Sure	109	25.2
	Disagree	25	5.8
	Strongly Disagree	8	1.9
	Total	419	97.0
Missing	System	13	3.0
Total		432	100.0

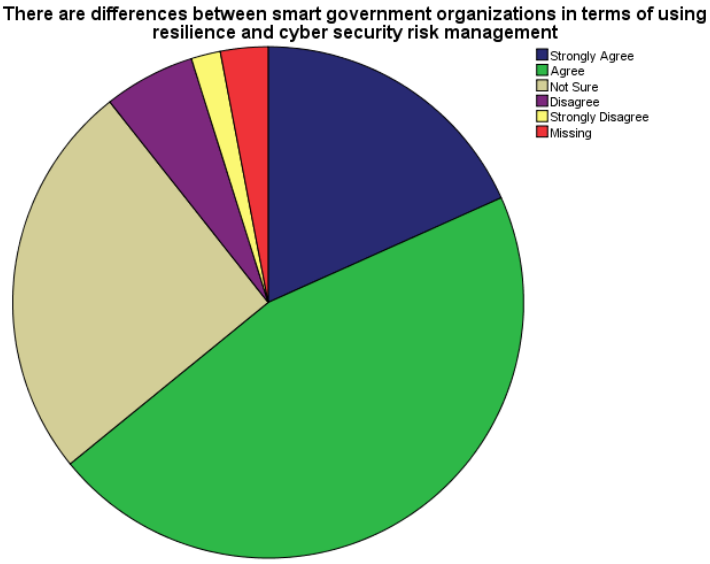

Figure 53: There are differences between smart government organizations in terms of using resilience and cyber security risk management

As per the data given above, there were 432 participants in total in the survey 18.3% of them strongly agreed, 45% agreed, 25.2% were not sure, 5.8% were disagreed, and the remaining 1.9% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that there are differences between smart government organizations in terms of using resilience and cyber security risk management.

The capability factors affect resilience in smart government organizations

The capability factors affect resilience in smart government organizations

		Frequency	Percent
Valid	Strongly Agree	75	17.4
	Agree	179	41.4
	Not Sure	127	29.4
	Disagree	25	5.8
	Strongly Disagree	14	3.2
	Total	420	97.2
Missing	System	12	2.8
Total		432	100.0

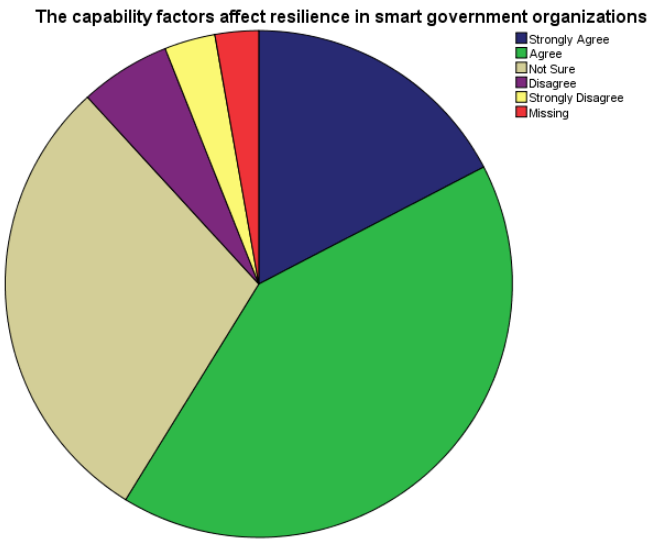

Figure 54: The capability factors affect resilience in smart government organizations

As per the data given above, there were 432 participants in total in the survey 17.4% of them strongly agreed, 41% agreed, 41.4% were not sure, 29.4% were disagreed, and the remaining 5.8% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the capability factors affect resilience in smart government organizations.

The change factors effect resilience in smart government organizations

The change factors effect resilience in smart government organizations

		Frequency	Percent
Valid	Strongly Agree	79	18.3

	Agree	177	41.0
	Not Sure	129	29.9
	Disagree	24	5.6
	Strongly Disagree	12	2.8
	Total	421	97.5
Missing	System	11	2.5
Total		432	100.0

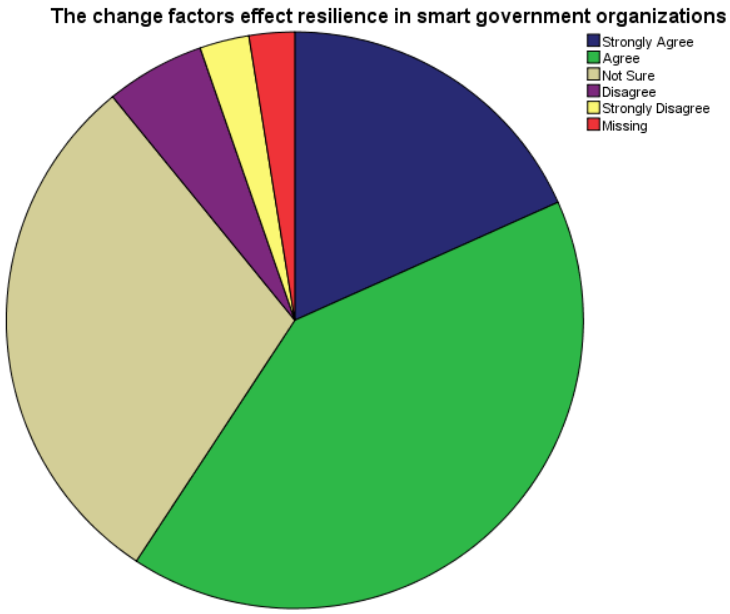

Figure 55: The change factors effect resilience in smart government organizations

As per the data given above, there were 432 participants in total in the survey 18.3% of them strongly agreed, 41% agreed, 29% were not sure, 5.6% were disagreed, and the remaining 2.8% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that

the majority of participants were agreed that the change factors effect resilience in smart government organizations.

The vulnerability factors effect resilience in smart government organizations

The vulnerability factors effect resilience in smart government organizations

		Frequency	Percent
Valid	Strongly Agree	92	21.3
	Agree	191	44.2
	Not Sure	109	25.2
	Disagree	17	3.9
	Strongly Disagree	10	2.3
	Total	419	97.0
Missing	System	13	3.0
Total		432	100.0

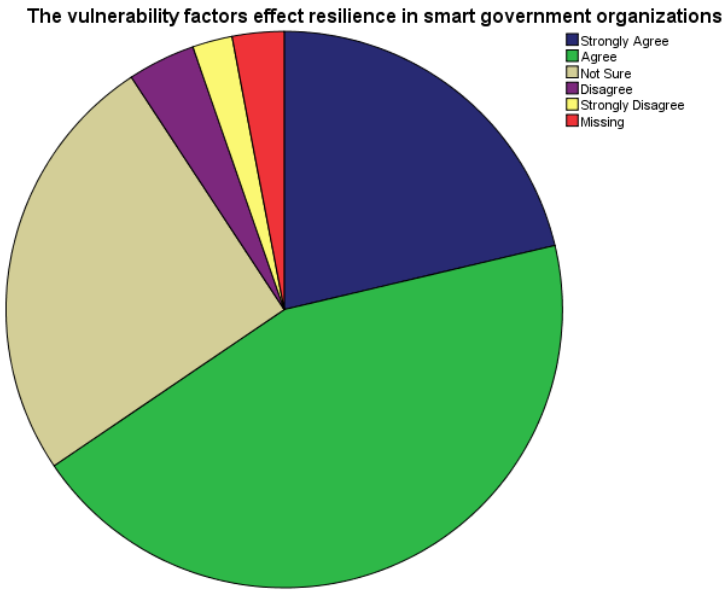

Figure 56: The vulnerability factors effect resilience in smart government organizations

As per the data given above, there were 432 participants in total in the survey 21.3% of them strongly agreed, 44.2% agreed, 25% were not sure, 3.9% were disagreed, and the remaining 2.3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the vulnerability factors effect resilience in smart government organizations.

The resilience framework is about detecting, preventing, and recovering from a cyber-attack

The resilience framework is about detecting, preventing, and recovering from a cyber-attack

	Frequency	Percent

Valid	Strongly Agree	95	22.0
	Agree	187	43.3
	Not Sure	108	25.0
	Disagree	19	4.4
	Strongly Disagree	10	2.3
	Total	419	97.0
Missing	System	13	3.0
Total		432	100.0

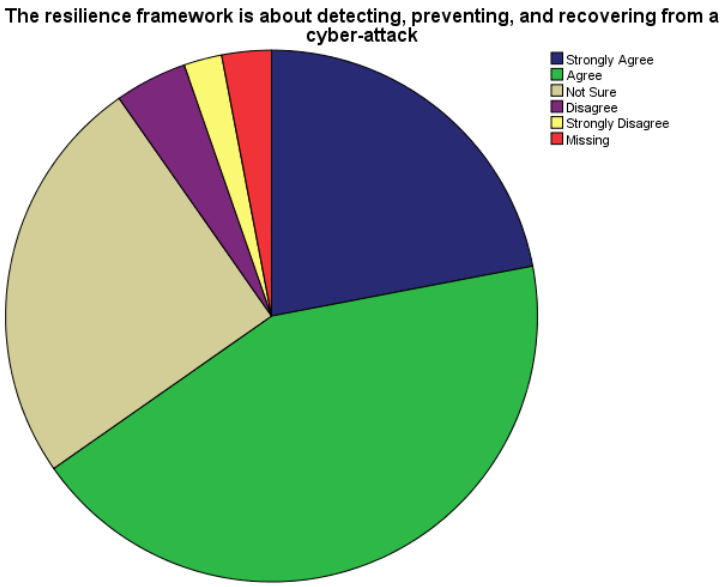

Figure 57: The resilience framework is about detecting, preventing, and recovering from a cyber-attack

As per the data given above, there were 432 participants in total in the survey 22% of them strongly agreed, 43% agreed, 25% were not sure, 4.4% were disagreed, and the remaining 2.3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the resilience framework is about detecting, preventing, and recovering from a cyber-attack.

The forces of change cause vulnerabilities that provoke the need for resilience in organizations

The forces of change cause vulnerabilities that provoke the need for resilience in organizations

		Frequency	Percent
Valid	Strongly Agree	75	17.4
	Agree	181	41.9
	Not Sure	124	28.7
	Disagree	29	6.7
	Strongly Disagree	12	2.8
	Total	421	97.5
Missing	System	11	2.5
Total		432	100.0

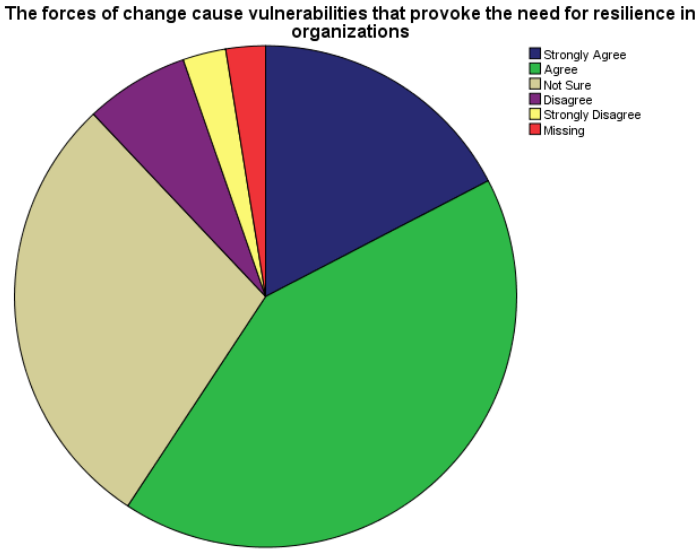

Figure 58: The forces of change cause vulnerabilities that provoke the need for resilience in organizations

As per the data given above, there were 432 participants in total in the survey 17.4% of them strongly agreed, 41% agreed, 28% were not sure, 6.7% were disagreed, and the remaining 2.8% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the forces of change cause vulnerabilities that provoke the need for resilience in organizations.

The implementation of balanced resilience can result in improved performance

The implementation of balanced resilience can result in improved performance

	Frequency	Percent

Valid	Strongly Agree	95	22.0
	Agree	196	45.4
	Not Sure	97	22.5
	Disagree	20	4.6
	Strongly Disagree	12	2.8
	Total	420	97.2
Missing	System	12	2.8
Total		432	100.0

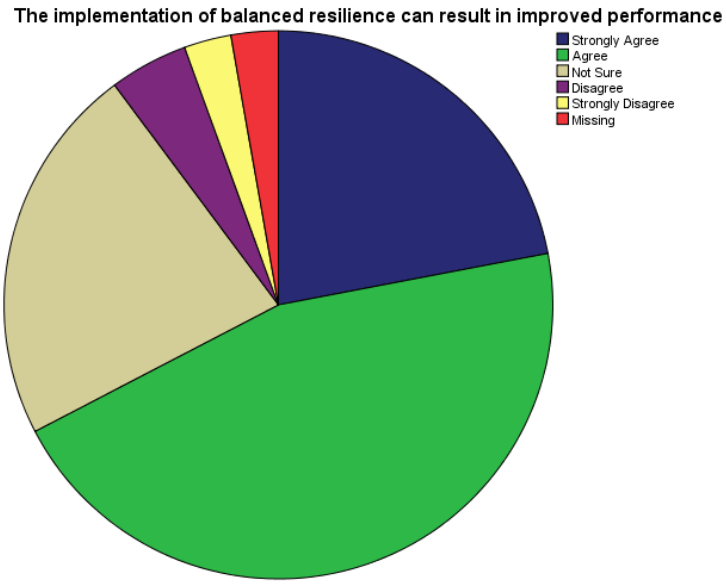

Figure 59: The implementation of balanced resilience can result in improved performance

As per the data given above, there were 432 participants in total in the survey 22% of them strongly agreed, 45% agreed, 22.5% were not sure, 4.6% were disagreed, and the remaining 2.8%

were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the implementation of balanced resilience can result in improved performance..

Unbalanced resilience in organizations can impose excessive frisks and erode profitability

Unbalanced resilience in organizations can impose excessive frisks and erode profitability

		Frequency	Percent
Valid	Strongly Agree	85	19.7
	Agree	200	46.3
	Not Sure	103	23.8
	Disagree	20	4.6
	Strongly Disagree	13	3.0
	Total	421	97.5
Missing	System	11	2.5
Total		432	100.0

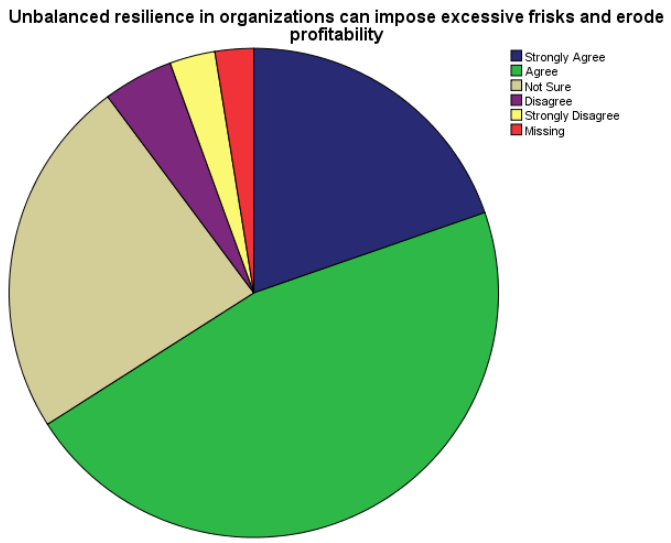

Figure 60: Unbalanced resilience in organizations can impose excessive frisks and erode profitability

As per the data given above, there were 432 participants in total in the survey 19.7% of them strongly agreed, 46% agreed, 23.8% were not sure, 4.6% were disagreed, and the remaining 3% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that unbalanced resilience in organizations can impose excessive frisks and erode profitability.

The resilience can help organizations in evaluating risks and challenges involved at multiple levels

The resilience can help organizations in evaluating risks and challenges involved at multiple levels

		Frequency	Percent
Valid	Strongly Agree	98	22.7
	Agree	195	45.1
	Not Sure	96	22.2
	Disagree	17	3.9
	Strongly Disagree	15	3.5
	Total	421	97.5
Missing	System	11	2.5
Total		432	100.0

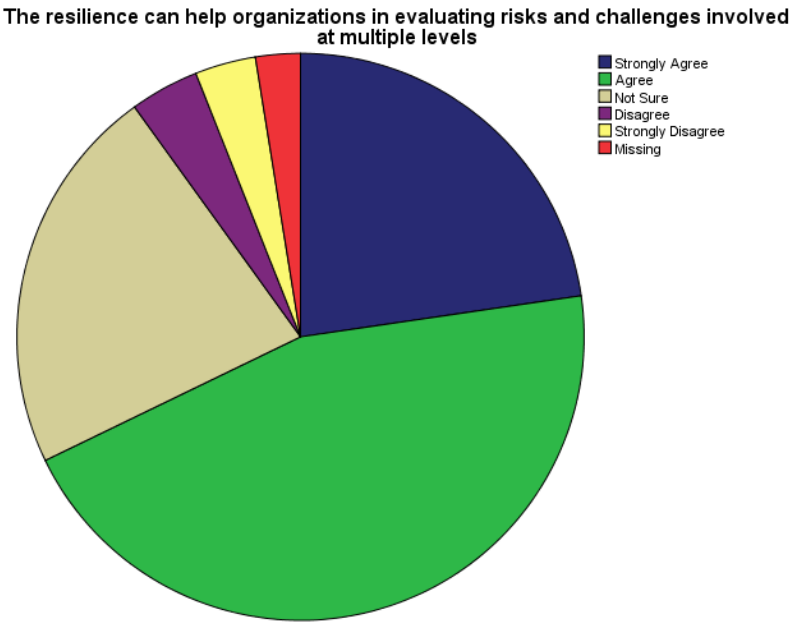

Figure 61: The resilience can help organizations in evaluating risks and challenges involved at multiple levels

As per the data given above, there were 432 participants in total in the survey 22.7% of them strongly agreed, 45% agreed, 22.2% were not sure, 3.9% were disagreed, and the remaining 3.5% were strongly disagreed. As per the given data in both chart and table, it is demonstrated that the majority of participants were agreed that the resilience can help organizations in evaluating risks and challenges involved at multiple levels.

[i] Read more: http://www.businessdictionary.com/definition/risk-management.html

[ii] Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press.
[iii] www.ecmweb.com

[iv] Cyber-Security & Risk Management, an evolving ecosystem, 2016
[v] NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009, p. 1

[vi] Cyber-Security & Risk Management, an evolving ecosystem, 2016
[vii] Cyber-Security & Risk Management, an evolving ecosystem, 2016