Modelling Risks for Physical Security Assets Development and Operation in High-Value Retailer Projects in the UAE

نمذجة و محاكاة المخاطر في تطوير الأمن المادي في مرحلة التشغيل والتطوير للمشاريع (في قطاع المحلات ذات القيمة العالية) في دولة الإمارات العربية المتحدة

by

SULAIMAN RASHED SAEED SULAIMAN ALSHEBLI

A thesis submitted in fulfilment

of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN PROJECT MANAGEMENT

at

The British University in Dubai

Prof. Halim Boussabaine

December 2017

Modelling Risks for Physical Security Assets Development and Operation in High-Value Retailer Projects in the UAE

نمذجة و محاكاة المخاطر في تطوير الأمن المادي في مرحلة التشغيل والتطوير للمشاريع (في قطاع المحلات ذات القيمة العالية) في دولة الإمارات العربية المتحدة

by

SULAIMAN RASHED SAEED SULAIMAN ALSHEBLI

A thesis submitted to the Faculty of

in fulfilment of the requirements for the degree of

PhD in Project Management

at

The British University in Dubai

December 2017

Thesis Supervisor
Professor Halim Boussabaine

Approved for award:

___________________________ ___________________________

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that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.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

As the drive towards efficiency and effectiveness in infrastructure spending intensifies, the topic of WLCC (Whole Lifecycle Costing) has taken added importance, aligned with the general mandate of providing the best value for money. The domain of spending on PSA (Physical Security Assets) thereby requires assessment not just regarding the cost but also in various dimensions of risk management, to fulfill the needs and requirements of the users. In addition to that, all elements connected with the PSA need to be analyzed and assessed with a holistic cost-benefit analysis framework.

The research aims at undertaking a stochastic analysis of the whole ambit of costs associated with PSA (physical security assets) from feasibility to disposal, with the aim of generating output regarding economic and non-economic indicators. This exercise would generate thus a model which can be deployed by both the private and the public sectors for making better decisions regarding PSA investments, and obtaining best value.

Data collection has been done through a survey and other sources, with probabilistic distributions derived for the relevant WLCC cost centers along with validation of the same through statistical tools. Monte Carlo simulation techniques have been used to provide the users with pre-defined parameters. Various sensitivity analysis measures have been incorporated to gauge the variability through changes to crucial inputs.

The proposed WLCC model would enable the users to assess the factual overall running costs of investment in PSA, along with risk management parameters, thereby facilitating investment policy implementation. As opposed to deterministic forecasts, it would enable the users to quantify the associated risks with a relative level of certainty. It would, therefore, contribute towards the more efficient use of budgets, equipping the users with statistical results to confidently make the judgment calls regarding various options of investment in PSA.

مقدمة

مع تزايد الحاجة الملحة الى الكفاءة والفعالية في الإنفاق على مشاريع البنية التحتية ، فإن موضوع WLCC (التكلفة الكاملة لدورة الحياة) أخذ أهمية إضافية ، بما يتماشى مع الولاية العامة لتوفير أفضل قيمة مقابل المال. وبالتالي ، فإن مجال الإنفاق على PSA (أصول الأمان المادية) يتطلب التقييم ليس فقط من حيث التكلفة ولكن أيضًا في الأبعاد المختلفة لإدارة المخاطر ، من أجل تلبية احتياجات ومتطلبات المستخدمين والأفراد. و مع ذلك ، يجب تحليل جميع المخاطر المرتبطة بـ PSA وتقييمها من خلال إطار تحليل شامل للتكاليف والفوائد.

يهدف البحث إلى إجراء تحليل عشوائي لكل نطاق التكاليف المرتبطة بـ PSA (أصول الأمان المادية) من بداية المشروع إلى المرحلة النهائية ، بهدف توليد المخرجات فيما يتعلق بالمؤشرات الاقتصادية وغير الاقتصادية. ويهدف أيضا أن يخرج نموذجًا يمكن نشره من قبل القطاعين العام والخاص لاتخاذ قرارات أفضل فيما يتعلق باستثمارات دعم البرامج والإدارة والحصول على أفضل قيمة

Acknowledgment

This was a challenging journey, but well worth it. It would not have been possible without the guidance and encouragement of some extraordinary and dear people who inspired and gave me the motivation to carry on.

I would especially like to express sincere gratitude and thanks to my supervisor Prof. Halim Boussabaine who instilled in me the belief and set challenging yet motivating targets on the course of this dissertation. His scholarly expertise and supportive demeanor made this a pleasant experience. Right from the planning “initial” stage to the execution and feedback, all along he was extremely professional and diligent in his overview and strategic direction of the dissertation. At times, I felt he was making me work too hard, but it all fell into place together every single time, as I emerged a better student and academic after undergoing the robustregime. He provided the perfect balance in extracting from me creative capacity and risk management skills, and in making timely interventions when he considered the work needed better alignment. I feel I am privileged to have won a friend too, and an invaluable area specialist whose superb command in the domain of risk management would be very precious for me in the future too. Myheartfelt thanks again to Prof. Boussabaine for his brilliant guidance.

Secondly, I would like to thank my parents and my family for their patience, as they knew their son was engaged in something critical for professional development, and the sacrifice they made through not being too demanding for my time all the while.

I am indebted also to the good graces of BUID Vice Chancellor Prof. AlShamsi who always carried a smile whenever I needed to discuss my academics during my time at the University. I am confident I have validated through this dissertation the confidence he has in me.

Many others facilitated my research through being amenable to data collection and discussion, both at my workplace and also regarding the management of the corporations I was engaged with for this research.

Thank you all for making me feels accomplished and making this dream possible!

Table of Contents

Table of Figures

List of Tables

CHAPTER 1. INTRODUCTION

1.1 *Introduction*

This chapter defines the research problem with little introduction, theoretical background of the research. The chapter also presents the research framework, questions, aims and objectives and subsequently methodology. The last section of this chapter provides a summary of this research and thesis.

1.2 *Research Context and Background Information*

Governments across the world have ways of ensuring that both public and private sector enterprises within their domains can deliver their services to customers in the most effective, efficient and economical manner. Hence, the notion 'best value' came to the fore in many European nations in the 1990s. This resulted in fundamental changes in infrastructure spending and models of procurement, thereby giving rise to the growth in understanding and implementation of the domain of Whole Life-Cycle Costing (WLCC). This goes hand in hand with the discipline of the general practice of procurement to obtain the most productive outcome of whole life-cycle costs and quality that meet user needs (Boussabaine & Kirkham, 2004).

Hence, best value can be asserted as the main concept that must be considered when contracts are awarded for spending, and on physical security assets (PSAs), too, since merely allocating on the basis of the lowest capital quote would not necessarily result in best practice. Such a process has to incorporate WLCC and thus the phenomena have been made mandated in the compulsory in the UK, whereby all public entities are required to employ WLCC to justify their spending. This also includes innovative public-private approaches. WLCC is essential for enhancing procurement models and thus for meeting stringent public sector requirements such as those in the UK. This becomes even more important in times of fiscal austerity and overall economic slowdown, where the value for money takes on another important dimension.

WLCC provides a more thorough assessment of overall costs when coupled with PSA spending. This is in contrast to the traditional approach of generally focusing on short-term acquisition and basic operational costs. An added feature of WLCC is its factoring in of the risk assessment procedures, thus providing a more holistic look at the spending process. By their very nature, spending on PSAs is long-term in nature, and thus risks abound relating to operations, life and maintenance aspects of the assets.

Quantification of risk is a central theme in WLCC, whereby risk-modeling techniques are employed. It aligns with life-cycle costing, which is a natural evolution of the theme, although it is more dynamic since WLCC is capable of providing updated projections on costs and performance throughout PSAs' lives. Here, it matches the requirement for PSA spending in terms of meeting and exceeding client expectations in overall costefficiency and design economies, monitoring, sustainability, and cost-effectiveness. The following definition lays out the essential elements of WLCC, especially with regard to the enhancement of the concept of life-cycle costing:

WLCC is a fully integrated process that empowers a stochastic performance evaluation of the facilities built up in this manner. Sundry features including the sustainability, their maintenance, ability to be re-used and features of their obsolescence are factored in. The outcomes – both economic and non-economic performance indicators facilitate the stakeholders throughout the lifecycle of a project (Boussabaine & Kirkham, 2004).

1.3 Theoretical Background

1.3.1 Prior Analysis

The aim of WLCC, according to Curran (1996), is to help managers, who, by using the method, become empowered to undertake a more useful and systematic analysis of the life-cycle costs associated with PSAs, such as CCTV systems. The ongoing utilization of assets such as CCTV is a critical factor to decide on, and as the phenomenon also includes accessories to effectively operate the equipment, WLCC grant decision makers a fuller view of the perspective.

Crime prevention has historically been the main reason for PSA spending, which also includes elements like physical supervision, defense,and lighting. Thus, CPED is the main theme relating to crime prevention through effective utilization of environmental design. A main functionality of CPED is to mitigate the likelihood of damage caused by crime by implementing a design that is highly sophisticated, with the additional perception of criminal risk. The physical defenses then detect and deter any likely penetration of protected zones. Ko, Park and Kim (2016) assert that even after much research and spending on technology, it cannot be absolutely assured that the same would not be breached, as there have been multiple cases of security system breaches, albeit sophisticated, thus raising questions over the whole apparatus. It must be understood, thus, that a system, however advanced, cannot provide absolute assurance against a breach. Nevertheless, the more robust a system is in terms of design and implementation, the higher assurance it provides, and the more it mitigates potential losses of millions of dollars to companies.

CCTV has become a main component of PSAs, especially in the wake of technological breakthroughs in CCD cameras and image intensification technology, according to Harris et al. (1998). Fennelly (2012) asserts that CCTV is still one of the most critical asset protection devices available and thus is invariably an essential component in a number of PSAs that aim to deter and detect an unauthorized entry in a protected space. CCTV has also improved the effectiveness of various other physical defenses. Kruegle (2007) conducts a study that concludes that locks and other physical security devices operate more effectively when linked to a CCTV system. Moreover, a study by Loughborough University (2003) validates that a CCTV system works better when integrated within a comprehensive security system, and the more it is coherently linked to the system, the better it serves, because remote areas can also be linked to it.

Siergiejczyk, Paś, and Rosiński (2015) state that cost represents the immediate outflow for an organization, but a needed analysis includes all the lifecycle–associated costs of a PSA. Hence, the overall cost is much higher than the initial PSA outlay, with wide ranges between alternatives, keeping under consideration the evolving environment and the needs of an organization.

1.3.2 Risk Assessment

This is critical to PSA spending and in evaluating overall results to a firm. The flux prevalent in the current environment further underlines this. Final decisions are based on the expectations, the management of the desires and the preferences of a number of stakeholders, with varying degrees of risk associated with each potential avenue. WLCC provides a system where risks associated with cost forecasts are enumerated through probability distribution and could be sounder if they could be defined as explicitly as possible (Boussabaine & Kirkham, 2004). An analyst can face many challenges and difficulties in this step, as many variables can be difficult to measure and quantify, especially those regarding inflation, operational costs, and other estimates. Thus, the relevance and importance of WLCC diminish in instances where a highly accurate measure needs to be calculated; when many interlinked variables are hard to quantify, the linkages can become very complex, rendering the process of estimation quite inaccurate and thus inoperative. Therefore, an important conclusion is that for a robust application, various models should be constructed for the purpose.

The designing, project parameters, design and costs (operative) of a PSA are determined early on in a project. They are filtered through owners' and project teams' own experiences and frames of reference and it is therefore not particularly suitable to manage risks and make decisions based on them alone. WLCC provides a systematic framework, as it evaluates parameters for existing methods that cannot be accurately quantified. To do this, the process has to include a strong risk management apparatus. Data collection requires considerable time and effort, but when not allied to strong methods and tools, it results in little utility and fails to serve its purpose for clients. WLCC addresses this issue by considers and evaluates the risk dimensions of all angles of a decision so that it extracts a productive result of risks and the associated expenses.

1.3.3 Requirements re data for PSA WLCC

The process calls for a well-composed body of steps that are required to extract the data, connected in a series of related phases of the WLCC. Various sources provide these data, including direct component cost estimates, historical information, judgment and performance-level models (Boussabaine & Kirkham, 2004). It is normally the case that the specialists and the contractors who deal with the PSA have with them through lists and other details of the associated costs.

Other models can be put to use to construct the data and draw up life-cycle profiles. In this regard, simulation data are considered to be better estimators than historical cost data in assessing applicability (Ferry & Brandon, 1991). Simulation essentially focuses on the oncoming, instead of the past, as the past can be a poor sphere to employ in forecasting. Historical data can also be supplemented with simulated data through advanced statistical techniques.

1.3.4 Use of Operational Research

The following steps need to be done in sequence regarding operational research (OR) (Boussabaine & Kirkham, 2004, p. 17):

- Composing a framework of the problem, along with the related constraints and the aims
- PSA system model to be formed up
- Achieving solution through the model
- Comparing and contrasting the solution with the given current solution
- Assessing the outcomes and continually monitoring the performance

Estimates and ideas need to be made regarding the major PSA parts, risks of failure of those components, quality, maintenance systems, cost constraints, maintenance duration and its impact, disposition viability and other replacements (Boussabaine & Kirkham, 2004, p. 18).

1.3.5 Obsolescence

As the contemporary environment is in a state of flux, with firms experiencing high technological advancements and breakthroughs, PSA infrastructure is vulnerable to obsolescence more now than it has been. The obsolescence factor directly impacts the useful lives of PSA components, and thus the structure of risk assessment must include this fundamental element, too. Crucially, the risks PSAs are geared toward mitigating may evolve, rendering the systems obsolete. This can become a complex exercise to anticipate and provide for, as it includes a host of intangible elements, including disruption and externalities, economic obsolescence, legal and regulatory imperatives of change, costs of disposition, wastage clearance, and cleaning costs.

1.3.6 Capital Costs, inclusive of Initiation and Acquisition

PSA practicality can be assessed by undertaking a return-on-investment measure. Although assumptions regarding capital commitments are not explicit, they have to be made for elements of pre-design costs, design, development, and installation, financial costs, etc. This also includes consultancy fees, survey feeds, camera and cabling costs, accessories and other elements.

1.3.7 Operational and Maintenance Costs

Ristimäki et al. (2013) state that the benefits obtained through WLCC rest largely on the validity of the assumptions made regarding future operating costs and CCTV maintenance costs. Although future costs may be calculated inexactly, that does not make WLCC useless; in spite of that fact, WLCC has the benefit of making analysts view more closely the ever-changing landscape regarding energy costs, regulatory imperatives, maintenance and others through a holistic framework that enables them to better assess capital spending and other associated decisions regarding PSA. Crucial costs of operation including the management systems of risks identified procedures for cleaning, regarding the staff, along with costs regarding disruptive elements and the control room costs. Costs of maintenance would include ones for replacing the assets, maintenance for routine and sub-contracted work.

1.3.8 Asset characteristics

WLCC computations must include an assessment of the physical structures within which PSAs are to be placed and positioned, along with the functional characteristics of the premises. A poorly maintained building, for example, or one that has structural faults likely increases the elements of risk associated with maintaining and even installing a PSA.

1.4 *Framework for WLCC Risk Management*

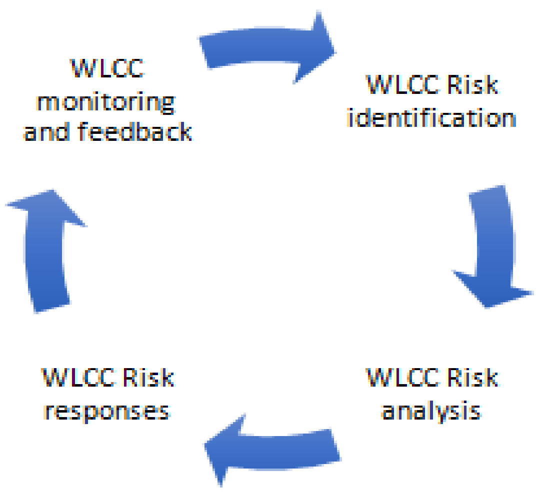


Figure 1-1: Derived from the framework for integrated WLCC risk management (Boussabaine &Kirkham, 2004, p. 23)

WLCC optimisation has taken on a new dimension due to the rise in PSA expenditures. Uncertainty generally abounds in this phenomenon, with decision makers having to face variability in assessments and the possible outcome that PSA spending is deferred or canceled. Moving away from PSA spending can turn out to be disadvantageous for a firm. In this context, WLCC provides a mechanism that accommodates the inherent spending uncertainties and provides useful tools for managers to evaluate the utility of PSA spending.

WLCC sidesteps the need to have the large amount of data required by conventional risk management systems, as it utilises data a company already has in possession. A combination of risk management techniques must be used for WLCC risk assessment, including breakeven and sensitivity analyzes. The high-level work methods of probability distribution and artificial intelligence measures can also be incorporated. An iterative linkage of the five elements enables stakeholders to carefully assess the consequences of various courses of action in a coherent and logical manner by considering the components' interlink ages (Boussabaine & Kirkham, 2004, p. 23). The sequence is given underneath:

1.4.1 Whole life risk identification

Each whole life-cycle process has elements of risks associated with it that can be harmful to the interests of stakeholders. Hence, those risks must be measured and identified in their entirety, with the work in this phase heavily impacting later analysis, quantification and risk response measures throughout the life of the PSA.

1.4.2 Whole life risk analysis

Sophisticated methods such as probabilistic and deterministic measures and AI can be used (Boussabaine & Kirkham, 2004, p. 24). As there is no measure that by itself covers the vast ambit of outcomes connected with a risky investment, probabilistic measures are required. The probability distribution is constructed such that a large number of avenues are considered, followed by statistical analysis to quantify the associated risk. Subjectivity is inherent in this exercise and AI can be employed to model the riskiness inherent in WLCC analysis by using historical data. There is no single method that can be judged to be the most appropriate and suitable for each and every case. Rather, that depends on the specifics of the case, the extent of data and resource availability, PSA investment size, skills and competence of the user and the user's judgment in ascertaining the best method to be selected and applied to the case at hand.

1.4.3 Whole life risk responses

In the next phase, responses to WLCC risks must be developed (Boussabaine & Kirkham, 2004, p. 25). PSA investments have to be protected through adequate risk responses upon identification of associated risks and their measurements. Risk avoidance, acceptance, sharing, absorption, and transfer are some of the practical choices that can be made, depending on the specifics of each case.

1.4.4 Whole life risk management plan

Roles and responsibilities of various connected parties in the mechanism regarding initiation and implementation must be carefully established with pre-determined and delineated courses of action. This must be coordinated carefully to be seamless so that the management can provide an essential input in the process by identifying and recommending staff to be assigned duties for each response at the relevant hierarchy levels.

1.4.5 Whole life risk monitoring and feedback

It is a norm in the case of PSA projects that initial decisions are changed to different extents as a project progresses. There is a need, thus, for continual assessment and for a feedback mechanism for risk management. Procedures would be assessed for their effectiveness, response priorities would be established, and risks would be monitored closely. Moreover, WLCC assessments would be updated continually and economic measures reviewed periodically to determine the appropriateness of an investment decision as a project moves forward (Boussabaine & Kirkham, 2004, p. 25).

1.5 *Objectives of the Research*

The main assertion in this thesis is that UAE PSA investment spending is not backed up by an adequately robust system of WLCC analysis. Hence to evolve a model that can be applied to the UAE is a specific aim of the exercise. This study has the following aims:

- To enable the stakeholders to apply a probability system for undertaking cost simulation where that information is not readily available.
- To enable users to calculate PSA WLCC estimates by employing probabilistic methods to values that can be related to the confidence interval.

- To provide a model through which the WLCC of PSA spends can be contrasted.
- To provide users valuable performance measurement techniques to draw useful inferences from

A risk-based WLCC PSA investment model achieves the above objectives and provides the following ancillary objectives, too:

- To review the evolution of the WLCC model by analyzing its theoretical constructs and mathematical techniques
- To review WLCC methodology literature with the aim of integrating its elements in work
- To assess the ongoing performance measurement techniques and link them to the WLCC environment
- To undertake a substantial review of the current UAE PSA investment practices and link them to the WLCC model for future policy formulation

1.6 *Research Questions*

- What are the mathematical techniques used by scholars and practitioners in performing PSA WLCC?
- What are the optimum approaches for PSA WLCC analysis?
- Does the established WLCC framework lead to effective and efficient risk management for UAE PSA investments?

1.7 *Methodology*

Prototype modeling is achieved through a thorough review of existing WLCC methodologies as currently employed in the UK and other European countries. This also includes applying stochastic measures to WLCC approaches with work on co-creation between the various parties. The relevant WLCC equation would thus be able to be extracted through this exercise. Hence, the following sums up methods used in this research:

1. A string review of the various WLCC literature sources along with the management of risks is carried out. This step will help in determining the most appropriate WLCC center for costs.

- A survey is conducted among planners, sponsors and other stakeholders in order to assess their opinions regarding PSA investments in UAE. It provides the researcher the needed data for realizing the related cost centers of WLCC.
- The data gathered help enhance the information and knowledge needed to analyze a major public sector investment. The knowledge gained can then be employed in applying to the UAE and thus in the research would serve as the triangulation to assess the extracted model.
- Cost data relating to WLCC cost centers are checked for their probabilities to obtain the needed elements.
- To establish the validity of the probability distributions thus obtained, chi-square and other statistical tools are employed.
- For all the cost centers, a WLCC model is evolved. Monte Carlo simulation is employed so that WLCC is given by the probability function.
- The present values of WLCC are gauged with reference to a range of performance measurement techniques.
- The findings of the above analysis are compared and contrasted to the existing WLCC models, and the main scientific analysis findings are identified and articulated.

1.8 *Outline of the Thesis*

This research is divided into 11 chapters to get the area of the theme clearly.

Chapter 1 includes the introduction, conceptual theoretical analysis, and the research reasoning. The justification for the research is also drafted, and the research methodology is covered.

Chapter 2 is composed of a WLCC literature review, and the relevant findings for UAE are identified and summarized.

Chapter 3 deals with the WLCC mathematical analysis and the application of risk theory to WLCC.

Chapter 4 discusses the theory and application of risk management in WLCC research. It covers an analysis of the five related components of the model and analyzes the statistical measures that have been used in the past. Deterministic and stochastic models are also analyzed in detail.

Chapter 5 includes work on the costs related to the PSA capital expenditure, with simulation methods applied.

Chapter 6 presenting the theoretical approach and research methodology which would be utilised by the researcher while conducting this study.

Chapter 7includes work on the PSA costs of investment WLCC systems, with simulation. Also, analyzes the most important questions related to the influence and impact of the costs into different life cycles phases.

Chapter 8applied the factor analysis and data reduction process for the number of risk factors in order to handle the task more efficient. Moreover, the presenceof whether risk factors data fit a specified probability distribution using Goodness-of-fit methodology. Using the software “Easy-fit”.

Chapter 9 describes the evolution of the final WLCC model, using Monte Carlo simulation and “@Risk“program

Chapter 10 explains and comments on the findings and other results of the thesis and supports it inthe discussion.

Chapter 11 the thesis is summary, its contributions to the knowledge and society, and suggestions are done for similar further researches.

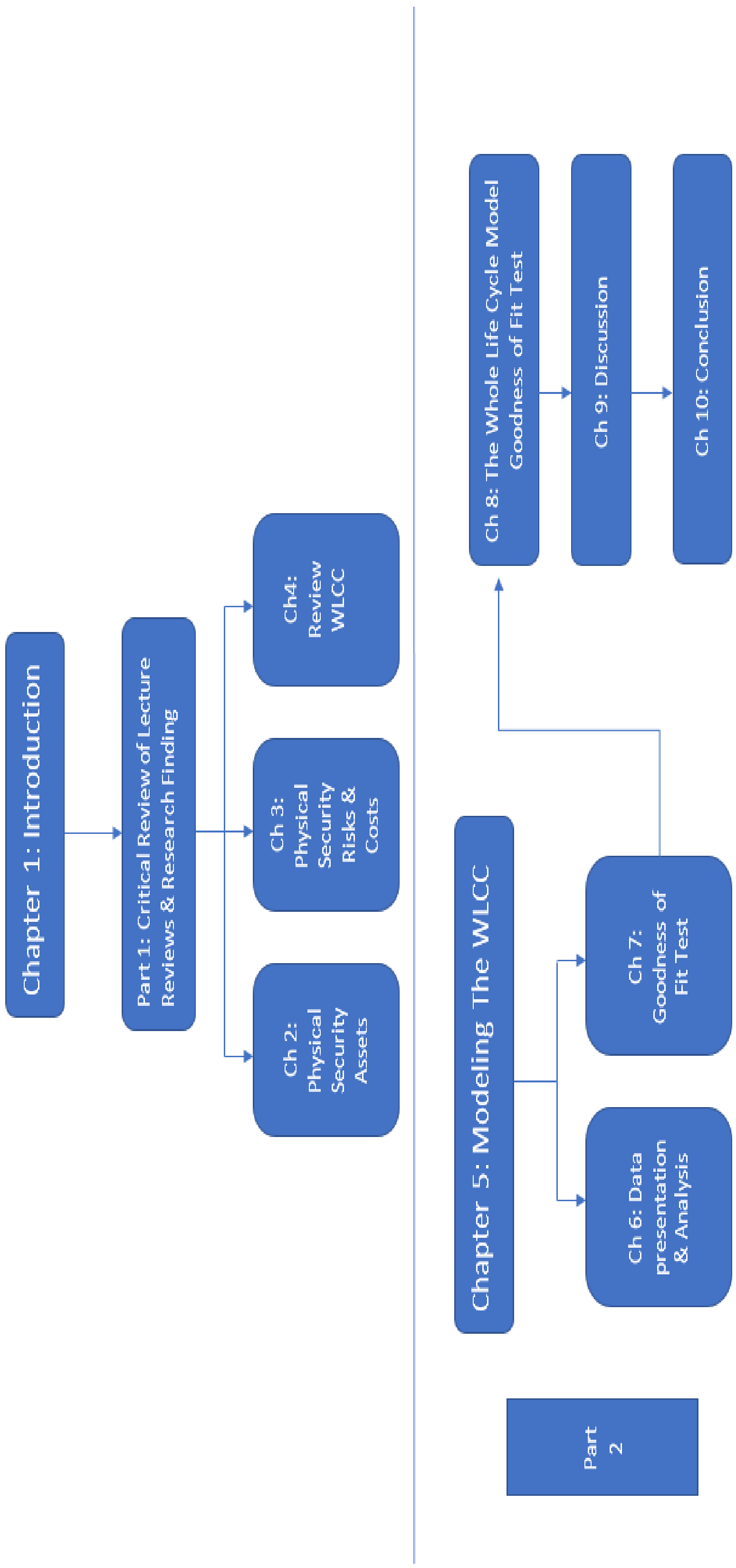


Figure 1-2: Thesis layout

CHAPTER 2. PHYSICAL SECURITY ASSET

2.1 Introduction

The aim of physical security resources can be considered to be to deflect or recognize an assault by a threatening adversary. Suggested is the idea that there exist only a few resources inside an association which must be shielded from assaults or undermining activities. These benefits may be identified with human, material, an office, an area, or a mix of all. In spite of its structure, these advantages have some worth to an individual or an organization, which may pick a mechanism of protection for ensuring it. As stated by USDHSISC, (2009), such a framework can be taken as a course of action of various types of wellbeing safeguards. Such security methods are assets that might have the capacity to distinguish, delay, or react towards an undermining circumstance. As pointed out by ISC, (2015), the decision of a physical security framework, along these lines, has costs concerning wellbeing measures or precautionary measures, which contains the framework both in the acquirement and operations of the guards. For picking the dangers associated with an option determination, an individual or an organization submits its assets comparable to the present estimation of these costs (USDHSISC, 2009). Henceforth, in this segment of the investigation, the specialist will lead an inside and outan examination of the idea of physical security, alongside that the scientist will likewise break down various sorts of ways which are being used by the associations with the point of ensuring their resources. Moreover, in this section, the researcher will likewise lead a top to bottom examination of the diverse sorts of physical security resources, and the lifecycle of these resources, which are being used by various associations. A short time later the scientist will exhibit a diagram of the outline and advancement of the physical security resources, and all the more vitally the establishment, and the functioning of physical security resources, that forms a basic segment for these associations.

2.2 Physical Security

Such systemic frameworks exist to safeguard the buildings to mitigate the risks of damage. To accomplish this, as Oriyano, (2014) contended, the leaders involved must focus on chiefs and leaders must concentrate on thedevelopment of the structures, crisis frameworks, directions in regards to arrangement and utilization of gear, control supplies, treatment of items, and relations with outside offices and contractual workers. Kairab (2005) trusts that an individual or a company looking for assurance for its advantages has restricted money related assets and, in this way, constrained choices of wellbeing methods wherefrom to formulate a security framework. For determining the methods that should be used, the type of the attacks on the benefits to the owners must be assessed. Ekelhart, Fenz, Klemen, and Weippl, (2006) expect the quantity of characterizations of undermining circumstance against a particular owner or an enterprise's advantages is restricted. On the off chance that a debilitating circumstance incorporates an individual traveling through an office, a movement sensor might be an achievable wellbeing measure to be consolidated into a security framework. Influencing utilization of a hazard evaluation to approach, undermining circumstances must be, in any event, considered concerning their likelihood and outcomes (Schumacher et al. 2013). On the off chance that the security measure is of considerable esteem, devastation or harm of the well-being measure must be fused into the resulting appraisal. Keeping in mind the end goal to figure out which wellbeing measures to consolidate, the outcome of the possible undermining circumstances is very basic (Proctor, Byrnes, Barber, and Moss, 2002).

Harris, (2013) asserted the ID of security methods for combating the debilitating circumstances against resources is done; an outline of the wellbeing methods must be charted out. A plan fuses quantity of particular wellbeing measures picked and furthermore the territory wherefrom they enmesh and, if pertinent, the situation of each security measure. For example, Stewart, Chapple, and Gibson, (2012) consider that a couple of is of view that two surveillance cameras can be had introduced ina similar zone with different headings covered.

Along these lines, a physical security framework includes an assortment of wellbeing measures and furthermore their plan and arrangement. In any case, unique option security frameworks might be utilized through different outlines and situation of a similar wellbeing step (Harris, 2013).

As propounded by Olenwa (2014), entry to the building must be restricted suitably in order to appropriately use the apparatus. The outward appearance of protection and security need not be there necessarily.

Boudriga, (2009) showed that the outlines for protection of a facility can be done without over the weight the workers. All things considered, on the off chance that workers require getting to, they will make them give, and they comprehend and keep up the security rules and strategies of the association. Wailgum, (2005) asserts that a valid Security

Agreement has to be provided by the individual before being granted access. This is needed for exemptions too. A portion of the cases of physical dangers to an association are:

- Natural disasters, for example, tremors, surges, and tornados.
- Other natural conditions, for example, high stickiness, outrageous temperatures, lightning, and overwhelming downpours (Stewart, Chapple, and Gibson, 2012).
- Purposeful harm, for example, vandalism, burglary, and burning.
- Not think demonstrations of harm, for example, terrible pipes, over-burden electrical outlets, and spilled fluids (Stewart, Chapple, and Gibson, 2012).

2.3 *Physical Security Countermeasures*

Irwin (2014) states that the measures to provide for security can come in different shapes and sizes. Retail associations can have access to such different combinations. Given the motivation behind keeping up this exertion, the countermeasures that are unrealistic to be useful in retail associations are not depicted in this area. As indicated by Abbott, (2002), the hypothesis and routine with regards to physical security frameworks join the undertakings of discouraging, location, postponing, and reacting. Physical security incorporates the thought of security inside and out, the usage of different layers of between dependent frameworks, for instance, physical blocks, lighting, CCTV observation, get to control, IDS, security gatekeepers, et cetera. Solid, (2012) guaranteed that these strategies of physical security are proposed for identification, deflecting, postponing as well as denying unapproved access to an association's offices, workplaces, assets, and hardware.

In this way, Garcia, (2006) called attention to the stance that when retail associations are being provided for, the most suitable physical security measures must be evaluated. Design of such systems is paramount for methods for hazard administration, use the capabilities of physical security advancements, arranging security tries and offering data to different partners. Similarly, the group tasked with theadministration of security must test the working of the framework, distribute assets concerning the association's main goal, and deliberately supervise human asset and planning regarding physical security framework. As Ekelhart, Fenz, Klemen, and Weippl, (2006) clarified, administration of physical security resources is a total method which fuses vital arranging, recognizable proof of goals, and furthermore legitimization and utilization of a practical planning anticipate a total physical security framework. Kairab (2005), puts forward the notion that a Director of Security with overarching role and duties can be assigned to maintain the security measures and the capacities connected therein. They must have the authority to make decisions regarding the design and implementation of the same, according to the necessities of the organization (Schumacher et al. 2013).

As indicated by Proctor, Byrnes, Barber, and Moss, (2002), as a suitable practice to ensure attractive level of security for associations, the administration should altogether gauge the upside of each perceived physical security countermeasure for their office/structures considering a thorough security chance appraisal and circulate assets according to their best utilization. In any case, Alshboul, (2010) fought that the appropriation of assets for physical security countermeasures, for the most part, includes spending constraints and distinctive complexities. For the most part, there are issues in aportion of physical security assets as for associations, their strategies, and devices that obstruct the design of association's consumption for buttressing the measures of security. Stewart, Chapple, and Gibson, (2012) suggest that the Director must evaluate fully the methodology as being suitable or not for the organization. This evaluation should then result in a report of ideas regarding the enhancement needed for the measures. IT should align well with the goals and objectives of the organization. According to Oriyano, (2014)

There cannot be a uniform best fitting practice for all circumstances and situations. Worldwide guidelines need to be met at times, and according to Boudriga, 2009), in the case of a wide-ranging retail association network, interconnectedness imperatives must be factored in.

2.4 *Type of Physical Security Assets*

Per Olenewa (2014), the push for security measures of PSA is insurance and other administrative factors. Border measures, fencing, monitoring through specialized controls are segments thereof. Wailgum, (2005) showed how stopping, verifying and delaying are also steps in the process. Attempts to attack and vandalize, to go through the assets rummaging them, must be stopped in its tracks through using entryways, and protection around the building edge. Foreswearing can also help through bolted doors and vaults. Irwin, (2014) found that systems for detecting intrusion are second in line of defense and can prepare the staff. According to Abbott, (2002), another layer of security can be included to prevent intrusion until the point where the staff arrives.

2.4.1 Physical Control

Irwin (2014), showed that structures do need checking of individuals before they enter the premises. Three different and varied measures here include private access, confined access or community. Each of the three would have their own reason for attempting entry and thus this must be factored in. Various systems and advances exist that permits controlling access benefits in an office/building. These advances are introduced for debilitating and recognizing passage from unapproved individuals (Hardy, 2012).

2.4.1.1 Perimeter Security

Entryways, mantraps, wall, and gates are generally utilized alternatives for outside security of the workplace or working to build up an extra security layer for the interloper before getting to the building (Mo et al. 2012). Schumacher et al. (2013) guaranteed that wall is utilized for plainly characterizing limits of the workplace or assembling and recognize open regions and secured office building. Materials utilized for making wall contrast in quality and quality. Ensured resources of an organization determine the protection levels. Per Kairab (2005), some fencing would be there, solid wall, laser systems for recognizing intrusion, and wall with electronic impulse. Proctor, Byrnes, Barber, and Moss, (2002), assert that doors are focal entry points and must have robust security similar to the ones seen on the walls. Doors have to be strongly protected as in case of emergency too when triggered, they can provide the route for easier entry or exit if not protected well. Johnston and Garcia, (2002) here assert that the entryway should contain solidified turns, locking segments, and shutting instruments. There ought to be a predetermined number of doors for a working with a specific end goal to solidify the assets needed for protecting them. IF security watches are not present, then CCTV should be there (Johnston and Garcia, 2002).

In case the gates are not easily discernible as compared to the walls, the level of security is enhanced. Entryways provide a singular course to the entrance and thus an individual can enter or exit the facility from it (Harris, 2013). If the mantraps are outlined, then it does not allow multiple individuals to gain access at a time, per Stewart, Chapple, and Gibson, (2012. Hence, until the identity of the person wishing to enter is ascertained, the mantraps provide the waiting space and confine them there. The entryway can give access once the authorization for entrance is obtained, per Mo et al. (2012). Hence this is a mechanism that delays the entrance phase and provides another check therewith.

- **Badges**

IT is essential to identify whether someone looking for entry into the premises is a guest or a worker, according to Boudriga, (2009). Cards can be termed as IDs, and other proof cards, to verify and validate identification process. PC chips attached therein provide a better access process. The RFID labels, data of workers and strips on these can provide security staff a better model.

- **Motion Detectors**

Olenewa, (2014), movement locators offer different cutting edge options in light of the organization's security needs. Movement finders are introduced for thelocation of interruption inside an organization and the gadgets perform alongside essential caution frameworks. Infrared movement indicators screen infrared light changes in the environment (Hardy, 2012). Warmth based movement finders screen modifications in warm levels of the environment. Abbott, (2002) battled that wave design movement finders utilize the frequencies that track any changes in the landscape. The offices that are not so well-lit can adopt the capacitance movement frequency tracker, per Wailgam (2005). Microwaveor ultrasonic frequencies that watch changes in reflection designs in the environment. Capacitance movement indicators watch changes in attractive or electrical fields in the environment. Wailgum, (2005) clarified that photograph electric movement locators screen changes in light and are introduced in offices that have almost no to definitely no light. Detached sound movement locators work by tuning in to abnormal sounds in the environment (Olenewa, 2014).

- **Intrusion Alarms**

Interruption alerts triggers and shows different locators and sensors. Such gadgets incorporate glass break locators, window and entryway contacts, water sensors, and movement finders and so forth (USDHSISC, 2009). Little changes in nature trigger the caution gadgets. In hardwired security frameworks, interruption alerts sense the adjustments in condition by gadgets by producing a wiring short (Hardy, 2012). Various types of interruption alerts are repellent, obstruction, and notice (Hardy, 2012). As indicated by USDHSISC, (2009), anti-agents alerts utilize brilliant lights and boisterous clamor or other loud sounds of alarm can force the intruder to leave. Hereby, hindrance alerts will deter the intruder by providing a wall between different zones, and operate the locks when needed. These alerts can be heard or quieted relying upon the expectation of the association to get the interloper or not drive them away.

2.4.1.2 Technical Control

The guideline accentuation of specialized controls is built mainly around access as that is the critical security point (Harris, 2013). The use of keen cards for access control is one of the mainly used safety measures per Caputo (2014). PCs and other systems must utilize the use of keen cards to enhance security. Multiple measured approaches should be deployed to keep the aggressors away from the facilities. One way towards this is the use of Interruption location systems. They pick up any intrusion in the building (Ballad, Ballad and Banks, 2011). Alach, (2007) then expounds that alertness and readiness to such episodes helpto manage the situation. There should be regular checks of all access logs, in order to keep track of attempts to intrude. (Ballad, Ballad and Banks, 2011).

- **Smart Cards**

The smart card is utilized as a part of situations when it is critical to check the proprietor (Ballad, Ballad and Banks, 2011). These cards have been in use since the 1970s. Types include chips cards and memory cards. Access control is enhanced through the use of chip cards. Keen cards, on the other hand, simply have the facility of providing the card to be checked after the PIN code has been punched in (Fay, 2007). As Kingsley-Hefty, (2013). The main element of the chip card is the ROM. This is made just once and another part is the EEPROM (electrically erasable programmable perused just memory). EEPROM keeps card information that has been hindered by PIN. Irregular access memory is used by the processor to carry out relative features. When the power is switched off, it vanishes. CPU is the crux of the card (Ricks, Ricks and Dingle, 2015). 8-bit microchips consisting of CISC design are used generally therein. They are more expensive than the memory cards (Ricks, Ricks and Dingle, 2015).

There are two variants of the smartcard – contactless and contact ones. Radio flogs prepare the contactless one whereas the contact card has to be featured with a pursuer (Şchiopu and Costea, 2015). Some cards mesh both approaches. Contact can be triggered through sliding or through pushing a weight. A limitation of contact cards is that they have limited life after which the contacts become inoperative. Circuits can be damaged by inaccurate contacts thereby giving rise to harmful electrostatic waves (Norman, 2012). Then again, contactless cards don't require theadditionof a pursuer. They should just be passed close to a radio wire to play out the operation. The perusing separation extends from 2 cm to 50 cm. The contactless cards are higher in price and generally last longer (Norman, 2012).

- **Smart Card Vulnerabilities**

According to Biringer, Matalucci,and O'Connor, (2007), aggressive intruders potentially want to gain access and steal information and other resources which they can then trade off. Interlopers attempt to sidestep the vulnerabilities of shrewd cards by various means, for example, programming assaults, side-channel assaults, blame age and small-scale examining. Johnston and Garcia, (2002) talked about that product assaults and side-channel assaults are seen as non-obtrusive sorts of assaults. Gadgets can include microchips with a code for programming. Be that as it may, this product isn't dependable since its vulnerabilities can be bargained. As Alshboul, (2010) nitty gritty, programming assaults include utilizing summons and codes to hack into the framework and charges that enables the interloper to extricate significant information. Ditty, Ballad,and Banks, (2011) showed that the assailants could harm the physical and data resources of the organization and wrongfully utilize them for their favorable position utilizing the defective shrewd card. These are not that recognizable as the hardware used for them resembles a routine gadget (Johnston and Garcia, 2002).

Data is uncovered regarding the use of shrewd cards without tearing it, according to Caputo (2014). It is a harder to track. The criminal gathers information about the keen cards through planning examination, electromagnetic investigation, and differential power investigation. As indicated by Kingsley-Hefty, (2013), timing investigation affirms the duration it takes for the process to complete. Frequencies can be tracked through the use of electromagnetic investigations. The handling power can be assessed through the use of differential examination. However, according to Fay (2011), a drawback is that the criminals can use this to get the data on the brilliant cards.

- **Proximity Readers and RFID**

Encryption of the cards can be gauged through blame age. The aim of the exercise this is to get to the encryption scratch in order to access the information on the cards. The clock rate is changed and thus blunders are put into the system. The temperature can also be modulated and also the voltage is tempered with (Harris, 2013). Kingsley-Hefty, (2013) asserts that a minor testing can be a more damaging attack on the organization as it includes interfacing to gain access to the microchip that is connected to the communications with other parts. The aim of this examination is to remove the microchip (Fay, 2011).

Small-scale testing can be utilized for removing the layer on the savvy cards through vibrations that are ultrasonic. A passivation layer is then emptied through EEPROM chips using a couple of needles (Fay, 2011). According to Harris, (2013), pursuers are used asa connection to access control systems for card checks and to validate authorization for entry. RFID sends the approvals stored in the microchip through using transmitter (Kairab, 2005).

- **Intrusion Detection, Guards, and CCTV**

The entry controls cards that have inactive labels can be used in a physical access control mechanism per Garcia, (2006). The closeness pursuers can control aloof labels through tapping into an electromagnetic field created by the pursuer. The swiped card transmits a flag that then gets affirmed (Harris, 2013).

Per Ekelhart, Fenz, Klemen, and Weippl, (2006), dynamic labels contain batteries to self-control the radio recurrence distinguishing proof (RFID) chip. Dynamic labels utilize an in-manufactured battery control source that aides in transmitting signals at more separation than uninvolved labels. However, the cost of dynamic labels is extensively higher with restricted life expectancy because of constrained battery life (Schumacher et al. 2013). Dynamic labels are ordinarily utilized for following high-esteem business resources. Pursuers can be utilized for following developments of the advantages and finding them when appended with the location frameworks and the system. On the off chance that the advantages of a venture are expelled from particular areas, the organization can have the alert activated through an entrance control framework (Schumacher et al. 2013). Mo et al. (2012), on the off chance that the physical resources of an association are moved or moved without approval, the interruption location frameworks (IDSs) can recognize and caution the people on call in regards to the of illicit passages. Interruption identification frameworks are indispensable for physical security of organization's benefits because in case an episode occurs or if there is any attempt to gain access that is irregular, the IDS will transmit a notice (Garcia, 2006).

Similarly, the security monitors take on a huge role in identifying interruption set-ups as they are more flexible and cover a larger ambit than automated frameworks, per Hardy, (2012). The guards can be located nearby or can be on patrol as scheduled. They must check during their patrol that entryways, doors,and windows are duly bolted and that the vaults too are secure (Oriyano, 2014).

The gatekeepers can be in command of looking at CCTV and IDSs and can respond when needed. The nearby police service can be used for catching someone attempting to gatecrash (Oriyano, 2014). According to Wailgum, (2005), CCTV or similar type frameworks of camera systems provide visual security, and there must be enough lighting in the area to make the exercise more effective. Inadequate lighting may render it impractical or impossible to indict the gatecrashers as images would be not of the right quality. Wailgum, (2005) considers that cameras can be the main points, and be customizable. As the end goal to screen a stationary protest or individual, it is important to utilize the correct sort of settled focal point in light of the width and separation that is being observed. Settled focal points can restrict, wide or wide-calculated (Oriyano, 2014).

Zoom focal point; then again, are prescribed when observing a point that requires abroader view, per (Stewart, Chapple, and Gibson, 2012). A type of such sort is tilt and PTZ camera. Another camera sort is container, tilt, zoom (PTZ) camera. These camera sorts are arch moulded that can move toward each path alongside the alternative of zooming in or out. As contended by Harris, (2013), PTZ cameras are suitable to track interlopers since the camera consequently faculties and takes after the gatecrasher. PTZ cameras can naturally track thedevelopment of items through mechanical or application methods. Harris, (2013) portrayed that cameras that work utilizing programming applications can change targets and screen out pictures that are stationary, subsequently sparing the capacity limit and data transmission. Johnston and Garcia, (2002) determined, computerized video recorders (DVRs) are additionally used for supporting cameras. DVRs are utilized for thecapacity of information assembled from the camera and can be replayed for identifying interruption or for prove. As per Alshboul, (2010), advanced video recorders likewise incorporate programming applications that license manual dish, tilt, zoom control. DVRs likewise have an in-constructed multiplexor, which can be utilized for at the same time recording encourages from numerous cameras and which can relay video films through different modes including IP and persuade. Per Proctor, Byrnes, Barber, and Moss, (2002), there are systems available that give the facility of additional storage or remote survey. IP cameras could be used for linking the PC recorder frameworks that are linked to host PCs. Schumacher et al. (2013) assert that it provides a solution since IP cameras need a higher stockpiling limit due to the need for better quality.

- **Auditing Physical Access**

Review trails and the entrance logs have to be paid special attention to determine the timing and attempts of false access or an attempt to enter a prohibited or unauthorized zone, as Ekelhart, Fenz, Klemen, and Weippl, (2006) expound. The location could be ascertained but the prediction element won't be there. The evaluating programming and instruments are utilized just for the location and not for anticipation. As indicated by Mo et al. (2012), solid checking of access logs and review trails are vital for quick activities. The examining framework isn't important if the organization can't react to the circumstance or if the reaction time is restricted. Administration of the organization must comprehend when the episodes happen with a specific end goal to settle on fitting security choices for ensuring the physical resources of the organization (USDHSISC, 2009).

Assets may need to be expanded further in order to protect more the particular assets in a particular situation. The logs and trail should outline fully when the abortive unauthorized access attempts were made including the time and the exact location (ISC, 2015).

2.5 *Physical Security Asset Life Cycle*

As expressed by Woodward, (1997), undertaking resource life cycle could basically be clarified as the procedure of the ideal administration of the physical resources controlled by an association with a specific end goal to limit the negative natural effect, and decrease of utilization of vitality, which thus brings about the boost of significant worth for the association. Henceforth, Gomes and Michael ides, (2005) asserted that in this setting the concentration of the organization is over the generation operations, however different procedures and arrangements could straightforward be executed for successful administration of the physical resources inside an association. Besides, Levin, (1998) contended that it additionally covers different angles which incorporate outlining of the plants, planning, and arranging of the undertakings, controlling activities and the like.

An important part of the utility of the lifecycle administration is how the structure is transferred when it is the pre-outline, according to Levin, (1998). With the venture advancing for the duration of its life cycle the data identified with the financial plan of the task, alongside acquiring data is gathered later on. Zhang and Wei, (2008) battled that to keep data administration more productive the potential providers are made a request to transfer the data according to the prerequisites for the improvement of the undertaking structure.

Henceforth, Gomes and Michaelides, (2005) battled that this aide in beating a major issue for the association which compelling administration of various resources and it empowers the associations to determine this issue in an effective way through lessening the administration workload, which has a noteworthy effect over the undertaking primary concern. As Levin, (1998) contended, each benefit has a lifecycle, and successful resource administration should be possible at any snapshot of time in which the advantage increases the value of the task.

Woodward, (1997) indicated that every benefit takes after particular cycle. An important element is to appreciate at which stage of the lifecycle does a resource exist and what advantage it is giving. Per Zhang and Wei, (2008), when this is known, spending plans can be put into place and changes can be made if needed. Generally, there are 4 phases - planning stage, improvement stage, and establishment stage in addition to operation stage.

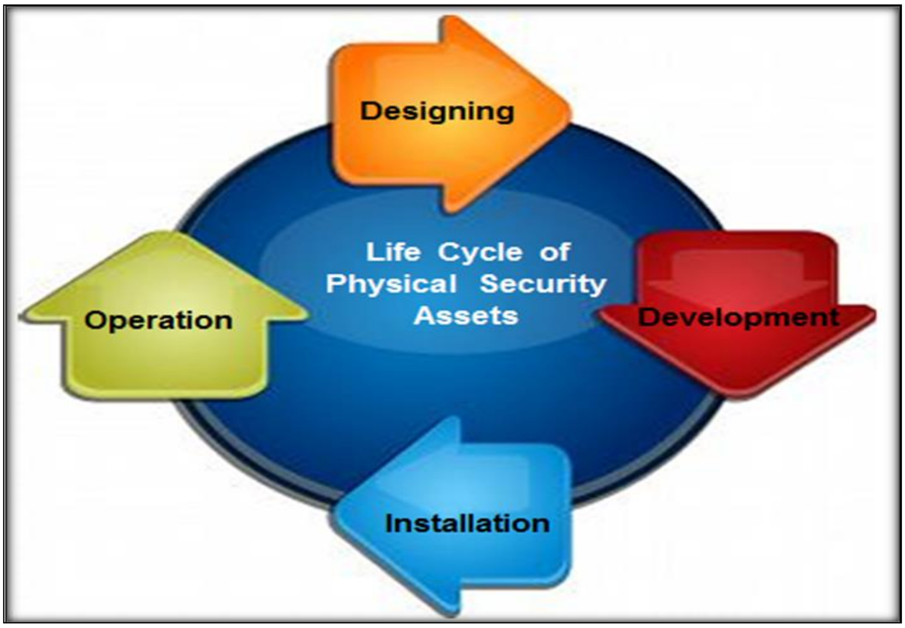


Figure 2-1: Physical Security Asset Life Cycle

2.5.1 Design of Asset

There is an iterative process involved for the period of planning where we have the outline, preparatory plan, and ends with the security framework outline for the clients. Per Fennelly (2013), it provides for the best arrangement and must include various dimensions of the security frameworks into account as follows.

- Development of Assets

Next stage is the advancement of buy or benefits. Per Zhang and Wei, (2008), the organization needs to pick whether the advantage will be acquired or created. Next, the financial plan for improvement or buy of benefits alongside the calendar for advancement or securing is set up. An organization gets a benefit, and it turns out to be a piece of the advantage administration arrangement of that organization. Basically, Levin, (1998) depicted that once the buy request of an advantage is finished and the affirmation is gotten from the provider, the obtainment arrangement of the organization educates the benefits administration arrangement of the organization. Fitting use of these exercises guarantees that the advantage is fit for utilization.

- Installation of Assets

The new plan of the physical security resources must be actualized in view of the required details, for example, the establishment determinations on CCTV systems by Abu Dhabi Police Buildings Guidelines (2015). Per Fennelly (2013), specialists must affirm any changes who are well aware of the consequences and the interconnected impacts. Some of the changes can be rather simple, but some may contrarily influence framework execution. For example, when the separation between light apparatuses is modified, the measure of the accessible light on a range will likewise change. Operational, useful and execution tests must be performed on recently introduced security frameworks keeping in mind the end goal to guarantee it's operating per the need. Security resources should be filling in obviously. At last, execution tests are attempted to guarantee that the security resources can address client issue and desire. The test outcomes are utilized to legitimize or withhold last instalments to merchants, contingent upon whether the framework breezes through the tests (Fennelly, 2013).

- Operation of Assets

Testing of the segments and framework all in all; and their legitimate upkeep are required (Fennelly, 2013).

- Site and Facility Consideration

Kairab, (2005), all destinations and offices for the physical security frameworks must have mechanized controls for ensuring the important physical resources of the organization. The essential line of resistance must be physical and specialized controls that were examined above; though, representatives of an organization are considered as the last line of safeguard.

Schumacher et al. (2013) expressed that controlling human collaboration with the gatecrashers decreases the risk of harm or damage. The physical and specialized controls are key for application and support of physical security to not just ensure the significant physical resources of the organization yet, in addition, the people, operations, and data innovation framework. Per Mo et al. (2012), the controls must provide for stopping in the tracks the gatecrashers, and the controls might be adapted. Every venture has its own need per Ekelhart, Fenz, Klemen, and Weippl (2006), considering the administration mode, the number and estimation of resources for are ensured, obligations ofthe security group, and different variables.

2.6 *Facility Plan*

Proctor, Byrnes, Barber, and Moss, (2002), while planning and advancement of physical security frameworks, the organization can utilize basic way examination, which is a precise technique for recognizing the connections between the organization's operations, procedures, and applications. The basic way investigation is the essential phase of securing both the physical and data innovation framework of an undertaking. Alshboul, (2010) demonstrated that these frameworks incorporate structures, hardware, servers, PCs, organizing gear, power and water structures, and atmosphere control. Alach, (2007), using existing and future mechanical advancements, for instance, cell phones or working frameworks in the meantime are vital. Existing mechanical developments help in enhancing, and new advancements rise as advances turn out to be better. Subsequently, it is important to arrange for how the new framework will integrate with the existing set-up. This is because the new capacity work may introduce harm into the existing system inadvertently. In a retail set-up, parallel running and working with a specific end goal to stay away from security dangers and fiasco, per Ballad and Banks, (2011). Fennelly, (2013) determined that one outline of the physical security frameworks is the interruption alert framework, CCTV reconnaissance, and fire caution framework utilizing a similar framework inside the association. Fay, (2011) brought up that one framework that associates diverse alert frameworks can bring about security issues as a gatecrasher can bargain the framework once and every one of these controls can quit working. Subsequently, Kingsley-Hefty, (2013) called attention to that having separate frameworks for to each physical and specialized control would lessen the risk of all frameworks flopping in the meantime. Fay, (2011), all people related with the organization and the security group including the representatives, administration, and especially wellbeing and security constraint, must add to the site arranging and outlining of the physical security framework. Administration of the organization must be engaged with the site arranging procedure to guarantee assets are open for the security framework venture. Ricks, Ricks, and Dingle, (2015) clarified that wellbeing and security worries of workers must be tended to while building up the office designs. Wellbeing and security workforce can feature the critical parts of the physical security framework.

2.7 *Site Location*

The zone, costs, and scale are the segments that involve for arranging when getting a site for constructing the framework, per Norman (2007). Security concerns and angles should be given consideration for the foundation. Şchiopu and Costea, (2015) asserted that this should be the case even when a new facility is being considered. Caputo (2014), discusses the responsiveness element in detail and calls attention towards considering the various harms and intentions of the gatecrashers when constructing the facility. Choice of territory must include these dimensions, for example, what is the state of the earth around the new set-up, the neighbourhood, both physical and the stakeholders, the local population etc. (Fennelly, 2013). Openness is another element. Kingsley-Hefty, (2013) showed howthe street approach, separation of air terminals, roads and stations can be critical. Song, Ballad, and Banks, (2011) assert that such locations that are prone to natural disasters may not be suitable options. Staff administration and wellbeing are also critical, per Biringer, Matalucci,and O'Connor, (2007). Taking care of cataclysmic events in the event that they choose to choose the site in a fiasco inclined territories. Fiasco recuperation designs must be a piece of the hierarchical systems, which ought to include the measures to handle the disaster per Alach, (2007).

2.8 *Facility Design*

Security parts must be investigated before the plans for the development of facility are put into place. Crisis departure, passage, and exit are to be included per Johnston and Garcia, (2002), and also unapproved section, caution use and conductivity. As Alshboul, (2010) point by point, the materials and strategies for development used to assemble the office must conform to the building principles and security measures. Delegate, Byrnes, Barber, and Moss, (2002) is of view that divider and roof configuration needs to agree to least fire appraisals vital in different areas. The sort of combustible material used in development and support for security necessities, for instance, insurance of server rooms or locales that have significant physical resources must beconsistent with the set principles. As Schumacher et al. (2013) expressed, the comparable principals of configuration are material for entryways and windows of the office. The outlining and improvement of physical security framework must consider the entryway and window plans, how entryways and windows persevere through theconstrained passageway, will entryways and windows be checked by the identification framework, solidness of turn, opening heading of entryways and windows, bolts and glass required. In addition, Mo et al. (2012) battled that the outline of flame identification and concealment framework must survey the sort of flame pointers, sensors,and their arrangement, stockpiling of flame concealment gear amid the testing stage, and the sort of fluids for concealment.

2.9 *Securing Data*

Per Kairab, (2005), the server rooms and vaults, and also zones where information is stockpiled must be secured well. These rooms containing imperative physical resources and data innovation resources have to be secured and access is given only to concerned and relevant specialists (Hardy, 2012). As much as access is limited, there is alesser danger of attacks to the organization’s innovation resources per Irwin, (2014). Oxygen dislodging sensors and chilly temperatures, added with low lighting and tight spaces help in securing (Hardy, 2012). These critical zones, as they contain invaluable information should not be situated on the ground, top floor, or the cellars per Wailgum, (2005).

2.10 *Product life-cycle management (PLM) of Physical Security Asset*

PLM is the assortment and combination of methods through which different utilitarian stages are crossed. The CCTV condition when sold must be taken into account and overseen suitably all through its lifetime. Stark, (2015) expressed that a guarantee could essentially be viewed as an announcement which is given by the merchant of the producer of the item that the item will perform in a predefined way for a particular timeframe. Notwithstanding, in light of the current situation where the item or the administration neglects to execute according to the guarantee, at that point all things considered the guarantee is affected. Individuals in the procurement department would be relevant here to manage this. Be that as it may, with regards to the transfer of the security hardware is has been encouraged to first counsel with the obtainment office of the organization. Portage et.al, (2013) expressed that the preventive support should dependably be considered as a schedules mind planned with the point of turning away the repairs which could end up being profoundly exorbitant. Be that as it may, through directing consistent assessments, and arrangement of preventive upkeep to the security frameworks and equipment's, a security supervisor may be equipped for evading and genuine security issues which may emerge because of the over-utilized or ignoring of a specific gadget. In this manner, this is the motivation behind why different associations consider preventive upkeep a basic part of looking after the security hardware and also the security frameworks. This is a training which is for the most part seen by the authoritative as exceptionally prudent, sound, and all the more critically savvy. Moreover, the confirmation of the normal upkeep could likewise improve the life-cycle and as a rule the execution of the items. In any case, amongst other elements, the critical matters to consider are interruption identification frameworks, CCTVs, magnetometers, and the vehicles hindrances.

2.11 *Design and Development of Physical Security Assets*

Per Oriyano, (2014), with a specific end goal to accomplish the ideal level of insurance, profitable resources of an association are arranged by significance in the security class. The grouping foundation is generally utilized. Corporate vision must embed the feature of security. According to Stewart, Chapple, and Gibson, (2012), the frameworks are there for a reason, which is to protect from and then to limit the damage. This implies the physical security frameworks have just a single fundamental prerequisite i.e. they might be powerful concerning its assignments (Wailgum, 2005). Besides, Irwin, (2014) fought that physical security frameworks ought to be assessed in view of their effectiveness and strategic execution to counter real dangers,the vital effect on the lessening of big business related dangers, and adjusted monetary execution of the framework. Along these lines, as per Abbott, (2002), areas of improvement must be outlined fully, with the usage instructions and training for the frameworks concerned and the systems to guarantee proficiency. Something else, the attainability of setting up a particular physical security framework can't be impartially legitimized (Wailgum, 2005). Solid (2012) is of view that perceiving the requirement for a reasonable way to deal with unravelling security issues, numerous vast mechanical and business endeavours, gatherings and organizations have built up their own particular physical security frameworks alongside the help of specific security associations. Making a vigorous endeavour security framework is resolved to take the correct choices in view of the examination of potential dangers to the security of the profitable resources, and a reasonable evaluation of conceivable outcomes for a successful arrangement of assurance considering the current choice and capacities (USDHSISC, 2009; ISC, 2015). Right now, it is difficult to envision the security of advantages of the venture that performs work utilizing classified data without the coordinated utilization of present-day specialized hardware and frameworks (USDHSISC, 2009; ISC, 2015). The most proficient way forward is building through the pre outline arrangement (USDHSISC, 2009; ISC, 2015). Following processes would help to consolidate the framework further.

2.12 *Installation of Physical Security Assets*

PSA's new outline should be executed in view of the required determinations of the organization and in addition the models set by the administrative experts, per Boudriga, (2009). Be that as it may, the general procedure of establishment of physical security framework includes following essential phases:

Site Survey: Establishment locales of PSA must be assessed. For example, territory saw dangers, kind of fencing, rejection zone, natural impedance, office length must be taken into account according to Harris (2013). Also, the security prioritization of the various office zones needs to be established. Providing for security framework in light of the requirements of office is significant for ensuring the profitable resources of the organization(Stewart, Chapple, and Gibson, 2012).

Property Mapping and Product Choice: Using the data that was accumulated in the site review, the establishment group must guide out the general format of the property and pick the most fitting physical security items for the establishment inside the premises (Ricks, Ricks and Dingle, 2015).

The positioning of the Security Controls: The following stage in establishment procedure of physical security framework is picking the position for introducing the physical and specialized security controls (Kingsley-Hefty, 2013). These security controls incorporate

CCTV observation, mantraps, doors, wall, movement identifiers, interruption cautions, watches, vicinity pursuers and RFID per users and so onwards.

Programming of Security Controls: Next phase is the programming of all the related controls and their coordination to be put into place. Representatives' database is essential with their own ID labels and the parameters for accessing various office ranges. Bypassing this or a weak approach regarding suitable writing computer programs isn't valuable (Norman, 2012).

Testing the Physical Security System:the last phase of the establishment procedure includes testing the physical security framework. It includes checking the framework and directing activities and training to tests the execution of the framework if there should be an occurrence of a fiasco or gatecrasher danger, per Fay (2011). According to Fennelly (2013), all testing needs to be done to ensure that outcomes are according to those planned. Operational tests are required to assess this per Fay (2007). Execution tests would have to be done to ascertain the status per requirements and desires of the undertaking (Fay, 2011).

2.13 *Operation of Physical Security Asset*

According to Interagency Security Committee (2015),, the support and operations of the framework includes making procedures to ensure appropriate usage of physical security resources, executing a reasonable upkeep get ready for physical security resources, deciding the general estimation of the security resources, practical progressing and change of existing security frameworks, directing execution estimation of working frameworks, specialized assets and HR identified with physical security framework and so on.

HR of an association can also validate the forming and quality of the framework(Kingsley-Hefty, 2013). To their needs, the operations of the framework, plus how much usage approaches are taken after or bolstered. Kingsley-Hefty (2013) perceived as basic elements for effective execution and working of the framework, including:

Systems Management: Employees must ensure that all elements of the framework are working, all things considered, to ensure the framework is performing atthe ideal limit and according to the desire (Kingsley-Hefty, 2013).

- Training: Training must empower the employees regarding the steps to be undertaken and the routines per Ballad, Ballad,and Banks, (2011)

- Monitoring: All the gadgetry and elements of the framework must be monitored regularly.
- Response to Alarms: The response and the process to be followed in these cases must be outlined and communicated to the relevant staff per Mo et al, (2012).
- Periodic Testing: All the framework settings and operations must be tested periodically to ensure smooth functioning per Kingsley-Hefty, (2013).

2.14 *Physical Security Assets for High-Value Retailers*

The advantages and disadvantages of the various options available to the high-value retailers in this regard must be considered fully. Starting with savvy cards and ID identifications, they provide a higher level of security, according to Stewart, Chapple, and Gibson (2012). Along these lines, savvy cards and ID identifications convey sealed capacity of data of the cardholders and their record points of interest. However, there issues connected with this. Customers may find it difficult to handle per Bourdiga (2009). Some applications would require changes to recognize the cards, or foundation adjustments will be needed at starting phases for the examination, per Harris (2013. The worker can feel lumbered with accumulation keen cards and ID identifications. For high esteem retailers, vicinity pursuers are ideal as a small microchip is embedded in the card for the data (Abbott, 2002). When someone swipes the card, the closeness pursuer requests the code and later transmits it to the savvy card. When a match is identified, the nearness pursuer allows access, per Abbott (2002). However, if the card is lost or stolen, other individuals with unauthorized access can gain access in case the PIN is not secured (Hardy, 2012).

Another element available is interruption recognition framework and alerts. Its focal points incorporate permeability and guard as the framework and alerts gives aclear perspective of the exercises happening inside the area and provides another layer of security per (Schumacher et al. (2013). Be that as it may, the burden here is that the interruption identification framework and alerts requires a great deal of support as far as the scanners, indicators, and cautions and so on. In addition, interruption location frameworks are renowned for false alerts. The quantity of false positives-sounding alerts can be diminished yet the blame can't be totally dispensed with (Schumacher et al. 2013). Additionally, security monitors are significant for recognition and discouragement of vandals and criminals in high esteem retailer business. Not at all like, are mechanized frameworks, security monitors fit for settling on choices and adjusting their exercises and calendars making it eccentric for the interloper (Ballad, Ballad &Banks, 2011). Be that as it may, the burden here is the cost of procuring security monitors, which is a huge sum paid on amonth to month premise. Then again, CCTV cameras are a standout amongst the most regularly utilized security frameworks in present-day organizations and this has turned into a fundamental piece of retailer organizations, per Caputo (2014).

Here, the cameras would help as they deter illegitimate movement and this can be used to press charges later too against the offenders. As long as the power line is adjacent, they can be deployed with ease. They can be the ones which are difficult to observe, or can be very prominent like ones used on boulevards and structures, per Caputo (2014). An issue here is how staff can complain about the levels of constant monitoring of their movements. Another element is the trespassers may have figured out ways to escape being observed (Caputo, 2014). However, this can be done for all day, every day monitoring to survey what goes on on the premises and can bea major deterrent towards wrongful access (Caputo, 2014).

RFID innovation is also relevant for the high esteem retailers. On the off chance that the association approves this transportation, the security authorities of the organization will think about the illicit action. RFID labels are situated inside high esteem things in the workplace building, and an alert framework is introduced at the leave entryways of the workplace building. In the event that somebody makes an unapproved endeavour to transport the high esteem things far from the workplace constructing, the caution gets activated (Olenewa, 2014). This security framework gives a considerably more grounded security when contrasted with straightforward reconnaissance cameras and scanners as the hoodlum is caught in the act. Nonetheless, RFID innovation ends up being very expensive for some organizations when contrasted with other following and recognizable proof advancements per Norman (2012). However, when metal and fluid surfaces are used, RFID pursuers may not work well because the radio waves can render the labels as garbled (Şchiopu and Costea, 2015).

Hence, the high esteem retailers in Abu Dhabi can deploy a combination of security frameworks through shrewd cards, ID identifications, CCTV, RFID labels to protect and secure their premises.

2.15 *CCTV, Physical Security, and Access Control*

The supervision is centred around the situational context, and for this reason, CPED remains for such counteractive action through utilizing the main plan. It reduces the chance of wrongdoing with using a very modern solid condition based onthe improved impression of criminal hazard. In this manner, these physical barriers genuinely, distinguish, hinder, and all the more critically stop the entrance of the ensured space. Notwithstanding, in an examination led by Ko, Park, and Kim, (2016). It was found that still there was no assurance that the frameworks could fill in as a non-rupture capable barrier framework, as there have been different instances of breaks which have brought up some major issues identified with the security component of this equipment. Therefore, it could be expressed that these frameworks regardless of how complex a progressed are not interloper confirmation, and the physical guard gave by these frameworks are as yet vulnerable. Notwithstanding, then again the abnormal state of security given by the frameworks is a fact, and has saved many from disaster. CCTV is a main element of the security framework, according to Chung (2014), in light especially of the recent innovations.

2.15.1. Shut Circuit Television (CCTV)

Fennelly, (2012) asserted that CCTV is considered a very imposing resource insurance in gadgets for associations, which is the reasons why they have turned into a fundamental segment of various physical security frameworks which are utilized essentially with the point of stopping and recognizing the undesirable section inside the ensured space. CCTV has been essentially effectively the viability of different other physical barriers. Kruegle, (2007) directed an investigation it was found the locks would be more useful inthe situation being what it is the place they are used close by a CCTV set-up.

CCTV's can be more productive if adequately put in the framework, in any case, their effect could additionally be expanded with the point of profiting the best advantage, as they can be used for securing distant territories. With regards to planning of very powerful security frameworks, an organized blend of the staff, methodology, and hardware's have turned into an exceptionally prevalent choice which additionally guarantees the expansion of every last components of the security, while in the meantime it likewise makes a noteworthy commitment to the counteractive action of misfortune, guaranteeing well-being, and through CCTV which is like a human eye. It is thus the main gadget which checks, locates and also providesthe evidence required for security apparatus (Matchett, 2003).

Thus, remote areas can be protected. In this manner, they are not just a very viable and effective mental obstruction which helps the anticipation of a wrongdoing;however, they additionally fill in as the facilitator fit for identifying and catching a suspicious action or a criminal, consequently guaranteeing that the general security cost of the associations lessened. Finish CCTV framework fundamentally involves hardware's, for example, cameras, video recorders, screens, and now and again they likewise incorporate the tilt and dish drives.

2.15.2 Operational Requirement for CCTV reconnaissance

An exceptionally precise arrangement of appraisals of the issues, which are to be settled in a viable way for the CCTV, must be put into place (Malmenbratt, and Brooks, (2015). Hence, the significant point behind the assurance of the operational necessities of the CCTV observation is the protection of a framework which is planned with a reasonable comprehension of the need and motivation behind the particular framework. Nonetheless, in the event that, the association neglects to distinguish a conspicuous need then, all things considered, the administration won't consider it to be a beneficial choice, and it won't be practical. The operational side of CCTV must incorporate main components includingthe concentration of the observation illustration movement, articles, or people. Along, with that CCTV reconnaissance could likewise be utilized with the end goal of checking, and watching the general population inside a territory. Nonetheless, every individual should undertake their part in making the security apparatus of the organization an effective one. This is something which could without much of a stretch be accomplished through setting up a working gathering which is fit for undertaking the entire exercise. Be that as it may, once, the necessities of the end client are caught, the specialized details are considerably less demanding.

However, in another investigation directed (Donald, and Donald, 2015), it was found that end goal to augment the general potential and all the more imperatively the strength of the framework, the general administration of the frameworks, and all the more significantly the running cost must be kept under thought amid the way toward arranging, and additionally the speculation evaluation. Assets, could without much of a stretch be given facility of CCTV, yet the expenses may be too high. Thus, it is needed that the frameworks stay set up, yet in the meantime, it should likewise stay maintainable. Indeed, even though lion's share of the framework possesses a time of guarantee, and in addition, the upkeep expense in future which will also include other elements.

Subsequently, operational training rules must be provided (Chen, Wu, and Hsieh, 2013), in a manual. Training codes for administrators and in addition the supervisors alike should explain a portion of the essential tips which would incorporate the controlling and operations of the camera, information assurance and the security approach, and level of responsibility over various issues, alongside the standards of the supporting operations of the CCTV observation framework, lastly the operation of the entire frameworks. Along these lines, the procedural manual fills in as the perspective for running the direction of the frameworks, while in the meantime it likewise manages the administration of picture quality and the control room dynamics.

2.15.3. Plan and Management of the CCTV control room

It needs extraordinary consideration; else it could bring aboutthe rupture of security. The control room is the hub of security per Beckers (2015). The administration rules, discipline,the commitment of staff, diligence, hardware, are features that make the framework a resounding success.

Only approved staff should gain access, and passageways must be protected (Pikaar et.al, 2016). The left approach should be set up keeping in mind the end goal to guarantee an abnormal state of security. Staff welfare, as well as security imperatives, should mesh in designing and operation of the control room. Effective and reliable staff is chosen for this profoundly essential activity, thus HR must do this task with special care and diligence.

Mitrou, Drogkaris, and Leventakis, (2014) directed an investigation in which they established that individuals have the basic privileges of the security, freedom, and self-rule, in this way, it is fundamental that these CCTV frameworks work inside a lawful system. Verifying the observation helps in keeping away from self-assertive interruption inside the protection of the people (Chung, 2014).

As indicated by the workplace of the Information Commission UK, Data Protection Act 1998 must be complied with in CCTV observation too. So is the case with Human Rights Act 1998 and Regulation of Investigatory Powers Act 2001 and other relevant laws. As the process involves surveillance of activity, it can be considered nosy and unlawful, unless the right protocol and systems are deployed. Also, the information thus gathered must be managed and protected, also used according to the rules afore-stated.

2.16 Physical Security/Information Technology Integration

The failure of some organizations to coordinate and adjust their security apparatus, data innovation venture, alongside different other security frameworks and parts helps the likelihood of the excess of the automatic endeavours. Besides, it additionally makes some real holes, or now and again it could likewise bring about sustaining the current vulnerabilities inside the security build of the association (Peltier, 2016). Moreover, the absence of coordination inside the frameworks could likewise bring about absence proper utilization thereof. Cooperation amongst the staff and proper line of hierarchy and work management is essential thus.

Ringer et.al, (2014) expressed that keeping in mind the end goal to finish an abnormal state of joining, guaranteeing monetary stewardship, legitimate portion of the assets, and the in the meantime guaranteeing the designation and additionally the usage of an exceptionally viable and multi-trains mechanically layered security approach there should be a non-debatable concentration of the physical security programming, alongside that there must a solid feeling of devotion towards planning of the product. Thus, reconciliation of very proper and compelling physical security innovation frameworks could gather and relate the occasions from the current security gadgets, and additionally, the data frameworks which would permit the PSOs to effortlessly recognize and in the meantime settle certain possibly hurtful circumstance in an ace dynamic way (Norman, 2014). Along these lines, it could be expressed that the joining of the physical security data permits various advantages which could be benefited by the associations, for example, administration announcing, security administration, expanded control, and all the more significantly situational mindfulness (Ali, 2014). Henceforth, suitable physical security data innovation coordination inside the association helps in diminishing the general cost for the association through expanding the general proficiency of the associations, while in the meantime it likewise enhances the general hierarchical security with the assistance of expanded knowledge.

A Complete and extensive physical security data programming involves the accompanying six highlights:

- Gathering: A viable physical data security programming is fit for gathering information for various unique security gadgets and in addition frameworks.
- Examination: A viable physical data security programming has the ability to break down the corresponding cautions, information, and the all the more critically the

occasion with the point of distinguishing the connection circumstance and needs them in light of their significance.

- Confirmation: The physical security data programming likewise exhibits the absolute most important data identified with the circumstance in an exceedingly complete and speedy way, which empowers the administrator to check the entire circumstance in an exceptionally powerful and effective way. Physical security data innovation programming presents the important circumstance data in a brisk and understandable arrangement for an administrator to confirm the circumstance.
- Determination: The product frameworks are equipped for giving standard working techniques, which takes a shot at well-ordered guidelines and also factor in the hierarchy and the apparatuses being used.
- Revealing: The measure is equipped for following every one of the means and all the more vitally the data which is required for consistent detailing, preparing, and all the more essentially the way toward leading a top toa bottom investigative examination of the framework.
- Review trail: The physical security data programming is likewise equipped for observing the way in which every administrator cooperates with the frameworks, and tracks down manual changes related with the security frameworks, and also the information, while in the meantime it is additionally fit for the computing the response time for each and every occasion.

2.17 *Summary*

For developing dangers, for example, the illicit activities of people, some measures are essential as identified (Stewart, Chapple, and Gibson, (2012). Proper costing and intention, and formulation of the set-up are essential (Oriyano, 2014). Different dangers (Wailgum, 2005) have to be guarded against, composed of:

- Unauthorized access to advantages, for example, robbery, theft;
- Disciplinary infringement;
- Illegal expulsion of property;
- Emergencies and so on.

Kairab, (2005), inside the system of an association's security arrangement is the physical security of its fundamental auxiliary component, went for the conservation ofthe property, life, and soundness of the workforce and money related assets. Mo et al. (2012) contended that the idea of physical security association gives ID of conceivable dangers to the working of the organization's offices, recognizable proof of the probable culprits of dangers, distinguishing proof of the most defenseless places in the office, i.e., conceivable resources for insurance, helplessness evaluation of the organization's important resources, consistency with existing distinguished security dangers, creating recommendations and completing the essential ways to assure well-being. Specialized arrangements for the insurance of significant resources and assets of the venture from the vindictive dangers and unlawful activities of people. It incorporates security powers and the insurance of the benefits, an arrangement of specialized methods for assurance, and the framework built up in the office and so forth. In any case, Schumacher et al. (2013) trust that physical security framework ought not to meddle with the ordinary working of the association, i.e. creation forms. Along these lines, recent innovations have enhanced the utility of CCTV systems considerably.

The Chapter deals with elaborating on the concept of physical security assets, along withan analysis of the various protective measures that organization may deploy in order to protect the PSA. The control measures inbuilt into the system, withan explanation of their needs, and the physical structures necessary to support the system have been explained. Integrative elements within the PSA are discussed at length. The different categories of PSA are assessed, with evaluation of the related lice cycles of those categories. Due emphasis has also been given to the dimension of maintenance of the assets under the connected lifecycles, asthe achievement of corporate objectives is taken up. The roles played by the various stakeholders in the planning, design, purchase, installation, maintenance, and disposal of the PSA is analyzed in depth. In summation, the researcher has evolved a way forward regarding design and development of a PSA, from planning, installation, and operation of the same.

This thesis discussed the cost of risk of insulting the CCTV equipment which been listed as:

- Camera
- Cables
- Switches
- Software for CCTV

- Monitors
- Storages
- UPS systems
- Accessories
- Multimedia Converter

CHAPTER 3. *PHYSICAL SECURITY EQUIPMENT RISKS AND COSTS*

3.1 Introduction

As the lifecycle of the structures of security has a limited life, the costs and benefits associated must be considered, with a specific end goal to guarantee effective operations. A portion of the dangers and costs which the business may need to look because of old, and debase physical security hardware may be very high, and now and again it could even have a negative effect over the execution of the business. In this way, it is basic that associations consistently screens; repairs, and updates it's obsolete, and out of date physical security resources keeping in mind the end goal to guarantee an abnormal state of security at the plant, or the business office. Physical security resources cost administration incorporates the procedures which are associated with the arranging, estimation, planning, and all the more critically the controlling expenses. This thusly will guarantee that the general resource costs are secured by the endorsed spending plan. Hence, as a minimum:

- Estimated costs: The estimate of expenses and in addition the assets required guaranteeing execution of the physical security resource, must be ascertained.
- Budgeting: Business must total the evaluated costs engaged with the setting, introducing, observing, and discarding the physical security resources, keeping in mind the end goal to build up cost measure.
- Cost Control: Cost controlling is vital as the framework must conform to the budget allocation and the overall financial plan of the enterprise.

  Specialists should be tasked with an inside and out investigation of the dangers, which an association may look regarding its CCTV physical security resources. A portion of the dangers which will be tended to by the analyst in this segment of the examination would incorporate; start cost chance, usage cost dangers, operations and upkeep cost hazard, securing cost chance, lastly the aura cost chance. In this manner, the choices which are taken in regards to the venture and its cost, supporting the item or an administration, or aftereffect of the task have solid ramifications on the physical security resources. Be that as it may, the basic leadership process can be enhanced through the life-cycle costing alongside the esteem designing strategies. Besides, the two specific ideas can additionally lessen the cost and the time required to enhance the measures. A single staff member can undertake a portion of this exercise on his or her own, for limited capacity to focus on time. Nonetheless, these procedures of physical security resource require diverse instruments and strategies. The exact need and the extent of the strength of the measures for a new undertaking must be defined well at the outset (PMI, 2014). Table I depicts an estimation of the costs involved.

The resources have to be evaluated towards their contribution to the overall safety framework. The future cost of the assets, have to be anticipated in view of the encounters, administration, ascertaining the time allotment.

Keeping in mind the end goal to finish the planned exercises in regards to the physical securities, at that point, the action cost gives a quantitative evaluation to the cost, which is related with the specific venture. The type of the specific gauge can either be in point by point arrange or in the outline organize. Moreover, the cost has to be estimated in a holistic manner, with all inter-connectivity and imperatives evaluated and anticipated. CCTV camera cost classifications are given below, as an example:

Table 3-1 Cost stages description

Types of Cost	**The Description**
Initiation Cost	Initiation Costs of the CCTV cameras Purchasing cost: Buying costs of the cameras, now and again it may likewise incorporate the transportation costs, depending on the sorts of agreement marked by the organization. The financing cost: Total monetary cost for buying, set-up etc. of CCTV cameras. Total establishment cost: Costs associated with forming linkages and interfaces as required.
Implementation cost	It incorporates the Installation cost: The basic hardware installation. Licensing Cost: Cost of obtaining and maintaining the permits as required by law. At times, as permitting from a legislative organization to screen the development of an area ofthe place, inside and furthermore outside the workplace premises. Service Cost: Adjusting costs, subsequently, this is a cost, which is brought about by an organization on month-to-month premise.

Operation and maintenance cost	Operations and upkeep cost: Includes the following Direct work costs: To install and then to maintain the same. Cost of the gear: Gear as required for the hardware of the CCTV system. Material cost: The immediate material costs.
Acquisition cost	Acquisition cost It incorporates following expenses: Commissioning cost: To initiate the frameworks and also the segments of the CCTV cameras are introduced, tried, worked, and kept up as per the operational necessities of the business. Hiring and preparing Cost: With the establishment of the CCTV cameras, the organization should enlist new workers for the checking and security of the building, in any case, theorganization will likewise need to extend some additional cash of the contracting, and preparing of these representatives. Cost of delivery of the CCTV cameras: The "carriage-inwards" as required for bringing the equipment to the premises, and included in the cost.
Disposition cost	Disposition cost The pulverization costs: The removal costs after the system gets outdated or needs to be replaced, in cases condition has crumbled. The modification of the duty stipend: It is the alteration of the expense recompense in the bookkeeping books of the organization. These are an arrangement of expense derivations that people can go up against their government salary assessment form. The rejecting cost: the scrap proceeds which reduce the costs.

3.1.1 Initiation Cost

This forms the most critical of the stages regarding costs associated. It includes a due identification of the exact hardware, including the gear needed for the physical security resource life-cycle, per Fennelly (2012). The money related element is a potentially major hazard, as the organization may not have the financial capacity for the same. In addition, afterward, the potential lack of accessibility to the physical measures to maintain the system would be a concern, per Pannell, Lampley, Ronci, and Spence (2015). Moreover, an organization may confront a security hazard because of the appraisals which are given by the venture administration group identified with the physical security resources, which could be very high, when contrasted with the prerequisites, and the RBS (resource breakdown structure) , both of which are typically reported once the physical security resources are introduced.

3.1.2 Implementation cost

This is another real cost which is looked by an organization during the establishment of the physical security resources inside the association. The execution cost is fundamentally the cost which must be brought about by the association because of the establishment of the physical security resources (McNeil, Frey, and Embrechts, 2015). This is a fundamental cost, which the organization needs to keep under thought while outlining a spending get ready for the buy of the physical security resources. The establishment of different physical security resources, for example, CCTV, Electronic Access Control Systems, and regional bars, every single physical security resource has a pixie mentation cost connected with it, alongside that there are a few dangers which are related with these physical security resources, for example, the benefit may be harmed amid creation, or the advantage may be harmed amid conveyance, or the advantage could be introduced in a deficient way because of which it won't prevail with regards to giving the security needed.

Costs of establishing the hardware and its maintenance costs are to be factored in, per Norman (2016). Also, regarding the costs of establishing the hardware, as sometimes exceptionally modern, and might require a group of experts to guarantee the benefits are introduced and are working according to the prerequisites of the associations.

3.1.3 Operations and upkeep cost

The security costs can constitute a significant part of the annual operating costs of an organization. Operational hazard thus is connected tothe assurance of methodical approach, and additionally the budgetary dangers. Establishment of physical security resources inside an organization might take up to 10 to 15% of the aggregate spending plan of the organization, alongside that it will likewise require visit upkeep, repair, and observing which would likewise expand the general support cost for the organization. Operational Security could basically be characterized as the procedure utilized for the production of strategies and in addition methods which are utilized for setting up controls, and in the meantime to preserve the data identified with the abilities, and all the more vitally the vulnerabilities of the association. This should effortlessly be possible through the distinguishing proof, controlling, and insurance of the interests connected with the trustworthiness, and in addition the unobstructed execution of the office. A portion of the basic components of operational security incorporates, the staff individuals; these are prepared security workforce who are in charge of the assurance and additionally the ones in charge of implementation of the security strategies and the methods representing the operations and all the more vitally the security of the entire office or the business. Consequently, operational security strategies are a noteworthy cost which an organization must cause, so as to guarantee that the physical security resources introduced inside the organization are successful and equipped for keeping the unapproved access of an outsider, or unapproved staff to the office. Operation and support cost dangers, which are being looked by the associations, incorporate;

- Cost of repairing harmed or broken resource
- Cost-relatedto the acquiring of the extra parts
- Insurance cost
- Administration cost
- The standard support cost

Sullivan, Pugh, Melendez, and Hunt, (2004) directed an examination in which they expressed that a portion of the previously mentioned expenses could undoubtedly be assessed. An organization can get astandard contract for protection, and additionally normal upkeep of the hardware, this may help the association in concealing an offer of the aggregate lifetime of the security resource. Though, then again a noteworthy hazard is being looked by the organization with regards to the forecast of the repairing expense of the extra parts which may be required for the security resources, as there are sure resources for which the extra parts won't be accessible, or it could be too exorbitant to buy which may build the general cost of the business.

Consequently, it could be closed it is fundamental for the organizations to distinguish the distinctive sorts of support which must be performed over various physical security resources, be that as it may, the most vital viewpoint in such manner is the assurance of the individual or the association, which will be bound to play out the assignment of upkeep. In this way, it is fundamental that an association sets up specific techniques with the point of updating the innovation and the physical security hardware's inside the association to keep the security frameworks of the association’s p to date. Besides, the associations should likewise set up and devise get ready for the post-improvement of the product, and all the more imperatively the equipment bolsters necessities. A portion of the prescribed procedures which could be trailed by an association incorporates:

Providing a depiction of the approach embraced to the upkeep, and additionally the supply field administrators, as they should be furnished with every one of the instruments important to guarantee that the frameworks work with no troubles.

The association should likewise characterize the standard emotionally supportive network gear which could be used successfully with the frameworks, and in the meantime the association should all examines the requirement for directing uncommon tests for the product and in addition the equipment hardware keeping in mind the end goal to guarantee that they are working in a compelling way.

The clients should the prepared, with a specific end goal to guarantee that they are fit for using the physical security frameworks set up, in a proper and compelling way, which is inthe best enthusiasm of the organization. Finally, the association should likewise give a depiction of the transportation of the same.

Moreover, another main cost element to the organization would be the upkeep cost, as the security resources require visit support for which the organization may need to enlist a gathering of people or they could sign an agreement with the support firm, that will as often as possible screen the execution of the hardware, and if there should arise an occurrence of any issue will make the corrections or repair the harmed resources. Subsequently, this is an additional cost which the organization may need to acquire related to the physical security resources.

3.1.4 Acquisition cost

The obtaining cost is another cost which is brought about by an association when an association gets new security resources. This cost could be related with the cost which the organization may need to look on the off chance that the obtained resources may endure some kind of harm amid the conveyance, or the benefits may miss a few sections which are needed per McDougall, and Woodruff (2016). And especially in cases, when the management has to refer to extra parts to another merchant, this can increase the overall cost estimates.

Also, the organization may likewise need to acquire the transportation expenses of the advantages, which could bring about enhancing the general expenses of the planned spending plan of the organization, committed to the buy of the security resources. Subsequently, it is fundamental that with regards to the procurement of the security resources, the organization must keep under thought the acquisitions cost, and it must keep some abundance measure of trade out submit case additional money is required. Along, with that, the organization can likewise influence an examination to thegroup, which will be in charge of guaranteeing the wellbeing and conveyance of the hardware, and it falls upon them to ensure that all resources thereof are integrated and operationally well looked after.

3.1.5 Disposition cost

Like the procurement cost, an organization may likewise confront some genuine dangers, or misfortunes with regards to the air of the physical security resources. There are a few circumstances where an organization may be expected to arrange off the physical security resources, for example, the gear may wind up noticeably outdated, or the hardware could be harmed, or the for some situation the organization simply needs to refresh the more established security resource with another one keeping in mind the end goal to guarantee an abnormal state of security at its office. Subsequently, there are a few dangers and costs associate includingan arrangement of the old resources, and of making way and substituting for the new gear.

Therefore, it is vitalfor an organization has an arrangement with regards to the attitude of the organization. The organization must devise an arrangement amid the underlying stage at the time of procurement, whereby the management must extract a valid estimate of the overall life-cycle costs associated with the resources. This will be afundamental exercise to conform to the overall financial plan of the enterprise.

3.2 Management of Risks Associated with Physical Security Assets

This element lies at the heart of the general basic leadership procedure of the organization. Besides, it additionally gives the association a portion of the key capacities, framework, and the processes as required in the overall plan of the organization. Hazard administration is a part of this exercise, per Fennelly (2012). Along these lines, recognizable proof, appraisal and additionally the moderation of the security dangers helps the organization in the general administration of the dangers related to the physical security resources. With regards to the administration of the physical security resources, the dangers administration could likewise be connected with the phase of the general hazard administration exercises which are being surpassed by the association.

The organization must devise a reasonable bearing over the hazard administration procedure of the physical security resources with the improvement and additionally the execution of the prerequisites related with the physical security strategy of the organization, as physical security resources are an indispensable segment of the organization. (Reason, (2016) expressed that the organization must receive a dangers administration approach for concealing the different zones of the security movement over the association, keeping in mind the end goal to guarantee an abnormal state of security is kept up over the association. At last, with regards to the improvement of a compelling danger administration technique for guaranteeing the administration of dangers related to the physical security resources an organization must have some defensive security arrangements, and required conventions.

The end goal is to recognize whether some kind of changes is required inside the strategy, or the additional security resources are to be introduced and used in the association. A standout amongst the most critical duty associations with regards to the administration of these dangers is to mitigate the risks to an acceptable level. A hazard cannot be always obviated, but in any case, the organization can find a way to limit the general dangers related to it. Thus, risk management procedures require due acknowledgment and mitigation of these hazards. The following depicts the levels essential for this practice:

Figure 3-1: Physical Asset Security Risk Management Process

Table 3-2 Risk stages classification

Risks	Risk Classification
Initiation risks	• Incorrect spending estimation: These relate to wrong estimates of procuring gadgets and the other apparatus. • Cost overwhelms: This is due to theexpansion of the costs, the overruns due to bad planning and estimation. • Project scope extension: Additional costs spend may be required due to theexpansion of the earlier defined security scope. • Inability to understand the dynamics: The organization may not have the capacity or the controls to figure out the extent of what is at stake in the process. • Technology and vulnerability: due to innovations, systems may get obsolete. • Risks in Specification Breakdown: May is not accurately identified, and hence later may cause issues. • Unrealistic desires: Unaligned expectations as derived from the systems, unrealistic ones of over-reliance. • Schedule imperfections: Schedule defects and the plan issues which the calendar brings about, making hindrance for the entire tasks. • Uncontrolled Requirements Inflation: There are sure situations where the aggregate cost of purchasing or offering a physical resource either

	increments or declines because of changes in the swelling rate.
Implementation risk	• Risks are not tended to appropriately in arranging: Improper distinguishing proof of dangers may lead towards uncalled for arranging which could end the general procedure of the buying and establishment of the undertaking. • Wrong time estimation: Inaccurate estimates regarding timing of phases which will delay then the overall tasks of completion. • Inadequate appreciation of complexities: The representatives of security apparatus and maintenance in the organization may not be adept at understanding fully the functionalities and technicalities associated. • Unexpected scope developments: Unrealistic venture expectations would lead to hike in costs. • Specialists not employed: The staff may not be competent enough to design and operate the system. • Staff Turnover: The group taking care of the physical resource may leave the association in unexpected numbers, which would expand the selecting, and preparing cost for new workers.
Acquisition risk	• Resources are not followed appropriately: While gaining certain physical resources the organization may confront certain dangers in following of the obtained physical resources, as the organization may neglect to track the general advance of the physical resource • Continuous evolving prerequisites: Another significant hazard which an organization may confront is the adjustments in the necessities. • Running out of storage: An organization may come up short on reserves while making buys of costly physical resources and might endure because of cost overwhelm amid the buy of the physical resources. • Market improvement: The creating market and the adjustments in the commercial center may likewise end up being hazardous for the organization, gaining the physical resources. • Changing needs: The needs of the organization identified with the physical resources may change with the progression of time, which

	thus may raise some genuine dangers for the organization. • Government lead changes: Changes in the administrative tax assessment, principles, and controls may raise some genuine dangers for the organization searching for obtaining physical resources. • Hardware and Software abscond: For gear resembles CCTV Company may require particular equipment and programming gadgets, and administrations, inaccessibility, and nonappearance of such particular terms could raise some major issues for the association. • Integration issues: The new hardware introduced by the organization might bring about expanding complexities as they would not be good with the organization's present foundation, and might raise some genuine worries for the organization.
Operation and Maintenance risk	• Monitoring gear disappointment: The Company may need to confront some genuine dangers because of the disappointment of the security resources, as might put the entire organization and its security in danger. • Technical dangers: These are the specialized dangers which an organization may look because of the perplexing systems of recent innovations regarding upgrading. • Failure to address need clashes: An organization may have issues because of setting up wrong needs while the acquiring and establishment of the security resources. • Failure to determine the obligations: The Company may neglect to determine the genuine clashes connected with general task duties inside the association. • Insufficient assets: The Company may likewise experience the ill effects of deficient assets with regards to the introducing of the physical resources, as the organization won't have adequate assets. • No legitimate subject preparing: These are the dangers which an organization may look because of uncalled for preparing of the workers related to the physical resources inside the association. • No asset arranging: Improper arranging of the assets may likewise

	have a negative effect on the execution of the undertaking, and absence of assets may likewise stop the physical resource buying and protection of the task. • No correspondence in group: Lack of correspondence among the administration and the senior workers could likewise bring about thedisappointment of the entire undertaking.
Disposition risk	• Health and Safety Risks: These can occur due to sub-par or obsolete physical resources, or even inadequate training of staff. • Selling Costs: The Company may endure some additional expenses while offering the obsolete physical resources, because of disintegration, and outdatedness. • Environment chances: This is in context with events of nature, which the resources may endure because of ecological changes and may end up noticeably defective and dissolved. • Out-dated and harmed gear: This is because of the aura of harmed and obsolete equipment. • Recycling cost dangers: Sinceorganization working in the present market is appearing to be as manageable as conceivable in this manner, the organization might look toward reusing of the old security resources, which could expand the general expenses for the association.

3.3 *Security Assessment*

Fennelly, (2012) expressed that fittingly imagined, and all the more imperatively implementable security programs, approaches, and in addition advances are critical in guaranteeing the protection of the office to various dangers, while in the meantime it additionally helps in taking care of the general security requests, for example, unwavering quality, uptimes, and all the more vitally the execution goals of the firm. Moreover, security designs are additionally basic to guarantee the security of the general population, data, and also the procedures, and hardware's which are housed inside an office or assembling office, as they are on the whole very expensive, and must be set inside the limits bound.

The deployment of resources that are designed to see, discourage and counter against the dangers and a very much arranged utilization of set up of security frameworks and components are revealed as dynamic measures. While, the utilization of scenes, design, and lighting to accomplish upgraded security by diverting, overwhelming or vindicating growing fear based oppressions are imagined as uninvolved physical security forms.

The wellbeing of information openness, unwavering quality, and secrecy from planned or incidental abuse by conceivable risk factors from both inside or outside of an organization is called Information Security. It incorporates guaranteeing to certify people the suitable access to intense frameworks and data; giving safety efforts to responsibility for; restricting data solely to approved elements; maintaining a strategic distance from unlawful changes; abuse of exclusive information; and ensure that information is exchanged to, bring by or pooled with just the proposed party.

The way toward framing controls to safeguard knowledge data with respect to authoritative capacities and protections and making strategies and methods for a robust system of organizational security is termed operational security. The assets have to be managed in a way that ensures true and proper execution. Qualified and able staff must be designated and selected for these tasks. Wrongful access has to be discouraged by the systems, as the framework of deterrence needs to be robust enough.

Be that as it may, regardless of how strict and complex the physical security gear is the security design has constantly demonstrated to the Achilles Heel of various associations. Pavlov, (2013) expressed that the real shortcoming which has been distinguished among various associations the nonattendance of far-reaching, and powerless hazard evaluation. They additionally expressed that different evaluation tends to the security of an association from the point of view of electronic frameworks in spite of examining it as a critical element thereof.

The system must have the capacity to distinguish the benefits which are required, and also helps the organization in identifying the requisite security resources, per Miller, and Beckman, Amazon Technologies (2013). This necessitates taking a holistic view of the framework, and by the HR working inside the association. Subsequently, the administrators in an organization have the task to decide on the level of uncorrupted and smooth operations that are desired.

The appraisal of security should lead to a recognizable proof of the dangers, and in addition, it should likewise give a portrayal of the dangers. These security dangers should likewise be seen as the potential events, with theunfriendly goal that could have an immediate effect over the association, and be equipped for making some genuine harm the representatives, and the general population connected with the association. Thus, an appraisal of the dangers to physical security resources defenselessness is exceptionally basic and must be mandated.

The harms related to this aspect come from three potential sources. To start with, are the harms, which come about because of thedisappointment of insurance of the secret information which is being held by the association, this information could be private data in regards to the customers of the association, where the loss of customer data can be fatal for the organizations.

Then, the lack of adequate upkeep and maintenance of the data will impact the smooth working of the organization and can antagonize the business partners in case of compromises. Hence, the breaches end up being exceptionally broad with both lasting and in addition contemporary harm to security systems affecting operations of the entity.

Then, there is the harm of private information put away inside the frameworks of the association, and the connected issue of unscheduled downtime with the concomitant loss of business to the entity. The misfortunes endured by an organization could be colossal. Besides, unscheduled downtime could likewise debilitate the wellbeing of the representatives working inside the association, the strength of the office, and administrative consistency.

Consequently, once every one of the dangers and in addition vulnerabilities is evaluated, at that point the organization could organize those dangers alongside the methods for countering and reacting towards those dangers in a powerful way. This is the last advance which enables the associations to distinguish the specific shortcomings and afterward address those shortcomings in a successful and productive way.

Consequently, so as to guarantee compelling and proficient security it is fundamental that an organization possesses a complete hazard evaluation design from the physical security frameworks, alongside that this appraisal design should likewise be considered from a spending point of view also. It is the obligation of the senior administration of an association to direct a careful examination of the dangers related with the physical security resources keeping in mind the end goal to settle on educated choices in regards to the assignment of the capital assets. These reactions could moderate the general misfortunes of the income, disturbances, and thus must be factored in for dangers administration of the process.

3.3.1 Threat Identification

The management has to anticipate the type of attacker sorts, for example, offenders, and psychological oppressors. Henceforth, ID of dangers, and the general population which could turn into a wellspring of those dangers must be distinguished keeping in mind the end goal to guarantee that such kind of dangers are precluded, so as to guarantee the security of the association, and all the more essentially the general population working inside those associations. In this way, it has turned out to be more critical for association today to actualize safety efforts which are outlined particularly for the assurance of the security offices, individuals, and the data frameworks of the organizations, which has all the secret data of the organization and its customers.

Subsequently, it has turned out to be fundamental for the association to plan and create security countermeasures and additionally approaches which could lessen the dangers and in addition, the difficulties which are inalienable to these dangers which have been saying above. In this manner, it has turned out to be fundamental for the association to build up a comprehension of the goals of the aggressors attempting to break the security of an association;

- Instilling the dread in the psyches of the casualties through theestablishment of profoundly powerful physical security resources
- Inflicting of damage or demise
- Damaging and devastating the property, hardware, offices, and all the more essentially the assets which could be used by the aggressors for harming the organization

Henceforth, the business organization must dissect the advantages, and also the dangers from aggressors to formulate own strategies therewith. A robust appraisal would help mitigate this and would sit well with the functioning of the organization as providing comfort to the staff.

3.3.2 Site Planning and Security Risk Assessment

With a specific end goal to play out a security hazard evaluation, it is critical for the business associations to see the physical security condition to be adequate. In the event that the business associations need to survey the security design, at that point it must need to utilize the site-particular hazard appraisals. Alongside this, the security necessities should likewise be tended to with the end goal of the improvement designs. The more the measures are brought in later into the system, the less viable and more costly would itbe. The CSO's must be counselledwith at the earlier stages with anearly meeting with respect to the physical security condition of their association.

Altogether for the business associations to set up another site security design, the associations should first choose their new site for their business operations. The security design might likewise stay for the Greenfield site and the offices which are under development. Additionally, the organizations should likewise build up a site security get ready for the offices which are experiencing significant renovation. Alongside this, the site-security designs created by the business organizations should likewise guarantee all together for the arranged reaction to produce results it is basic that the security control measures ought to determine a postponement. Besides, the physical security needs, which should be executed by these partnerships, should likewise address the issues of how to help in operational strategies. The issues of over-locating and specialized reconnaissance have to be differentiated and specialized security measures need to be incorporated therewith.

While considering the above variables, the business organizations should likewise consider taking the physical safety efforts on account of new structures at the underlying stages in order to be most effective and efficient regarding the cost spent.

3.4 *Mitigation Responses*

Periodic updates are essential to guarantee adequate focus and achievement of security objectives, per Rose, Rajendran, McDonald, Karri, Potkonjak, and Wysocki (2013). An issue that is most relevant is the case of confusion amongst the representatives taking a shot at various floors in a building. The real issue which emerges under such conditions is incongruencies which emerge between the bases building administration frameworks and in addition the security frameworks that are being utilized by singular organizations working inside the building. Thus, this could have a spiralling effect on the security costs due to duplication of work, and wastage of time. A simple way to resolve this issue would be to have two separate security appraisal frameworks – one for the base building and the other for the different floors of the buildings. The ideal choices have a solitary UI which could be incorporated with the contribution from alternate floors, this would guarantee compelling arrangement of the safety efforts, and also for the base building.

A quite common mistake done in theinstallation of CCTV cameras is to have a plethora of cameras showing a lot of surveillance without due monitoring of the images as relayed. Moreover, the time required to survey, chronicle, and all the more significantly store the simple or the advanced data is additionally ignored in numerous cases which leads towards disappointment of security. Moreover, it is basic to adjust the quantity of CCTV cameras conveyed, with the quantity of security staff's accessible. For the most part, this normal is something close to 1:20, thereby meaning that 20 cameras are for one individual. Images sent to basic zones to identify the endeavoured unapproved passage at the site or the area. The interruption recognition frameworks must be based over the system, and in the meantime, they should likewise be based over infrared, movement, vibration indicators, evaluation, and acoustical and in addition the commence control unit, committed reaction, and all the more critically the security reaction conventions and in addition the techniques.

Besides, inability to give adequate regulatory help to appropriately enlisting, confining, and all the more vitally expelling the representatives inside a security framework is a standout amongst the most widely recognized oversights submitted by the associations. Another real error which is made often is the lack of required safeguards in the remote areas of the frameworks – encryption and programmed firewalls would help in mitigating this issue.

3.4.1 Conducting Risk Assessments of Physical Security Assets

The assessments can be by nature experiential, well-being, or trial stages, and so on. Evaluation items are the inside for proper innovation valuations, operational necessities definitions, the procurement projects and arrangement choices examination. Leading Risk Assessments Security experts plan every one of the necessities and requirement for helplessness and Risk appraisal in view of the gathered data as it is key for the underlying advance in changing or building up every one of the projects and strategies. The objectives and goals of hazard appraisal are to survey outcomes, assess trustworthy dangers and abilities which are illicit or non-unlawful in nature and distinguish powerless regions. At the point when thechance evaluation is splendidly collected, it should recognize and connects every one of the openings to existing cautious security frameworks. Aptitude with security structures/mechanical assembly's and measures of accomplishment and adequacy ought to be seen through the use of operational involvement in theinformation of related procedures and physical security. Supports to address dangers and the revelations of hazard evaluation must be completely archived in discoveries of hazard appraisal reports.

3.4.2 Vulnerabilities Identification linked to Physical Security Asset

Every one of the breaches and vulnerabilities is seen through the use of security encounter, recognition of safety efforts and hardware, measures of accomplishment and viability of security techniques and consciousness of related procedures. Deficiencies in security countermeasures and misfortune counteractive action program in security assurance frameworks and data innovation frameworks a portion of the vulnerabilities which incorporate the greater part of the dangers postured to an office. As the hazard valuation is led, the security authorities should give careful consideration to blemishes and susceptibilities which make a benefit more inclined to hurt from a threat or risk. Everything adds to the thoroughness of harm when an episode happens. The appraisal for powerlessness gives outline premise danger exact to the office's task and belonging and henceforth, hurts an association or office. The office will have the capacity to extend a system to protect the basic missions, regulatory necessities when the LOP concerned and the related plan risks have been assessed.

3.4.3 Auditing Physical Access

Logs and audit trails have to present in order to conduct an audit on the physical access control systems because they can enable one to guess the exact time and place where someone accessed or was trying to access the premises unlawfully. The tools and technology used for auditing purposes are neither detectives nor preventive. The organization has to respond swiftly to the audit trails and access logs to ensure that the physical security of the facility is not tampered with because failure to respond on time will lead to intrusions on the system. It is important that the organization provides enough security to cater to the extra resources being acquired. The exact date and time in which someone tried to access the premises illegally have to be included in the access logs and audit trails. There should be a record captured for all unauthorized access attempts, regarding the employee and the specific location of attempted access.

3.5 Costing and Life-Cycle Management of Physical Security Assets

An organization can improve its operations through management of physical security assets because this promotes adherence to the outlined managerial laws and also offers the necessary support to the administrators within the organization concerning thesafety of the physical security assets by initiation of internal controls. The organization should ensure that each person accessing the premises should be informed of their responsibilities and the areas where they are permitted to access the facility. Successful implementation of such strategies demands proper stewardship and care and the organization should be prepared for financial consequences together with unforeseeable consequences associated with data loss.

According to Straub, and Welke, (1998), the physical security policy has to get the necessary support from managers in the organization together with the accountability of the physical security assets and systems. The organization should take up the responsibility of managing and safeguard the properties it has acquired, obtained or leased all through the lifecycle of the property. The organization can achieve this through custody and accountability up to the time when it decides to formally get rid of the asset through disposition or after a successful investigation concerning assessment for property loss.

The physical security asset management system should always include important assets in the organization such as badging, CCTV, cars, sensors, magnetometer, sensors, door locks, metal detectors, etc. Flexibility is afforded to the entity through automatic asset management (Shahidehpour, and Ferrero, 2005), regarding replacements to the security apparatus. This system can also be used to manage the maintenance contracts of the equipment together with the total training costs. The company can be able to easily determine the type of equipment which should be exposed to cross-leveling the support of higher level facility using this system as well as determining the location of each equipment separately and if it has been installed properly and operating according to the specifications. The system also enables the company to identify the person in charge of the maintenance practices on the physical security asset.

Some companies are unable to acquire the automated physical security asset management systems. In such a case, the company should opt for a manual system should be installed and will be assisted by electronic records of the physical security assets with details such as the exact location of the asset, quantity, value, and the state. All the assets must be labeled s that their identification for different reasons later can be established easily. The company has to seek the help of the equipment vendor or logistic firm in a situation where the physical security asset lacks a national stock number so as to establish whether the national stock number of the particular equipment exists. Keeping an equipment in the company that lacks a national stock number may make the company incur extra expenses in future which can be avoided. When such an equipment is damaged or develops a problem, the company will have to foot the repair or replacement expenses because the warranty would be considered invalid. The other type of cost which the company has to incur when purchasing a physical security asset is the tracking cost. The company has several physical security assets and each asset contains a number of components e.g. the CCTV system. The company should, therefore, be able to track each of the components in the physical security asset individually and other factors such as theprice of the physical security asset can be used when classifying the component or systems for tracking purposes.

The company can be able to choose the suppliers who are selling their equipment at the most affordable rates which will enable it to save on costs. If a component on the equipment develops a fault, the system can be able to easily identify the specific component and all this depends on the policies and timelines which the company has set concerning repair and general replacements of equipment which are faulty.

3.5.1 Managing and Accepting Risks Related to Physical Security Assets

According to Spielmann et.al (2006), organizations can employ cost-benefit analysis to be in a position to choose the most appropriate approaches they can use for recognition and mitigation of the risks which the physical security assets in the organization face. The risk evaluation approach which the organization has decided to employ and also the baselines initiated by the organization should be the factors that influence the decision by the organization to allocate the necessary resources and accept the risk

After the baselines for the physical security assets concerning risk evaluation have been established, the organization can eliminate the cases of cross-leveling between the unmitigated risks by establishing the assets that have been overprotected and transferring the security measures to a different asset with minimal protection. Through this process, excess resources in specific areas can also be distributed to other sections where the resources are inadequate and this will enable the organization to adopt the most valuable and cost-effective security program. With such a system in place, the company will be able to utilize appropriate mechanisms to manage and secure its resources.

According to Roper, (1999), some risks cannot be tolerated by the business after a cost-benefit analysis is conducted maybe because the consequences associated with the risk have lesser effects to the business or when the probability of the risk occurring is very low. The business can decide not to take any action pertaining such risks after analyzing the costs incurred and the benefits of implementing the risk reduction approaches. In every instance or location when it is suspected that a certain risk is likely to happen, it is important that both the decision was taken and the policies of the business concerning that particular risk are documented.

3.5.2 Product life-cycle management (PLM) of Physical Security Assets

Product life-cycle management refers to the variety of approaches employed in security management, and a number of functional stages are followed in the security management process. As time moves, the original condition of a product such as the CCTV equipment changes and this necessitates proper care of the equipment all through its lifespan. Stark, (2015) defined a warranty as a document issued by the vendor or manufacturer of aparticular productwhich explains the manner in which the product is expected to function for a given period of time. The warranty becomes useful if in any case the product fails to function in the manner specified by the manufacturer and the owner wants a refund or if the product is to be replaced by another one of the same kind.

It is the responsibility of the staff in charge of procurement in the company to acquire, repair or dispose of the equipment. On matters concerning disposal of the physical security equipment, the procurement department in the company is advised to inform the procurement office of the agency first before proceeding with the disposition. According to Ford et.al, (2013), routine care of the physical security asset should involve preventive maintenance in order to avoid carrying our repairs on the equipment which can sometimes bring additional expenses to the company. Utilization of a preventive maintenance strategy and inspecting the equipment used in the security system regularly can make the person in charge of security avoid any major security hitches caused by over usage of particular equipment. The preventive maintenance approach has been implemented in most companies because of its effectiveness in relation maintenance of the security systems and the components involved. Most companies consider this approach as sound and very cost effective.

It has been proven that the lifespan and performance of the equipment can be increased through regular maintenance practices. Several things are however considered when dealing with the issue of preventive maintenance with the important ones being CCTV systems, intrusion detection systems, magnetometers and vehicle barriers. The design of each of the measures for improving security is based on the main goal which is minimizing the risks concerned with theissue of security.

3.6 Whole Life Cycle Costing Of Physical Security Assets

Activities like monitoring and planning of the physical assets have been incorporated in physical asset management. These activities happen throughout the lifespan of the physical assets in the company. Managers in the organization have to dedicate enough effort in order to achieve effective management of physical assets and such an initiative has to happen throughout the lifespan of the asset in the company. Physical asset management is conducted in order for the organization to find the most appropriate solution that involves minimal costs in purchasing, usage, maintenance and disposal of physical security assets. This is done to in order to achieve the security targets of the company (Boussabaine, and Kirkham, 2008). Physical asset management can then be defined as a process that involves planning, purchasing, maintenance and finally disposal of the physical assets and considering the costs which the organization incurs. Physical asset management also ensures that the organization strictly adheres to the existing policies set by the government within matters related to physical security.

According to Hastings, (2010), physical lifecycle costs can sometimes exceed the expectations and most people working in the budgeting department of the organization may fail to notice them. Some operational costs may be incurred by the organization in relation to the physical assets and failure to detect such costs may create complications in the budget forecasting process. This may also be a problem for theeffective management of the company's incomes. When new capital assets are acquired in the company, the lifecycle costs of the assets have to be identified so that comparisons can be drawn concerning the costs of other available alternatives. Budget forecasting can then be conducted after the above comparisons have been made. It has become a common practice among companies to embed the activities related to monitoring and controlling of physical asset lifecycle costs. This is done in order to minimize the costs related to physical assets which are incurred by the companies and also to counter the difficulties encountered in controlling the physical assets.

3.7 Costs Estimation Methods: Modeling and Simulation

This constitutes one of the critical activities in the security framework dimension. At the beginning of the project, estimations are conducted on the initial costs, acquisition cost and maintenance costs (Kishk et.al, 2003). The company utilizes a variety of approaches and models for collecting relevant data from previous records for purchases made by the company. Estimation of the overall cost of the project is done using a mathematical expression.

Detailed classifications for the main software schedule and approaches for cost estimation are highlighted below:

- Learning Oriented Models
- Regression-Based Models
- Composite Bayesian Methods
- Expert Based Approaches

According to Rahman, and Vanier, (2004), the erroneous tendency associated with the form of estimation is a normal issue. This is because an estimate can also be considered as an assessment that depends on the precision and probability of the future state of the physical asset, therefore it can be difficult to encounter such in the whole process.

Monte Carlo simulation is the most commonly used model for cost estimation purposes. Companies use this model to assess the costs of the assets throughout the different related phases to estimate the cost of physical assets throughout the lifecycle of the project. A tool that can be deployed effectively here is the Monte Carlo simulation. It also ensures that the estimated uncertainties concerned with physical assets are well managed in the company.

Monte-Carlo simulation can be defined as a tool that helps in the simulation of modeling processes where chance variables are involved. In the Monte-Carlo simulations, there should be a very big number of iterations, possibly in hundreds or even in thousands where the number of physical assets is too large (Emblemsvag, 2003). Each sample generates a single probable outcome for the concerned variable. The range of possible outcomes can then be determined after analysis of the results distributions. The final value can be converted into a stochastic variable using deterministic simulation and thereafter the effects of these changes on the stochastic variable can be recorded on a spreadsheet.

A number of approaches are used in the Monte-Carlo simulation method to get the solutions of mathematical problems employing repeated random testing. When performing the computations, some calculations that utilize random numbers are used in place of the random test results. The random variable concept and the transformations of both discrete and continuous variables can be assessed. Examples include the diffusion mechanism and attainment of the required balance between the systems at different temperatures, per, Touran, and Wiser (1992).

We can use the above two examples to understand what is meant by the term irreversible process and the variations that take place in the steady state.

The available details concerning the decreasing potential law during thebreakdown of a radioactive element into a different state that is stable. Note that from a basic model of the radioactive nucleus, where the breakdown process occurs in a random manner, with the chances of its occurrence relying on the width of the probable obstacles which are contained in the particles that make up the core of the element. Additional examples include the study of a system having fewer states in preparation for the study concerning the behavior of a paramagnetic material which has been exposed to a magnetic field at a particular temperature. We will then examine how a dielectric material behaves and this will be a demonstration of the uses of thetransformation of a continuous variable. (Emblemsvag, 2001). The main issue associated with Monte Carlo simulation approaches is getting the value of both the discrete and continuous variables with the probability distribution functions p (x) from the value of a random variable with a uniform distribution in the interval (0,1), generated by a computer or a different program which is part of the routine.

It is advisable to use a large number of random numbers when simulating a physical processor when computing the answer for a mathematical problem. The roulette number method is too slow and also actual physical systems produce random variables which have distributions that are somehow different from the ideal distribution. Tables with uniformly distributed random numbers can also be utilized although they have to pass through a comprehensive test based on special statistics. Such tables can only be effective when the Monte Carlo simulations are performed by hand, and this rarely happens because of the complexity of the task. The simulation exercise is easier when the random numbers are used as produced by the seed and throughan iterative process, with a uniform distribution in the range (0.1).

Triangular distributions are the most common types of distribution in Monte Carlo simulation because the process of obtaining the input data is very simple. The other major advantage associated with Monte Carlo simulations is that it doesn’t rely on lengthy investigations (Fleischer, Wawerla, and Niggeschmidt, 2007). Usage of the triangular distributions in Monte Carlo simulation modeling is the main contributor to their high status and also its usage in the software. Triangular distribution can also be used where two errors are involved each with a uniform distribution within the bounding limits and also whose means have been merged linearly. Triangular distribution is also used to model the cases of uncertainties and in such situations, the asymmetric triangular distribution is utilized as demonstrated in the expression below:

$$x_i = \begin{cases} a + \sqrt{z_i \cdot (b-a) \cdot (m-a)}, a < x_i \leq m \\ b - \sqrt{(1-z_i) \cdot (b-a) \cdot (b-m)}, m < x_i \leq b \end{cases}$$

The mean and the standard deviation are given by:

Mean: $$\mu = \frac{a+m+b}{3}$$

Standard Deviation; $$\sigma = \sqrt{\frac{a^2+m^2+b^2-am-ab-mb}{18}}$$

According to a research, the distribution and the density functions for the parameters are asymmetric Brémaud, (2013), and can be expressed as:

$$f(x) = \begin{cases} \frac{2(x-a)}{(b-a)\cdot(m-a)}, a < x \leq m \\ \frac{2(b-x)}{(b-a)\cdot(b-m)}, m < x < b \\ 0, elsewhere \end{cases}$$

The cumulative distribution function is therefore given as follows:

$$F(x) = \begin{cases} 0, x \leq a \\ \frac{(x-a)^2}{(b-a)\cdot(m-a)}, a < x \leq m \\ 1 - \frac{(b-x)}{(b-a)\cdot(b-m)}, m < x < b \\ 1, x \geq b \end{cases}$$

Graphs are used in the Monte Carlo simulation model to present cumulative distributions. Plots on the graphs at class boundaries represent the cumulative frequencies and then straight lines are later used to join the resulting points on the graph. In other situations where the values for relative frequency are represented over the normal probability graph, the graph will be represented by a straight line for the random variable with a normal distribution. It is possible to use the normal probability graph in determining whether the observations have been sourced from a population having a normal distribution. It is, however, important to note that the values given in this method are only approximations.

3.8 *Life Cycle Cost Analysis*

This can be defined as the original plans to acquire a physical asset up to the time an asset would be disposed of after use. The lifecycle of an asset is made up several major phases, i.e.

- The original definition of the idea
- Creation of comprehensive report concerning the design requirements, documentation and specifications of the asset.
- Construction, Development, and purchasing
- Warranty period, initial stages inthe utilization of the physical asset.
- Prime period of the physical asset, operational support together with the maintenance activities, operational costs of the asset in relation to modifications on the asset and renewal.
- Disposal and clean-up after the physical asset reach the end of its physical life.

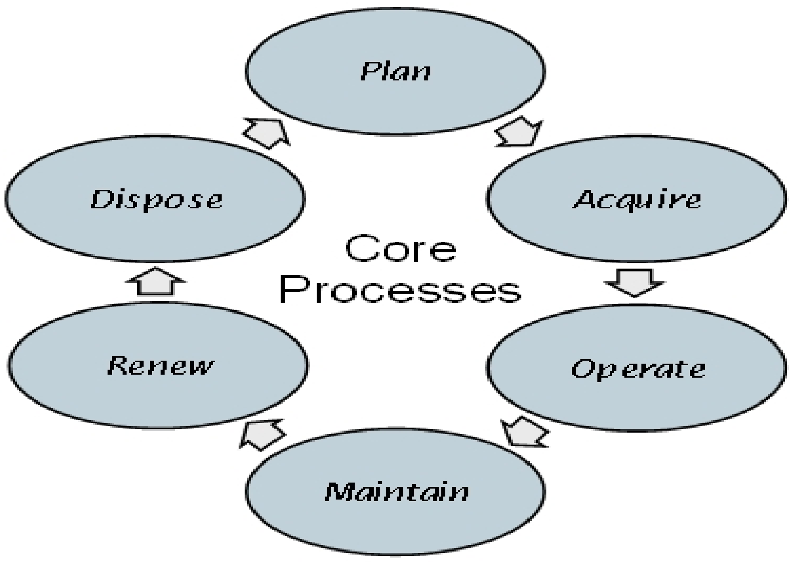


Figure 3-2: A representation of Lifecycle cost of physical assets

The illustration in figure 1 above is a representation of the daily periodic and strategic activities for an asset that has been purchased by a company for the sole purpose of enhancing the security within the premises of the company (Márquez et.al, 2012). The first stageof the lifecycle of an asset involves strategic planning and then shifts to themanufacturing of the asset, usage, maintenance, renewal and the final stage involves disposition after the physical life of the asset has ended.

Lifecycle costs can, therefore, be defined as the cost whose main objective is to optimize the overall costs incurred by a company for owning a physical asset. The costs are estimated by identifying and quantifying each of the significant net expenditures which are accrued by the company due to ownership of a particular physical asset. According to Kaming, and Marliansyah, (2016), most companies acquire new physical security assets every year and the only costs which are considered are the acquisition costs. The acquisition costs may seem attractive to both the purchasing department and the overall management of the company because it may prove to be a good deal for the company even in future due to minimumoperational expenses. It is very important to note that the low cost of acquiring the asset doesn’t mean that the overall costs involved in the lifecycle of the asset would be low, therefore the low acquisition costs can’t guarantee that the company would reap maximum profits from the deal. After evaluating the trade-offs between the varying costs, the main objective of the lifecycle cost is to ensure that the selection, usage, and replacement of the physical assets is done in a way that is beneficial for the company. Different types of companies all over the UK are currently utilizing lifecycle cost analysis.

Lifecycle cost analysis ensures that a company which has acquired a physical asset gets the best deal possible for the money invested on the physical security asset. There are factors that affect the possibility of a company realizing the expected benefits from the investment such as access to fast, precise and useful information (Santos, and Ferreira, 2013). Such a process begins with the vendors dealing with therequired asset, thefunctioning of the current assets owned by the company, utilization of the best statistical approaches in predicting the expected costs that the company will incur due to ownership of the asset. A company should, therefore, ensure that it adopts the best ever measures in conducting the evaluations, which will then ensure that the management information systems designed are able to perform the necessary analyzes on the data. All these procedures are followed to ensure that the lifecycle cost analysis of the physical assets produces accurate outcomes.

Lifecycle cost analysis is considered as one of the most important tools as far as the security of physical assets is concerned, and therefore the company has to put in enough effort to minimize any possibilities of the security being compromised. According to (Beckers, 2015), the security can be monitored in a control room and operations in the control room are not affected by factors such as its size and location. The factors which have to be considered to ensure smooth operations in the control room include security, the instructions issued by the management in the company, the basic operating procedures, the necessary equipment and finally offering training to the staff members in the company who will be monitoring security in the control room.

According to Pikaar et.al, (2016), several measures have to be put in place in order to ensure that confidentiality of the control room is maintained. Such measures include safekeeping of pictures and other important details from unauthorized access, ensuring that the control room cannot be accessed by unauthorized individuals at all times. According to Piza et.al, (2015), the company is supposed to implement strict close door entry and exit laws to ensure that the security of the control room is not compromised at any instance. The organization should also ensure that the design of the control room meets all the required standards in order to be able to guarantee thesecurity of the premises. Each of the health and safety regulations should also be strictly considered during thedesign of the control room to ensure effective operations. The employees hired by the organization to work in the control room should be capable and trustworthy due to the high level of privacy associated with the control room.

A research was done by Mitrou, Drogkaris, and Leventakis, (2014) and the outcomes from the research revealed that human beings have the fundamental rights of privacy, choice,and autonomy. The organization is therefore supposed to ensure that that the CCTV systems are used within a legal framework which abides by all the laws concerning privacy. It is therefore mandatory for the organization to put into consideration all the legal requirements associated with people’s privacy before deciding to proceed with implementation of the CCTV systems in its facilities to help in surveillance activities. According to Chung, (2014), it is important for the organization to issue a proof of the surveillance activities in its premises in order to avoid cases of random intrusions which may have an effect on the privacy of people.

The office of the Information Commissioner in the UK recommends that the organization should ensure CCTV surveillance must follow the regulations contained in the Data Protection Act 1998, Human Rights Act 1998 and Regulation of Investigatory Powers Act 2001 together with other laws that apply in the United Kingdom. The existing laws also recommend high levels of familiarity on the issue of CCTV surveillance because images of people are recorded by the CCTV systems and such an exercise is considered as extremely intrusive with regard to the privacy of people. An organization should, therefore, ensure that all the legal mechanisms have been followed before proceeding with the implementation of such systems which intrude into the privacy of people. The laws that have been set by the UK government should all be followed before engaging in surveillance of people. The Data Protection Act, 1998 is an ACT that is applied within the United Kingdom and is considered by many as the essential Act with regard to CCTV surveillance. This Act was formulated mainly to offer protection to information which was being collected from individuals using the CCTV systems.

According to Schuman, and Brent, (2005), the ability of a physical security asset to be able to offer its security services continueuntil the company is what determines its life. In some cases, the effective life of the physical security assets comes to an end even before they become non-functional and such a situation sometimes happens due to changes in either company policies or amendments to the existing laws within the country that relate to privacy. The effective life of the physical security asset may also come to an end if the company perceives that the economic importance of the asset has gone down, and therefore its operations within the facility are stopped. The company may also decide to terminate the services of the physical security asset if the services it offers fail to meet the minimum requirements expected by the company (Cabeza et.al, 2014). It can therefore be concluded that the two main factors that may cause the effective life of the physical security asset to end before the asset becomes non-function are: changes in technology due to introduction of better and more advanced technology as compared to that of the current asset and changes in the organizational demands where it may be perceived that the current asset is not offering sufficient services as required.

One can be able to determine the effects of a certain product or service on resources and the environment in general by conducting an analysis of its lifecycle. After getting results from the analysis is when a decision can be made on how to minimize the effects by considering other alternatives of the product. Lifecycle analysis (LCA) of a given product involves a systematic evaluation of how the product affects the environment throughout its lifecycle (Audu, H.A.P., Aniekwu, and Oghorodje, 2015). Such an evaluation on the product involves the movement of materials or energy into and out of the product through the various phases of its life from the point where raw materials were extracted up to the final phase. Standardization of the LCAs by ISO (14040-14043) began in 1994.

After conducting an analysis of the lifecycle of a given product or service, the outcomes can only be declared as good when it satisfies the conditions below:

- Minimal natural resources were utilized in the manufacturing stages. It includes energy, water,and other resources.
- Renewable ones are those that can be reused or recycled.
- It is possible to reuse or recycle the product at the end of its physical life.
- Minimal or zero cases of environmental pollution were reported during the manufacturing stages, it has minimal or no effects on global warming, it has minimal or no impact at all on the ozone layer, it has brought minimal negative impacts on the ecosystem and has no negative effects on both plant and animal life.
- When plant and animal life, and the ecosystem in general benefits from the manufacturing, utilization,and disposal of the product at the end of its lifecycle.

A company can be able to select the most suitable product or service from a number of alternatives to the product by conducting a lifecycle analysis of the various product ranges. Through such an analysis of the products, the company can decide on how to utilize the selected product sustainably (Whyte, and Gayner, 2013). Analysis of the lifecycle of a given product can also allow the company to utilize the product in the most suitable way before the end of its physical life and to ensure that maximum benefits are reaped from the product. The Life Cycle Analysis of a given product is conducted by an organization on two main occasions:

- When the organization is making purchases for raw materials and supplies that are used in its daily operations. Lifecycle analysis allows the organization to establish the behaviors of a certain product or supply and to make comparisons with other alternatives of the product or supply so as to be able to choose the most appropriate one. Grid lasting acquisitions help in making these comparisons of the products varieties.
- An organization may decide to conduct the Lifecycle Cost Analysis on the commodities or services which it supplies to the clients. After conducting such an analysis, the organization can be able to determine the stages in the life of the commodities or services, their effects on the environment and any form of enhancements that can be made on their products or services. Each of the factors that may take place all through the life cycle of a product or

service from when it is introduced are noted by the company. Such an approach may be referred to as eco-design or sustainable design.

The initial stage of the cycle for a relevant asset is at the stage of acquiring it, and then it comes to an end when the company either decides to dispose it or to withdraw its services from the facility. A life-cycle cost analysis is therefore conducted by the organization with the main objective of optimizing the costs incurred in getting the asset, its ownership and then the consequent use, through using the present value approach whereby the organization attempts to establish and quantify the major costs which the physical asset accrues all through its life cycle (Durairaj, Ong, Nee, and Tan, 2002). An organization may decide to conduct the life cycle cost analysis in order to quantify the various ranges of products or services available with the main objective of ensuring that it will attain maximum benefits from any option it chooses. The life cycle cost analysis also allows a trade-off between the cost elements in the various stages of the life of the physical asset. It is important for an organization to consider such aspects so as for benefit maximally from any of the choices that might be made concerning the products or services.

The life cycle cost of a physical asset such as a CCTV system is made up of two major types of costs namely: Capital costs and Recurring costs. These costs have been described below.

Table 3-3 Type of cost

Type of Cost	Description
Capital Costs	Regarding acquisition of the asset
Recurring Costs	This occurs on a regular basis or an approximated cost that is documented with a single record.

3.8.1 Capital Costs

This is usually defined as the acquisition cost of an asset, and in our case, it can be considered as the cost of acquiring the physical asset. The capital cost involves more than just the costs involved in purchasing the physical asset or the equipment. Any extra expenses charged concerning the physical asset are all considered as capital costs such as the costs incurred during the delivery process of the asset and the cost of installing the physical asset before it begins functioning. Per Malmenbratt, and Brooks (2015), the CCTV system requires a complete and well-organized analysis of the issues which the organization wishes to settle and using the most appropriate approach. The main reason why an organization may decide to establish the operational requirements of the CCTV surveillance is to get the assurances that the design of the CCTV surveillance system is done in line with the requirements and functions of such a system. In a situation where an organization is unable to identify even the basic needs of such a system, the management won't prioritize the acquisition and implementation of the system.

According to Dadashi, Stedmon, and Pridmore, (2013), all the factors associated with the focus of the CCTV equipment such as traffic, objects,and human beings must all be considered in the operational requirements of the CCTV surveillance systems. Other uses of the CCTV surveillance system include monitoring and observing the movements and behaviors of people in a particular geographical location. On the issue of preparation of the operational requirements, the organization has to ensure that an exercise of such importance should be conducted in a precise and organized manner and also in a way that convinces everyone within the organization. All the workers and stakeholders in the organization should be encouraged to offer their opinions as part of the inputs in drafting the operational requirements of the CCTV surveillance system. The most effective way of accomplishing this task is by forming a working group with members who are capable of taking part in such type of activity. After the group has finalized with the requirements of end users of the system, the process of establishing the technical specifications of the system becomes much easier and the tendering document will now be based on the aspects mentioned.

According to Donald, and Donald, (2015), the organization can be able to achieve maximum output from the system and also ensure that the system lasts the longest time possible. To achieve these goals, the organization has to give special attention to the general management of the systems and the costs incurred in the day-to-day operations of the system. Such factors have to be considered by the organization in the planning stages and during investment appraisal. The organization can cater for the expenses involved in theinstallation of the CCTV equipment but there are higher chances that no funds will be set aside to cater for the day to day operation and management of the system. It is necessary for the organization to consider all the costs involved in theoperation of the CCTV systems and to ensure that it has the ability to sustain the presence of such systems. Most parts of the CCTV system have warrants and may later require funds to be set aside by the organization to cater for their operational costs on issues like replacement of faulty parts; the budget planning section in the organization is responsible for performing such tasks.

Chen, Wu, and Hsieh, (2013) stated that the organization must ensure that operational guidelines should always accompany the CCTV systems and they must also be very clear and precise. The operational guidelines comprise a set of rules explaining the behavior of the system and an operation manual. The set of rules which have been defined in the operational guidelines require that anyone operating the equipment is well-familiarized with them including the management of the organization. These rules provide very important information concerning the camera operations, information privacy policies, the policies that govern the functioning of the CCTV surveillance system, the level of accountability over various aspects and overall operations of the surveillance system. The operation manual which is also part of the operational guidelines is where users of the system will source instructions about the configurations of the system. The operation manual also helps in sorting out issues related to image management, location, and design of the control room, staffing of members who will be in charge of the control room and stating the tasks of each one of them and the monitoring process which will be conducted in the control room.

The capital costs also involve various other costs apart from the ones that have been explained above. Examples of these costs include the cost incurred when carrying the feasibility of the research and the costs incurred during the tendering process of the asset. Another major cost also exists which is part of the capital costs but is rarely recognized by most companies. It is known as the financial cost and is mostly associated with the monies which are contained in the value of the assets.

A different type of cost also exists which is not categorized as part of the capital costs. This type of cost is termed as future appropriations and is classified as part of the running cost. Since the running costs are charged with an interest, this will also be the case for future appropriations. According to (Boussabaine, and Kirkham, 2008), this type of cost can also be considered as a finance cost, and this implies that it won't extend to the life of the asset. In addition to this, the way in which companies incur a financial cost upon the capital fund can be considered as directly proportional, or it can also be considered as foregone interest, which in other circumstances could be accessed by organizations. Particular costs must be identified by organizations in other situations for example in the assessments of non-asset solutions and the approaches used in theacquisition of other alternatives of a certain product or service. Additionally, it is also important to consider the particular cost when dealing with the private sector where there are plenty of other alternative products or services that are available.

3.8.2 Recurring Costs

The types of costs that have been classified as recurring costs include the maintenance costs, cleaning costs and the energy cost for each of the physical security assets. An organization has to consider several issues with regard to the physical security asset such as cameras, LCD Displays, and the surveillance system. These systems require maintenance, energy, and cleaning of the equipment which should be done after a specific period of time which is determined by the management (Cheng, Aerts, and Jorissen, 2010). The costs incurred by the organization in recruiting staff that will operate the surveillance systems are also classified as recurrent costs. Any form of repairs or enhancements that may be carried out on the physical security asset during its lifespan is all categorized under recurrent costs during the planning process. The only instance when disposal costs can be classified as recurrent costs is when the cost incurred during disposal of the physical security asset is significant. Such a situation is considered when there is aneed for remedial work on the activities and assets which are related to the projector when there is aneed for ratification.

Environmental considerations are very important in particular cases. A conclusion can be made that the relative significance of capital is significantly affected by the nature of the physical security asset. It can also be concluded that the overall life-cycle cost of the physical security asset majorly depends on the recurrent cost. According to (Smith, 1999), the costs involved in theinstallation, operation, and utilization of a given physical security asset exceed the costs of acquiring the asset by a very big margin. An organization should, therefore, conduct alife-cycle cost analysis to assess all the available alternatives in the market to ensure that it will reap maximum benefits from the choice that will be made.

3.8.3 Basic Principles of Life Cycle Costs of Physical Assets

Physical assets are considered to be very important resources in any organization and that justifies the need for asset planning for security and stability purposes. The only way to make sure that the organization acquires the necessary inputs at minimal costs is to implement the asset management principles. Below are the principles that must be followed to guarantee an effective physical asset management process:

- Incorporation of strategic planning with asset management
- Assessment of the need to implement asset planning over other choices which consider the expenses related to life-cycle, risks, and other ownership benefits.
- There has to be accountability concerning the state of the physical security asset and its usage.
- Asset disposal decisions have to be established on grounds that will enable the organizationto achieve a favorable net return under a fair trading framework
- Creation of a functional control scheme which operates under the asset operation and management.

3.9 *Components of WLCC*

This refers toan approximation of the expenses involved in the purchase, commissioning, functioning, maintenance, and disposal of the physical asset. It was also referred to as cradle to grave cost analysis by Kumar et.al, 2012). Life cycle cost analyzes are mostly conducted so that an organization is able to account for all expenses related to physical assets. The organization can then use the life cycle costs during planning, budgeting, and purchasing of physical security asset.

Elements of the whole life costing are explained below:

Table 3-4 Components of WLCC

Components of WLCC	**Description**
Acquisition Plans	On the decision to acquire the assets.
Life cycle Asset Management Plan	Regarding monitoring and maintenance the asset.
Replacement Choices	This represents the decision made by an organization to replace the asset and incur extra expenses associated with the decision.
Effect of Analysis Timing on Minimizing	This is related to cost reductions arising from the prolonged usage of an asset.
Life Cycle Costs of the Physical Assets	Regarding the overall associated costs

3.9.1 Acquisition Plans

A major reason why an organization should conduct life-cycle costing is noted at the pre-acquisition stage where the organization has to evaluate the overall life-cycle costs, primarily at the boar-brush stage, after which the information would be used in the acquisition stage and in the decision-making process where the best deal has to be chosen from a number of alternatives (Mele, and Sangiorgi, 2015). The most important issue here is to evaluate all the available options in the process of acquiring a physical security asset due to the fact the final decision may be an underestimation or overestimation of the real cost.

Life cycle costing is mostly conducted in the acquisition stage so that the organization can be able to determine all the expenses involved in the acquisition of a physical security asset and these costs will be considered all through the lifespan of the physical asset (Silalertruksa et.al, 2012). Life cycle cost analysis for the physical assets is first introduced in the broad-brush stage and then changes are later effected on these costs as the organization concludes its decision to acquire the physical asset.

The different types of expenses included in a life cycle cost analysis include the overall acquisition expenses of the physical asset, the operational expenses, the lifecycle of the physical asset, the life of the major elements in the asset and the expenses incurred in theacquisition of spare parts. A summary of the lifecycle of physical assets is given by (Zamagni, 2012). Zamagni, (2012) which contains the cumulative costs and the opportunity of manipulating the costs. It is in the planning and acquisition phases where there are opportunities for manipulating the costs. The advantage of this is that when the firm is choosing its physical assets, the issue of logistic support must always be considered. Presence of the asset in the firm can cause a negative impact if such issues are not considered and this may affect the expected benefits related to the initial cost.

According to Stark, (2015), acquisition costs are classified as dominants and it’s the same case even for passive items. For equipment like CCTV and RFIDs which use electrical power. The original costs might be lower as compared to the operational expenses. For such type of assets, the operational expenses have a significant effect on decision making on whether to make the purchase.

3.9.2 Lifecycle Asset Management Plan

This can be explained as a scheme that is usually initiated after the operating regime of a given asset has been determined and is associated with repair and maintenance processes on the equipment, the expected lifespan and disposal plans of the equipment by the organization (Campbell, Jardine, and McGlynn, 2016). A lifecycle asset management plan is part of the lifecycle costing process and both activities are conducted together on the physical assets. One of the most important reasons for conducting a lifecycle cost analysis is the need for a plan.

Budgeting for expenses related to the asset and planning of finances can be achieved with the help of a life cycle asset management plan. This scheme can also be classified as the broad brush which is experienced at the pre-acquisition stage, even though it has to be exposed to some changes at the feasibility analysis stage when the asset is being used in the organization.

The maintenance needs of the physical assets consist of both routine maintenance and unscheduled maintenance procedures. The feasibility stage where installation of the physical assets takes place involves a logistic support analysis which acts as an input for this plan.

The manufacturer of the equipment has to provide the basic guidelines explaining the maintenance procedures to be followed. This particular requirement can be exposed to some changes depending on the type of activity and also the environment in which the equipment is operating. If the rate of operation is higher in comparison to the normal conditions, the severity of the situation would increase and therefore the organization has to consider both the life cycle asset management plan and the general expenses involved (Blengini et.al, 2012). The main regulatory regimes should also be considered in the lifecycle asset management plan, but in a situation where the physical assets are not standardized, a different method like the Reliability Centered Maintenance can be used to select the most suitable maintenance plan.

3.9.3 Replacement Choices

This is also one of the main reasons why an organization has to undertake the lifecycle cost analysis. As times goes by, the company's physical assets also age and become outdated and new decisions have to be made on whether to renovate the aging asset or to make replacements. The organization makes such choices after accessing the expenses incurred in maintaining the current asset and the cost of acquiring another one. According to Jardine, and Tsang, (2013), the organization can only decide to replace the old asset if the yearly maintenance expenses for the old asset are more than the cost of acquiring a new one, and this cost is determined over the lifecycle of the old asset. The costs incurred in acquiring new equipment should, therefore, be considered before the organization chooses to replace an old one.

3.9.4 Effects of Analysis Timing on Minimizing Life Cycle Costs of the Physical Assets

Per Basbagill et.al, (2013), parts of the consequences that happen in the initial stages of conceptual design are mostly responsible for the expected lifecycle costs. Such choices which the organization makes during the design phase, the designated functions, maintenance needs and the context of operation of the asset are the ones that will finally determine the lifecycle costs of the asset. The level of cost minimization which the organization can achieve in various phases of the project is shown in Figure 2 below. Shifting of the project from the strategic planning stage is also illustrated together with the choices which an organization makes relating to the expenses incurred in purchasing the new asset.

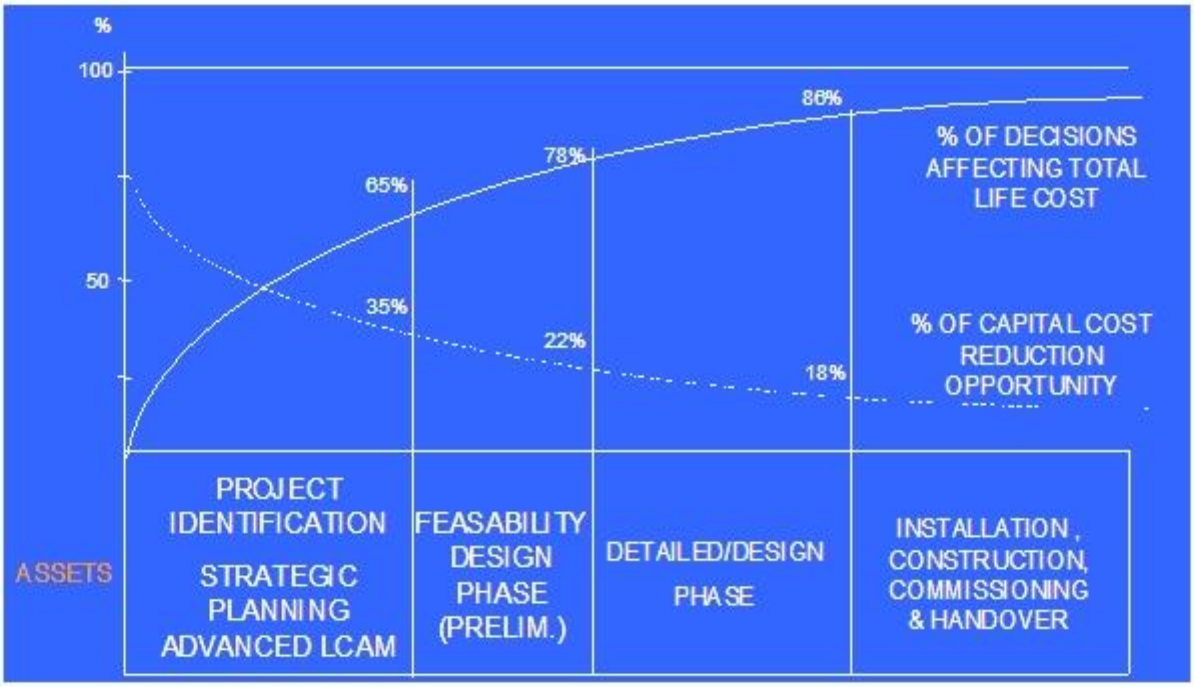


Figure 3-3: Time of the Opportunity for Cost Minimization

It is at the initial concept design and the development stage where the organization can be able to implement the cost minimization strategies in the life cycle costs of the asset. The costs are usually locked as the process reaches the final stages and cannot be changed. If the organization plans to acquire the physical asset with minimal costs, then research on the following issues should be undertaken:

- The alternative options that can be taken concerning the project.
- The expected time period in which the equipment would be functioning.
- The costs for other alternative options.
- The level in which the asset would be used in the organization.
- The initial cost and operational expenses of the equipment.

The company can be able to analyze the other alternatives for a given physical asset utilizing the framework provided in thecontext of the lifecycle of the physical asset.

3.10 *Overall Lifecycle Costing Procedures*

Lifecycle costing is done in four procedures namely:

Cost elements of the interest: These represent the cash flows that occur in the lifespan of the equipment. This has to be considered during thedetermination of the lifecycle cost which will obviously include all the expenses the physical asset has accumulated from the time it was purchased by the organization up to the end of its lifespan (Settanni et.al, 2014). Even though there is usually an agreement that defines the type of expenses to be counted, each decision relies on a number of opinions which have to be considered.

Defining the cost structure: This process involves combining all the expenses involved after which the possibility of trade-offs can be determined, and this will enable the organization to attain the desired levels of the lifecycle costs. The required extent of the lifecycle cost study together with the total number of alternative cost structures are the ones that will determine the model of the cost structure.

Cost estimating relationship: This is a mathematical equation that is used to define the estimating purposes, and also the cost of a given equipment as a function of more than one independent variables (Liu et.al, 2014). There is enough evidence to show that these types of costs account for the overall collected costs. Hyperbolic, linear and parabolic relationships have been used to prove this.

Determination of lifecycle Cost formulation method: The best methodology that can be used in the lifecycle costing process of the physical asset is chosen here.

3.11 Lifecycle Costing Elements

All the expected costs together with the benefits were determined by the lifecycle cost method. The method also lowers the costs to match the current value using discounting methods which allow easy access to the economic value of the project. The lifecycle costing elements below play a significant role in the lifecycle costing process of the physical asset:

Initial capital costs: These can be classified further into thecost of acquisition, cost of financing, cost of setting up, training and commissioning (Finnerty, 2013). Assessment of other costs such as those for spare parts of the equipment will be included in the acquisition costs. The organization can obtain quotations from prospective suppliers which can be used to estimate the physical security assets. The costs associated with effects of alternative funds and gearing are included in the financing costs. The additional costs are set up costs and costs involved in training the users of the equipment.

The discount rate: Choice of the discount rate is a very important aspect of the lifecycle costing process because the discounts arean issue depending on the current value of the costs. A high discount rate will, therefore, favor the alternative having minimal capital cost, maximum recurrent cost and minimal life cost (He, and Krishnamurthy, 2013). Even though the effects of minimal discount rates wouldn't be as desired, the effect of the earning power of cash invested can be revealed together with the inflation effects.

Life of the asset: The lifecycle costing process is affected by the expected lifespan of the asset due to the fact that this variable has an exponential effect on the asset (Settanni et.al, 2014). The life of the asset is associated with five main aspects. Assets needs are expected initially, as articulated by the functional life. Then is the period during which the asset will retain its physical shape until a replacement is found. The third is the technological life which represents the time period until when the technical features of the asset will fail and a replacement is acquired with improved technological features. The others are alegal and social life which represent the time period until when humans decide to replace the asset or as a legal requirement.

Operational and maintenance costs: This involves operating the equipment using the least possible costs. Determination of both the maintenance and operational expenses is an important step in the quest to lower the lifecycle costs of the asset (Kincaid, 2013). Labor expenses, material expenses,and establishment costs are classified under operational costs of the asset. The performance of assets of the same kind is used in the approximation of these costs. The downtime expenses can be lowered through the implementation of a normal, organized and precautionary maintenance policy. Maintenance expenses can also be lowered through the implementation of a 'run it until it breaks' policy. Replacement of old parts on the equipment can also be done to minimize the expenses accrued because of downtime. It is important for the organization to undertake the appropriate maintenance level which is in line with its objectives of incurring the least possible expenses.

Disposal costs: This represents the costs an organization incurs after the working life of the physical asset comes to an end. Destruction costs, thesale of the asset, scrapping, and taxes charged in any other transactions related to the asset are all classified as disposal costs. After the useful life of the physical asset comes to an end, such costs are subtracted from the residual value of the asset (Woodward, 1997). Different businesses offer various levels of discount rates and this is the duty of accountants within the organization to settle this issue instead of relying on theminor subjective determination. Concerning evaluation of the appropriate swelling rate, it is easy to calculate the applicable discount rate.

3.12 *The general cost structure of Lifecycle of Physical Security Assets*

The function of the general cost structure (GCS) in the project is to explain, list and organize each of the costs and revenues over a period exceeding 10 years (Heijungs et.al, 2013). If the main objective of the project is to acquire and utilize the system, the cost structure will come from the system. This incorporates each of the direct costs and part of indirect costs (LCC).

In case a privately owned organization is in charge of the project, the expenses incurred by the customer will be considered, and associated risks along with the return (IRR) will also be included (Lee et.al, 2016). The risks taken by the organization undertaking the project operations should match with the TRI.

A detailed explanation should be provided for each of the sections and no cases of repetitions should be reported on the topics list. The CGS, therefore, varies with respect to the concerned fields (aeronautics, space, naval, land, building, etc.) in order to satisfy the stated conditions.

Three major constituents are contained in a simple item of cost: a resource utilized by any process related to a product e.g.

- Cost of consumables for maintenance (process) of an engine (Product)
- Employee expenses (resource) for growth (process) software (product)

Stages of the lifecycle are fully experienced in the activities e.g. for the initial stages we have management, engineering, design, production, integration, testing and on-site setups. The use phase involves functioning, maintenance, replacement, continuous learning and technical support. A product tree is used to explain the activities. It is mainly composed of major and additional elements (maintenance facilities, education facilities, spare parts, infrastructure, etc.). Resources for these elements comprise various classes of the staff, consumables, the common organizational means and the services where an organization subcontracts the service from outside.

The whole-life cost of any given system may be lowered using the total cost method (and related project) through mastery of the financial effects of choices related to design and service withdrawal. The expected costs can be forecasted using this method (e.g. to create an expenditure plan or respond to a request for tender) and adoption of the most appropriate and cost-effective plan. Extension of the prediction and optimization functions is what differentiates the total cost approach from the other traditional method.

3.13 *Cost Approximation of Physical Security Assets*

Most of the approaches employed in cost approximation of physical security assets rely on historical data. Keeping records of the costs is therefore necessary. The process of approximation through analogy is achieved by comparisons with some elements or getting comparisons for other processes (Estébanez et.al, 2015). Guidelines have to be given in this process by experts.

Mathematical expressions which include a cost to the explanatory variables are used by the parametric approaches e.g.

Estimations for the total yearly maintenance in terms of load in kg (LOAD), number of level (NBNIV) and the speed of the lift in m/s (SPEED) utilizing the model below:

$$COST = 655.46 + 0.481 * LOAD + 38.56 + 522.68 * * NBNIV\ VITESS$$

Estimation of the costs incurred in theinstallation of CCTV cameras in the company can also utilize an equation that is somehow similar to the one above, i.e.

COST = cost of Installation (£15,000) + Monitoring Costs (£20,000 Per Camera) + Maintenance Cost (12.5% of the total Monitoring Costs) + Management Costs (10% of the Monitoring Costs)

Technical analysis of the system and related processes (Case of purchasing and utilization; dynamic description) are included therein. The analytical approach is widely used and may even rely on the product description or the service under assessment (installation activities, equipment, etc.) or the process to provide the guidelines.

It can only be possible to implement process modeling (production and maintenance) when there is adequate information in place concerning the system (Nicholson et.al, 2014). Earlier estimations in the project are therefore discouraged. The dynamic characteristics of any given system are reproduced in the simulation in a certain period of time considering the random phenomena it is exposed to.

3.14 *Summary*

The main objective in this Chapter is to determine and clarify the different classifications of costs related to lifecycle cost analysis of PSA, so as to straighten the activities related to planning, maintenance, disposition,and replacement. The sundry risk management aspects concerned with PSA overall lifecycle cost analysis are also identified and explained in this chapter. A comprehensive method adopted towards PSA has to include detailed analysis concerning all the aspects, their relationship, state of their timing incidence and different other steps adopted to handle the risks. All the sections have been highlighted in this Chapter through an extensive effort in theformulation of the costs while considering all the available alternatives. Monte Carlo simulation methods have been proposed for use in modeling and cost approximation, but an exhaustive review would be in provided later. It will then be possible to evaluate, monitor and control the lifecycle cost analysis using a recently developed model that contains a framework where users can have access to different elements related to the costs and risks.

CHAPTER 4. EVALUATION OF THE OVERALL LIFE CYCLE COST FOR PHYSICAL SECURITY (CCTV)

4.1 *Introduction*

Various researchers and departments within the sector have given different versions of definitions. There is currently no definition of lifecycle cost analysis that can be used for each of the projects of equipment e.g. the CCTV systems. The researcher will, therefore, use this chapter of the research to explain various definitions of lifecycle cost analysis uniquely associated with CCTV systems. The researcher will also reveal the definition being used at present concerning lifecycle cost analysis which has been suggested by global standardization organizations. Secondly, the main elements of lifecycle cost analysis will also be introduced by the researcher in this chapter. Thirdly, the readers will get a summary of the lifecycle cost analysis procedures, an explanation of the CCTV systems cost structure and cost evaluations concerning CCTV systems.

This chapter will also contain a summary of the primary elements of lifecycle cost analysis and the researcher will then provide details concerning the data requirements and the resources needed in conducting a lifecycle cost analysis for CCTV systems. The researcher will highlight the possible sources of data for the CCTV system and data from organizations that are currently using CCTV systems. Data will also be collected from companies that make the CCTV equipment as well as historical data concerned with CCTV equipment and data to be used for modeling and forecasting.

An assessment of the current cost model and technological abilities in the lifecycle cost analysis will be done in the next section. The researcher will then finalize the study by presenting the measures for economic performance in the overall lifecycle cost analysis. Examples of the measures include the basic economic performance measures, discounted and simple payback measure, theratio of savings to investment, etc.

4.2 *Lifecycle costing Definitions*

It is quite difficult to select the most appropriate definition of lifecycle costing for a particular organization due to the existence of quite a number of definitions suggested by researchers, project managers,and industry standards. This difficulty arises due to the fact that none of the definitions which have been proposed so far can be fully accepted by each of the companies in the sector. Dhillon, (2013) defines lifecycle cost as the combination of several terms which can be able to describe the estimations in the overall cost. Even though most of the suggested definitions have a similar basic theme, there is no precise information concerning the total number of definitions being used by the various organizations in the sector. Part of the lifecycle costing definitions is highlighted below.

4.2.1 The 2014 ISO 15686-4 Definition

This can be explained as an ISO standard concerned with service life development. It is the decision process concerned with thedevelopment of the physical security asset's service life (Hernández-Moreno, Ocaña-Ponce, and Mejía-López, 2014. This ISO standard defines lifecycle cost as the overall cost of ownership of the physical asset over its whole life. Such costs include the financial costs which can be easily computed, social and environmental costs. Some costs are very hard to compute and quantify particularly in instances where numerical values of the costs are required. The basic expenses which are usually included in lifecycle cost include purchasing costs, acquisition, operational costs, maintenance costs, and disposal costs.

Organizations wishing to purchase new physical assets can use the lifecycle costs to evaluate each of the alternatives present. The lifecycle costs can also help in decision-making processes where the overall costs are to be optimized in the lifespan of the asset (Kaming, and Marliansyah, 2016). An organization may also use the lifecycle cost to compare it with the real cost of physical assets which are of the same kind e.g. CCTV camera and use the same when there are plans to purchase new assets.

Environmental costs are also assessed, and companies can be able to consider all the options available before finally arriving at a decision for example in situations where a company is supposed to make a decision with more than two alternatives to choose from. For a project where power sources have to be installed to enable the CCTV equipment to operate in the company premises, the environmental effects caused by the power sources can be evaluated with the help of a lifecycle cost analysis (Lemer, 2015). A comprehensive lifecycle cost analysis conducted by the organization can enable it to evaluate if any of the options has the desirable environmental cost. The organization can also be able to determine the social cost related to the project and therefore when CCTV equipment is installed in a particular region, they will be able to monitor the activities of people e.g. when the CCTV cameras are installed around malls, there are higher chances that residents near the malls will raise complaints concerning the effect of the cameras to their social life. It is, therefore, the responsibility of companies to evaluate the effects of the cameras on thesocial life of people and lifecycle costing approaches may be used in such situations to compute the social costs related to theinstallation of physical security assets.

4.3 *Main Elements of Lifecycle Costing.*

Lifecycle costing is made up of several elements but this study will only focus on the main elements related to lifecycle cost planning.

4.3.1 Lifecycle Cost Planning (LCCP)

LCCP is one of the most important elements associated with lifecycle costing. LCCP aims to determine the overall cost incurred in theacquisition of the CCTV equipment. The fact that lifecycle cost planning incorporates the operational costs and capital costs related to theacquisition of the CCTV system makes it one of the most important elements (Green, 2014). A company can be able to use lifecycle cost planning in comparing the costs of CCTV cameras being offered by different sellers in the market. The manner in which LCCP presents these costs is very consistent and comparisons can be easily drawn using the discount approach, and therefore the company can be able to get the best deal concerning thepurchase of the CCTV cameras.

The administration within a company may use LCCP to obtain a variety of techniques that will be used to transform the diversity associated with a number of costs into a completely reliable measure, which is associated with theeffectiveness of the cost, mostly in matters related to theacquisition of the CCTV cameras. It can, therefore, be agreed that budget organizers in the company who are responsible for acquiring the CCTV systems can use lifecycle planning to come up with the cost targets. The budgeting section of the company can also use LCCP to make estimations concerning the price of the CCTV equipment using comparisons which are supported by this particular approach. General approximations can be proposed by the budgeting section after considering various alternatives offered by different dealers in the market. The main disadvantage associated with LCCP is that the processes involved in making the comparisons take too much time. Errors in the figures provided can also be experienced and this is because the data being handled is sometimes too much. The existence of such errors on the figures may affect the capital costs related topurchasing of the CCTV systems.

4.3.2 Life Cycle Cost Analysis (LCCA)

This can be defined as a means of determining the best alternative in terms of associated costs in comparison to other available options in the market (Audu, Aniekwu, and Oghorodje, 2015). All the factors have to be observed within the company to ensure that everything is going on as planned. The example of LCDs for the CCTV system can help in explaining more about lifecycle cost analysis whereby the department in charge of budgeting in the company has to include all the user costs such as the setup and functioning of the LCD screens. The budgeting department can also determine agency costs through lifecycle cost analysis. The agency costs are associated with upcoming tasks for the company such as occasional monitoring and maintenance of the screens. It is important to note that all the costs involved are discounted by the lifecycle cost analysis with the present day value (net present value).

According to Lee, and Lee, (2017), lifecycle cost analysis can be defined as a technique used for evaluating the overall ownership costs for physical assets e.g. the CCTV system and other equipment, each of these assets come with an extra cost. Lifecycle cost analysis also allows the company to determine the CCTV equipment with advanced technological features, and the ones that will allow the company to save on costs. All these processes will make the total costs involved in acquiring the CCTV system to rise, but in the long run maintenance and operational costs would be lowered significantly. The lifecycle cost analysis is, therefore, an easily explainable technique used in theassessment of the economy. Other approaches including the Net Saving method and the one relating to Savings to Investment can be utilized together with the lifecycle cost analysis approach because they are all compatible and the two other approaches are consistent with the measure of evaluation using life-cycle costs analysis. It is important to note that the length and parameters involved in the research must be equal.

4.3.3 Lifecycle Cost Management (LCCM)

Lifecycle cost analysis is associated with lifecycle cost management, such that after analysis of the costs, LCCM proceeds with the process to detect any form inconsistencies in the costs suggested by lifecycle cost planning and lifecycle cost analysis. If any form of inconsistency is detected in the costs, the cause of the inconsistency is assessed together with the actions to be taken in order to eliminate the problem. The major advantage associated with Lifecycle cost management is that on the issue of installation of physical security assets like CCTV systems in the company, it advises the company on some aspects which will guarantee proper maintenance of the CCTV systems and the company will be able to save on costs (Bakker, Helmer, and Schavemaker, 2014). The other advantage of lifecycle cost management is that it offers some recommendations to the company about tax issues related to the installation of the physical security equipment.

4.3.4 Full Year Effect Costs (FYEC)

This can be defined as the business estimate for the current year's financial performance, which is then utilized in thepreparation of the upcoming financial term for the capital purchases of the company. Changes are made on these costs monthly depending on the performance of the business, and therefore the business can be able to make short-term decisions concerning the physical security assets. In a full year cost approach, evaluation for performance improvement is done by drawing comparisons between the present costs and the future costs.

According to Taylor, (1981), the budgeting department and the company as a whole can use the full year costs to strictly consider the capital costs together with the operational costs of the CCTV equipment after some stated time, mostly between 1 and 3 years. The useful and educated estimates can then be determined with the help of the full year effect costs. Such estimates are obtained from the operational costs arising from usage of the CCTV equipment and it is important to note that these are costs don't fall into the category of discounted costs. It is equally important to also note that issue of inflation can be easily accommodated by the budgeting team during the costing process. The main disadvantage associated with full-year effect costs is that it has minimal impact on issues concerned with theevaluation of short-term costs, and this explains why the company uses it in the budgeting process.

4.4 Lifecycle Costing Procedures

(Ristimäki, Säynäjoki, Heinonen, and Junnila, 2013) stated that the steps listed below could enable the lifecycle costing process to be conducted successfully.

4.4.1 Determination of the Cost Structure

This process involves classification of the costs into various categories to a level where the company is able to effectively handle the whole information depending on the difficulty of the activity. Classification of the costs into various groups can be beneficial to the company such that it can be able to establish trade-offs, which will ensure the lifecycle costs of the CCTV equipment, are optimized.

4.4.2 Defining the cost estimating therelationship

This involves a mathematical expression that is used to describe the estimating activities associated with the operational costs of the CCTV equipment together with several other independent variables.

4.4.3 Determining the approach for LLC formulation

This refers to the approach that will be used by the organizations to evaluate the lifecycle cost of the physical assets. This approach isn't the most appropriate to be used in lifecycle cost analysis due to the absence of vital information. The major disadvantage associated with this approach is that it is not able to evaluate the operational and running costs of the CCTV equipment.

4.4.4 Establishing the Strategies for a 5-year Service Period

Lifecycle cost analysis is mostly conducted in a company in order to quantify the suggestions provided about CCTV equipment together with the expected operational and maintenance costs associated with the CCTV equipment for a five year period (Pizzol, Weidema, Brandão, and Osset, 2015). For the company to be able to realize the full capabilities of the CCTV equipment, very high operational and maintenance services are required. This may also involve repairs to the CCTV equipment in case faults arise which may affect the normal operation of the system during the five year period.

4.4.5 Building up Activity Timing

The life-cycle costs are affected considerably by the execution and later upkeep of the CCTV systems. It includes the cost base, and the client's expenses because of the costs related to the support exercises.

Henceforth, the operational CCTV administration frameworks could help in giving viable information to the assessment of the state of the CCTV frameworks, alongside that it could likewise give information with respect to the execution of the CCTV frameworks, that would facilitate the execution pattern of the framework, per Laura, and Vicente (2014). This further strengthens the perception and security frameworks, and with the related support, and the attitude expenses, it could have an immediate effect on the costs, which must be brought about by the firm. In this way, the underlying cost, term, operability, and support costs are on the whole critical elements to be factored in.

4.4.6 Evaluating the Agency Costs

The CCTV frameworks costs include those related to the costs spread across various phases, including its maintenance. Thus, management must decide on the extent of CCTV coverage that is optimal. The cost investigation correlation dependably happens between the totally unrelated contending elective, which gives an immediate impression of the differences that appear due to the change in quantities as desired.

Organization costs comprise the considerable number of costs that are acquired by the organizations amid the obtaining, establishment, support, repair, and mien of the CCTV frameworks. In this way, the likewise comprises of the underlying establishment expenses that are connected with checking the systems, per Guinée, and Heijungs (2017). Additionally, the upkeep and maintenance of the framework must be included in a master dynamic way, keeping in mind the end goal to guarantee to idealize operation of the CCTV frameworks. Be that as it may, a fundamental perspective to consider here is that the standard support cost of the CCTV frameworks does not have exorbitantly high expenses, yet they assume a noteworthy part in the upkeep of the execution of the CCTV frameworks.

The demeanor cost which at atime is thought to be the negative cost furnishes the organizations with the estimation of the speculation elective, which normally happens once the investigation time frame closures, and it is fundamentally needy more than two noteworthy parts initially are the serviceable esteem, and second is the remaining quality. The remaining quality could straightforward be alluded to as the net an incentive from the reusing of the CCTV frameworks, thus, the differential incentive between the reusing of the CCTV frameworks isn't generally extensive, and when this esteem is reduced over some stretch of time, at that point it has a tendency to have a practically zero effect over the after-effects of the life cycle cost investigation. Though, then again provides abig portion of the esteem part of the organization, being one of the motivations for keeping differentials in mind regarding the CCTV systems.

4.4.7 Assessing the User Costs

The three different cost segments, which form part of this being, the conveyance costs, expenses regarding postponing by the client, and harm expenses whereby the organization relies on the contract that regards the assets when acquired as being free-on-board. Conveyance is related to the upkeep, but there can be huge differentials arising from different varieties and specific features in the market. Operation and maintenance costs are also added here.

4.4.8 Hazard Analysis

The notion of hazard in the investigation more often than not originate from the vulnerability which is related with the future occasions, for example, the powerlessness of recognizing what precisely the future holds on the off chance that a specific move is undertaken. Both objective and subjective hazards may arise, per Haimes, (2015). The subjective ones cover individual recognition, for example, taking choice in light of instinct, in regards to how hazardous a circumstance could be, a straightforward case of this could be an organization should seriously think about failing of the camera less dangerous than the breaking down of the LCD. Therefore, this particular impression of hazard could be all the more unequivocally connected with the results that may emerge because of the disappointment, alongside that the failure of the firm of controlling the circumstance.

While target chance then again is related hazard connected to the “disappointment” of the framework that may be encountered. It is a matter of perception and hypothesis, however, the perception would focus on the importance attached to the functioning of the framework.

The examination of hazard deals with the related questions of – what could go wrong, how could that happen, and what are the results thereupon.

Along these lines, chance investigation empowers an association to answer the previously mentioned inquiries through consolidating the depictions of information parameters through PC programming – a feature that enables characterization of the harms related to the framework. The vulnerability points are also thrown up, which is generally attached to the life cycle cost examination approach. It provides the leaders with vital data regarding risk assessment, according to Bahr (2014). Various systematic models exist which consider the info factors as the discrete settled esteems, similar to those qualities are sure, in any case, a fundamental viewpoint to consider here is that there are various information factors which are very questionable. In this manner, the financial models are not something unique, and thus the vulnerabilities can be assessed readily. These vulnerabilities generally emanate from incorrect appraisals, assumptions, and case projections.

4.5 Real Elements of Lifecycle costing

The real components associated with life cycle costing would be included here as follows:

4.5.1 Start Costs

The calculated costs of obtaining the frameworks are fundamental to the expenses that the firm bears. The LCDs, cost of cameras, and different attachments and fixtures appended are included to guarantee that planning for the CCTV frameworks is done in a suitable way. In any case, as a less than thedependable rule, which is not fundamental, to incorporate into these expenses incorporates

- Additional costs associated with different unforeseen possibilities
- The “right of way” costs
- Costs of examination
- Costs of theorganization of the CCTV frameworks

4.5.2 Usage Costs

This includes the fitting, establishment, and the set-up of the CCTV system. The cameras, and also the choice regarding the more vulnerable zones regarding breach of security, association connects to the screens, all being part of the usage costs. Moreover, once the CCTV frameworks are initiated, the wiring, server connection are the principle framework costs. Then, there are the costs in the control and observation room, checks to the CCTV frameworks, and related monitoring costs. A special feature is of "mechanized caution" that affects the evening time, as there are set number of individuals inside the association amid the evening, at times there are night monitors. Consequently, this alert is straightforwardly associated with the neighbourhood police division. In this way, on the off chance that somebody strongly attempts to gain access, prompting thearrival of the police to check the incident.

4.5.3 Procurement Costs

This includes obtaining the cameras, the LCDs, and different other associated necessary items for operation of CCTV framework. Freight and other carriage-inwards costs are also to be included including the tariffs to be paid by the organization. The additional factors that must be borne in mind are the difference between free-at-delivery and free-on-board type of contracts, as the latter can mean additional unforeseen costs to be incurred by the organization. Similarly, the installation and training costs should be considered too.

4.5.4 Operations and Maintenance Costs

This would include costs associated with proper functioning of the framework. The working and fitting must be checked and ensured to meeting the standards, considering the end goal to guarantee that the framework playing out its activity viable, and keeping in mind that in the meantime it additionally guarantees that the framework is in operational condition, in the event that some kind of bug or blunder emerges the group consequently distinguishes and amends the mistake. Henceforth, with a specific end goal to guarantee operational productivity, the organization may have to get the services of specialists who know how to best set up and look after the CCTV framework, or in any case, the organization may decide to train its own staff or hire permanently some specialists for this purpose. If the organization chooses to prepare its representatives, at that point it should contract an expert and devote both times and push to guarantee that the workers are instructed technique to guarantee proficient working of the framework.

Besides, the upkeep costs must be borne by the organization, despite the fact that there are a few sellers which gives support benefit at a particular cost, the organization can either the profit the administrations gave by these merchants, or the organization can decide on some other upkeep firm. In the event that the organization chooses thechoice of support firm to ensure the fruitful and proficient operation of the CCTV frameworks, the organization may need to bring about additional expenses, which must be paid for regular checks, depending on the agreement entered into. Thus, the related spending must be estimated by the organization on the off chance that it selects to introduce CCTV frameworks inside the association.

4.5.5 Manners Costs

This relates to the disposition stage, once the firm decides or is required to remove the framework as it may get obsolete, or dysfunctional. Subsequently, in such cases, the organization either needs to go for repairs or on the off chance that the harm is a long way unrecoverable then all things considered the organization needs to settle on supplanting or arranging off the old hardware and supplant it with new gear. Henceforth, when the organization discards more seasoned hardware, there are sure charges, which the organization needs to pay, and the cost the organization needs to bring about, which is otherwise called the rescue expenses. Hence, such disposition costs should be factored during the phase of acquiring the framework.

4.6 *Information Requirements and the Resources required forever cycle costing*

There are some necessary features that must be adhered to by all organizations (Stark, 2015), with regards to the usage of the life cycle costing philosophy inside firms, particularly with regards to the acquiring of the physical security resources like the CCTV frameworks. Henceforth, an association needs to guarantee that it is outfitted with the frameworks through which the innovations could be used in a more successful way, alongside that the organization must have a framework set up that has very much characterized lead and rules set up to follow theproductive operation of the CCTV frameworks. Along, with that, the organization should likewise take the evaluations of the underlying and in addition the running expenses related to the life cycle costs. The impact over nature is gathered and dissected for leading the life cycle investigation. Indeed, even thoughlife-cycle costs have now developed as the fundamental apparatus in the planning procedure, there are a few elements which have assumed a basic part in the improving the general potential effect over the association. In this manner, the doubt existing among the organizations in regards to the way that the general estimation of the life cycle cost is off base has, all things considered, ended up being valid.

4.6.1 Data Sources

With regards to the gathering of information, the teams tasked with setting up the frameworks in terms of designing and requisitioning could contribute to overall assessments. Other sources may be the specialists which can be consulted with as it is their domain specifically.

4.6.2 Data from Companies

Life cycle expense incurred by firms can be shared and used by related organizations, as well as through interviews conducted of the management that has already dealt with procurement and maintenance of the frameworks. Thusly, basic information identified with different part of the physical resources, for example, the CCTV frameworks could be gathered straightforwardly from the organizations.

4.6.3 Information from Third Parties

With regards to the establishment and in addition support of the physical security resources like the CCTV frameworks association more often than not outsources these errands to outsiders. Thusly, these outsiders likewise have the data identified which helps in observing and supporting the systems. However, thereliability of the information being shared is a major concern in this dimension.

4.6.4 Verifiable Data

The analyst can gather chronicled information additionally with respect to the life-cycle costs, which can be obtained, from the security archives when available. The security archives can be accessed for the information, regarding the historical costs associated with existing frameworks and the associated points.

4.6.5 Models and Forecasts

On the off chance that there is information recorded information accessible to the organizations, neither there is any information accessible from the association, the analysts would then be able to select towards theuse of various re-enactment and estimating models. Along these lines, utilizing these models the specialist can include the access information in the framework, or the scientist can make certain presumptions in view of which the analyst can perform reproduction with a specific end goal to get the outcomes as gauges which could then be used by the analyst with the end goal of computation. Be that as it may, these outcomes won't be sufficiently exact, and could just furnish the specialists with a few estimates.

4.7 *Existing Technologies and cost models in life cycle costing*

It’s been over a decade that intense investigation into life-cycle costs has started. As far back as then various analysts have assessed the idea of life cycle cost examination keeping in mind the end goal to decide the strategy which is more appropriate for the assurance of the option that is most doable for the association, with regards to influencing the interest in the securing of the physical advantages for like the CCTV frameworks. In this area of the investigation, the scientist will show an inside and out anexamination of the straightforward cost demonstrate utilized for the costs.

4.7.1 Straightforward Cost Model

A generic model is as follows:

LCC = Ic + IMc + Ac + O&Mc + Dc

Where

Ic = Initiation Costs

IMc = Implementation Costs

Air conditioning = Acquisition Costs

O&Mc = Operations and Maintenance Costs

Dc = Dispositions Costs

The above can be adapted subsequent to experiencing an abnormal state of intricacy, which includes thegathering of the information, alongside a few different imperatives related to the association. Subsequently, a fundamental angle to consider here is that it would turn out to be very troublesome for the specialist to appreciate this condition, on the off chance that where the analyst does not have finish access to the database which has every one of the information identified with the life cycle cost.

4.7.2 Numerical gauging techniques

These methods can incorporate modern displaying procedures, conveying estimation systems that are outside of the model, or joined in that through sub-models including relapse examination (Sherif and Kolarik, 1981). The decision depends basically on the particular reason for the examination being attempted. Yield along these lines acquired, can extend from a solitary number to a point by point diagnostic breakdown of the anticipated expenses as far as eras, supplemented by scattering strategies. The LCC models have principally been doled out more than four lines. Genuine LCC display is the aggregate cost demonstrates coordination's bolster show that spotlights on the operation stage, outline exchange models that can be arranged and repair models around the support stages. The following six classes exist:

- Accounting models re the LCC segments
- Heuristic models
- Cost evaluating relationship models

- Failure-free guarantee models
- Reliability models that work to distribute unwavering quality and viability
- Economic investigation models

The significant LCC model depends on the specific needs and reasons for the assets, as opposed to the frameworks, where different parameters can be attempted, instead of depending on an all-inclusive one.

Scientific determining models by and large comprised of an arrangement of numerical connections that support the specific part of a framework. As far as possible to the degree of multifaceted nature of the framework, the model's capacity to mirror the genuine framework's execution. Thus the scientific models go from those covering particular parts of a framework to the ones that address ads up to framework LCC. Particular LCC numerical models incorporate the item innovative work (Freiman, 1975).

4.7.3 @ Risk program

@ RISK is a complex scientific displaying programs that utilizations Monte Carlo reproduction to exhibit conceivable results and in this way the related probabilities of various results (Palisade, 2016). Along these lines situation, theinvestigation can be completed impartially, with the model producing the related probabilities and related dangers identified with each unique result. This enables the client in thedetermination of dangers that to acclimate to the hazard resilience runs, along these lines obliging for settling on significant choices. Propelled highlights of the program incorporate coordination of Monte Carlo recreation with most recent explaining innovation that streamlines spreadsheet with unverifiable esteems, utilizing hereditary calculations. This can encourage the best portion of assets, ideal resource designation, effective booking and related highlights.

4.7.4 Monte Carlo Simulation

Likelihood hypothesis has been utilized principally in speaking to hazard. Bunches of programming bundles are accessible in the market for measuring hazard. In any case, an exact development of hazard probabilities is accomplished in Monte Carlo reproduction. It conveys in spite of the fact that with it, the issues identifying with displaying the suppositions. The critical part here is to develop the conveyances at first utilizing the most persuasive arrangement of factors contained in the model. These are stochastic methods that depend on created irregular esteems and probabilities so as to evaluate issues. The utilization of Monte Carlo recreation is in financial matters the distance down to atomic material science and is utilized broadly by governments crosswise over open segments. Monte Carlo (MC) has various varieties in it that take into account alternate points of view and necessities. In any case, the normal component among them all is the utilization of irregular number and likelihood appropriations to produce comes about. Results show up with uncertain esteems at the beginning, with various ward factors. The imprecision’s contained in that from rehashed MC investigations requires that the expert knows about the critical impediments related to utilizing it as a hazard appraisal device. Vulnerability and inconstancy must be isolated. The vulnerability is the absence of data, though changeability speaks to the varieties that surface in costs and different projections and real figures. The connections between the components contained in that should be discovered and considered in. On the off chance that these were overlooked, MC results would be intensely one-sided. This thusly will prompt truly wrong appraisal of dangers. The essence here is that such relationships are hard to have, in actuality, with the utilization of testing giving for the most part insufficient outcomes in regards to projections over to the populace that is little and speaks to long-haul conditions.

Latin hypercube inspecting technique in MC produces suspicion esteems amid re-enactment. It sections the suspicion's likelihood conveyance into covering interims. These interims havea level with likelihood and from in that, the recreation can create arbitrary esteems as indicated by the related likelihood dispersion of the interim. These qualities as chose by the re-enactment shape the hypercube test. It is upon the client to determine the example estimate to control the number of interims in that. This Latin hypercube demonstrate is more dependable than the custom MC in creating arbitrary examples as the full scope of likelihood circulations is examined all the more reliable and all the more uniformly. In addition, it has been exhibited as requiring fewer model cycles to achieve the coveted variable dissemination than the customary MC technique. The whole scope of every factor is secured by it. With respect to comes about in this way acquired, lists of vulnerability and of affectability would be created that identify with the impacts of information demonstrate predictions. To determine the most incessant and greatest classes from display recreations, the hypercube show gives the office of ordering the recurrence circulations f display state factors.

Along these lines, Monte Carlo is utilized to remove a likelihood thickness work, and the outcomes are broke down to find the best match as relating to the class and qualities of the PSA as per the judgment of the investigator. Affectability investigation engages the structure through characterizing the confinements of suppositions in a way whereby the clients can gauge the effect of movements in the qualities.

4.7.4.1 Affectability Analysis

It accommodates surveying the effect of transforming at least one key factor on the PSA venture results. Accordingly, affectability examination is an estimation ofthe monetary effect that outcomes from elective estimations of dubious factors that influence the operation and support of a PSA structure. Albeit one presumption is by and large changed at once, however, affectability investigation accommodates checking the effect of switches simultaneously in different factors as well, consequently accommodating a situation examination portrayal. In situations where the forecasts can render additional vulnerability due to lack of accurate and relevant information, Monte Carlo can be deployed to create the related arrangements. Such examinations can be used to adapt the parameters for the forecasts.

4.8 *Estimation of Economic execution in the WLCC*

The last examination of the set-up is critical for assessing the lifecycle costs. It acts as choice basic leadership instrument for the securing and establishment of the CCTV frameworks, accordingly the qualities which were gotten quite recently furnished the examiner with the data that the establishment of the CCTV camera would end up being financially practical. While, with regards to this present reality this data is very insufficient, and not sufficiently pertinent, because of the way that every one of the choices accessible to the firm is not being looked at.

Bracco et.al, (2014) expressed that the use of the financial execution markers close to the costs underlines the data that is needed for assessing the options. Life cycle cost investigation underpins the data that is required for the evaluation of the options. Many strategies for assessing these are available. However, benchmarking and KPIs can be used, with the researcher also duly assessing thesuitability of the diverse options available regarding the life cycle costs.

4.8.1 Standard monetary execution measures

The needed crux here is the achievement of robust hierarchical control over the CCTV resources. Hence, the authoritative execution stays as the focus, to assess what are the security points inside the organization, and how are they being vulnerable, with ways to address and generate measures to mitigate these.

Be that as it may, the administration should gather more top to bottom data for discovering answers for the issues;generally, this could turn into a noteworthy wellspring of worry for the association in the more drawn out run. Besides, through figuring out what really has been occurring, the administration of the association could essentially decide with a lot of assurance, and also conviction whether the things are going admirably inside the association or not, however on the off chance that the things are going on according to the arrangement, at that point whether the association might want to go ahead with a similar methodology, or still might want to roll out a few improvements. While, then again if the association confirms that the consequences of the executive administration are not sufficiently steady, and there are some real issues with the execution, at that point all things considered the administration of the association can make some genuine strides keeping in mind the end goal to determine the circumstance. In this way, with regards to the entire life cycle cost examination the estimation of the execution of the firm, could assume a huge part in furnishing the administration with the data in regards to the last after-effects of the investigation, which his to a great degree gainful for the administration to take the choice whether to go ahead with the task, or select the following best option.

4.8.2 Basic and reduced payback

Basic and additionally the reduced payback are tools that can be used to estimate the time it takes for the recovery of initial investment. This can help in deciding the level of investment that is justified.

Accordingly, when it happens to the entire life cycle cost investigation there exists a noteworthy issue between both the basic and in addition the marked down payback, as a noteworthy inadequacy exists where both the techniques are not equipped for making a correlation between the fundamentally unrelated, and all the more imperatively numerous speculation choices Furthermore, these measures are likewise not fit for allotting positions to the options which are available in front of the firm, thus the firm can't separate and break down various choices, because of which both these measures are not being used by firms where there are more than two choices accessible before the firm, with regards to making the venture for the CCTV frameworks.

4.8.3 Net reserve funds

Net reserve funds help in the count of the net measure of the venture made by the firm, it fundamentally gives the vale in the present esteem pounds, which is the choice of speculation that is assumed control over the financial administration life of a physical security resource. The net funds from a task are generally communicated as far as PV, it exhibits a delineation of the reserve funds, which could either be above or at times finished the sum which would come back from the underlying speculation made by the firm, at the reduced rate. Consequently, the estimation of net reserve funds for a venture is done through utilizing the equation given beneath.

$$\mathbf{NCC = LCC_{Base\ Case} - LCC_{Alternative\ Case}}$$

Nundy et.al, (2014) expressed that till the time the estimation of the net reserve funds stays to be higher than zero, at that point all things considered the speculation that is practical and worthy of attention. The connection between the lifecycle costs and the reserve funds direct towards the funds those are potentially available to be invested. Both the funds and the costs can then be matched.

4.8.4 Reserve funds to speculation proportion

It is the fund made available to the organization for the venture and helps connect the speculation costs. With regards to the life cycle cost examination the SIR fills in as a basic component in the basic leadership for buying physical security resources, thus, when there is an expansion in the underlying costs, it thusly brings about expanding the general operational cost. Thus, SIR could be cleared for monetary execution, for example, the net reserve funds, particularly due to the reality, there has to be made a base case for determining relationships between the choices.

An SIR return that exceeds 1 is practical for giving a monetary legitimization with regards to the appraisal of the option (Leontief, 1937). In any case, a noteworthy contrast is there between the net funds and the SIR – as the lower estimation of the cost. SIR must not be used by merchants, but should rather be used by diverse sellers.

4.8.5 The inward rate of return

This is the discount rate that makes all netflows to present value equal to zero, and hence is the embedded return in a project. It is a marked down rate without bounds end up plainly like that of the underlying speculation (Magni, 2013), in basic words it could likewise be alluded to as earn back the original investment purpose of the venture.

It is used to assess the practicality and commerciality aspect of an investment and must be calculated according to assumptions before the investment is made.

Patrick et.al, (2016) opined that it should be higher than the cost of capital for it to be considered worthy of execution. It is especially true in case of hard capital rationing when the amount of investment funds is heavily constrained. Thus, internal rate of return is a profoundly helpful apparatus for the partnership hoping to lead an examination of the capital ventures, alongside that it is additionally utilized by the enterprise for the assessment of the stock buyback programs, in this way, considering the present situation where the association has dispensed a generous measure of the stock buyback, at that point this investigation furnishes the association with data that provides a higher return as a vastly improved choice, as opposed to putting resources into different assets.

The recipe for IRR is:

$$\sum_{t=0}^{n} \frac{A}{(1+d)^1} = 0$$

Interior rate of return is very basic for the organizations hoping to procure physical security resources like the CCTV Systems, because of the way that it empowers the administration of the association to rank the general ventures or the undertakings in light of the rates of return of the task at hand. There are some drawbacks including the fact that it can lead to thechoice of a smaller profitable investment over and above a better larger one because the magnitude is not measured. Moreover, it can lead to multiple and even negative rates of return if the direction of the cash flows switches over the timeframe of the investment.

4.8.6 The balanced inward rate of return

This is the annual yield over the administration life of the resource. The balanced interior rate of return is e-strategy which has been utilized by firms for the count of the base worthy rate of return over the capital contributed; which is fundamentally the most minimal measure of the income that is thought to be adequate by the firm to undertake a particular buy or task. The base satisfactory rate of return is normally same as that of the cost of capital, alongside that it likewise adds the arrival to the aggregate esteem, now and again or venture it is additionally alluded to as the obstacle rate.

If the rate is higher than the cost of capital, it should be invested in and vice versa. Notwithstanding, in the event that the balanced inside rate of return is same as that of the reduced rate than it is said to achieve earn back the original investment, which makes it temperate nonpartisan.

If the re-speculation of the reserve funds leads to a higher rate, then the rate of return being considered cannot be put back into the past modeling, as the decision would already have been made, and the firm should look at incremental benefits and costs related to the future for making the judgement call regarding additional spend.

Also included in the limitations here is the need for making assumptions regarding the speculation and in addition the sparing streams that are comparable to that of the inner rate of return. The following formula that can be used for estimating the adjusted interior rate of return:

$$\frac{\sum_{t=0}^{n} St\,(1+r)^{N-1}}{(1+i)^{N}} - \frac{\sum_{t=0}^{n} \Delta I_t}{(1+r)^{t}} = 0$$

As

St = Cashflows inwards as resulting from savings that can be reinvested.

R = rate of re-investment available,

$\Delta I_{t/(1+r)^t}$ = This is the present esteem venture costs, in light of which the aggregate return must be boosted.

4.8.7 Net terminal esteem

This is an estimate of the returns from the CCTV framework near the end of its life. The equation is:

$$NTV = A_1 (1+r)^{n-1} + A_2 (1=r)^{n-2} \ldots.. + A_n - C (1=r)^n$$

Whereas the calculation of the net present esteems rebated in reverse with the prevailing estimation, the net terminal esteem makes it in consonance with the administrative life of the assets.

4.8.8 The advantage to cost proportion

This measure helps to equate the benefits and costs associated, through factoring in the conceivable expenses, and additionally the advantages, it contemplates both the subjective and also the quantitative expenses, for securing the new CCTV frameworks, of arranging off or supplanting the old CCTV frameworks. The proportion is used for the estimation of both the subjective and in addition the quantitative components, however, at times the expenses, and also the advantages are difficult to gauge solely in money-related terms. Along these lines, whenever conceivable it is fundamental to make an interpretation of the subjective elements into quantified form as then the outcome is more useful. This measure helps compare and contrast options regarding their benefits and costs. The higher the proportion, the better it is. Discounting is carried out to find the present values of both the inflows and the outflows.

In any case, the long haul advantage to cost proportions like the ones happening because of the climatic changes is very touchy to the marked down rate, with regards to the count of the net present esteems. Along, with that in different conditions, there are entirely agreements inside the association, in the matter of what should be considered as the real rate of estimation, and of cost proportion. Other issues emerge with regards to the treatment of the non-money related impacts, as they are connected with the cost through evaluating the financial terms, using the eagerness to pay, which are very perplexing and in the meantime hard to survey. At long last, another real intricacy related with the advantage to cost proportion is connected with the exact meaning of the expenses and in addition the advantages, which could be flexed according to the financial plans regarding the CCTV framework.

CHAPTER 5. MODELING THE WHOLE LIFE CYCLE COST FOR PHYSICAL SECURITY ASSETS

5.1 Introduction

The chapter charts the evolution of life cycle cost (LCC) to apply to the PSAs. In the first segment, different cost centres are expounded on regarding the cost processes taken up. Then onwards, the WLCC process is considered for evaluating the economic costs and benefits for CCTV products. Finally, the last section discusses the present value appraisal method and the sensitivity analysis for identifying the risk and uncertainty of PSAs such as CCTV cameras.

Strategy and approach can get drastically misaligned in case the estimation and modeling process does not factor in the associated risks and uncertainties. Decision support systems can be deployed here. The field of costing traditionally has been heavily geared towards costs that are generated inside the organization, with a view to controlling the expenses.

5.1.1 What Does Cost Mean?

Costs start getting generated even well before the management has decided on whether or not to procure an asset. Commitment stage is critical to cost control. Although the awareness is quite universal, cases abound where there is a lack of due care exercised by management in this sphere. The US Department of Defence employed LCC in the 1960s, whereas it was adopted in Japan too right after WWII. For the Japanese recover from the disastrous results of WWII, cost control at earlier stages was far more important than at operational phases. Oddly, many firms still treat cost management as a reactionary measure, thereby missing out on significant savings from the beginning. The proactive paradigm is far more useful and productive than the reactionary one as the latter considers it to be an expense rather than as an investment. Hence, the general results in many cases can be seen that atthe design stage, critical factors are missed out due to reactionary rather than a proactive approach to cost management.

5.1.2 Value Proposition

Value can be articulated as the level of satisfaction resulting from resources used. It is directly proportional to the quality and inversely proportional to the costs involved. Thus, organizations that strive for high value have to focus on both the quality and cost aspects. However, Economic Value Added concept bypasses this holistic picture, as being reflected through the deployment of traditional cost measures. Hence, for an effective and efficient cost management regime, the design process must accommodate strategies that are focused upon value-creation. This has to be accompanied by a suitable adaptation in culture as well.

5.1.3 Defining Cost in the Present Study

For simplification purposes, expense and cost are terms that are used together, but a clear difference does exist. The expense is reflective of the capacity provided for a task, whereas cost shows consumption relating to a job demand. The WLCC views that it should reflect a cost consumption angle, but regardless many LCC models adopt an expense model.

However, the cash flow models get their needed attention and focus when revenues are connected to the investment in the assets directly. Time value of money must also be provided for, and also the opportunity costs associated with the cashflows in question. For PSA, real and financial investments have to be treated separately, as in the case of real assets, there's a preset life, and hence the assets have to be duly depreciated over the lifetime. Real assets valuation is termed "economic valuation", and is very useful in decision-making due to the use of economic analysis.

Environmental impact can also be considered through the use of Environmental costing whereby the various principles of costing into those of lifecycle and traditional costing is applied, as being for the PSAs.

- For the entire stages, from design, procurement to maintenance, the sundry associated costs are included.
- The amortised annual cost of a PSA for the various stages.
- The attributable costs of the PSAs.

Costs can be classified under different systems, with acquisition and operation costs being two of them. In the case of the life cycle costs, there are four types further – liability, hidden, usual and the less tangible. Traditional costing approach in these cases has been criticised for focusing too much on the aspect of cost control and not on value. Hidden costs are also included, whereby the regulatory and other non-conventional costs come into the fray. When future liabilities are not managed well, the liability costs occur, for example, due to clean-up when there is non-compliance with the rules.

Some relevant examples related to PSAs are the legal fees, fines, customer and employee injury claims, and property loss or damage therewith. Less tangible costs then come into consideration. The brand image and relationship costs are much hard to quantify but are nevertheless critical.

5.2 *Asset Management*

Asset management involves planning and monitoring of the PSAs. Adequate management of PSAs demands a high level of interest from the organization, as well as an increased maintenance need for the time the asset is with the company being in its use. As PSAis so important, afair amount of resources need to be allocated therewith. Therefore, an aim is to achieve the best-cost solution at initiation, implementation, the maintenance and other phases. Regulations have to be duly considered too.

Physical asset management is a long-term asset that requires capital budgeting process (Hastings, 2010), and here it gets distinguishable from a current asset in that the utility from the assets accrue to a firm for longer than one year. The life of the assets depends on many factors, which can be decided upon and designed for at the initial stages. According to the relevant accounting standards, being the IFRSs and the US GAAP, the costs spent on the capital acquisition of the assets have to be capitalised and depreciated over the useful economic lives of the assets. This is to apply the matching concept whereby the expenses for generating the revenues are matched. The concept of prudence dictates that appreciation of the asset, in terms of valuing it up cannot be done, although write-downs are required when the assets lose their utility at a quicker pace than initially had been anticipated.

Whole lifecycle costing has gained considerable importance and recognition in recent times. Thus, there are the prevalent examples of practitioners and academics deploying WLCC for assessing theoperational and economic efficiency of assets such as CCTV systems. Furthermore, the concept of WLCC can also be used to gauge the options according to the different avenues available. KPIs through stochastic modeling can be used, and related revenue impact needs to be incorporated to identify and evaluate the true economic impact of the investment.

WLCC aids the management in responding to the weaknesses and vulnerabilities pertaining to time period specification and also helps in analyzing the economic impact of PSAs like CCTV for the entire life of the assets (Boussabaine and Kirkham, 2005). Hence, WLCC can be effectively deployed for acquisition and disposition decisions regarding the PSAs.

Assumptions and estimates regarding the future costs associated with operating and maintenance of the assets have a large bearing on WLCC per Ristimäki etc. (2013). WLCC use has to be seen in the context of appropriate risk modeling. However, this fact should not deter management from making estimates and assumptions as this is required in any modeling work to be undertaken. The estimates rarely in any dimension turn out to be totally accurate but nevertheless have to be made for planning purposes.

Analysts and the management of firms have frequently used life-cycle costing as a decision-making tool to select the best supplier of PSAs. The author proposes that it should be used for assessing PSA investments, such as in for systems used in CCTV. A critical aim here is that it is not sought the managers would be equipped with a single figure for the WLCC under question but rather given different models that depict the modalities of various cost elements, along with their risk elements that the managers have for their specific PSAs under consideration. Thus, in other words, the present author suggests the use of WLCC for whole life cycle costing for all the phases associated with CCTV systems.

An issue with the conventional handling of WLCC is the preponderance given to numerical values, which in themselves, do not necessarily equip the managers with all the information regarding decision-making process. Therefore, in this study, basic economic performance measures would be used too to enable the analysts and managers must consider the variations and uncertainties inherent. Korpi and Ala-Risku (2008) assert that many firms are using WLCC without adequate consideration for the uncertainties in the longer term, however, this being related to the forecasting model innately.

5.3 *Determining LCC while Considering Risk*

In this thesis, the life cycle costing of security systems (CCTV) is organized into four categories: initial capital cost, replacement cost, maintenance cost, and operation cost. The latter also contains utility and electricity costs. Figure 5.1 represents the life cycle costing organizational structure for security.

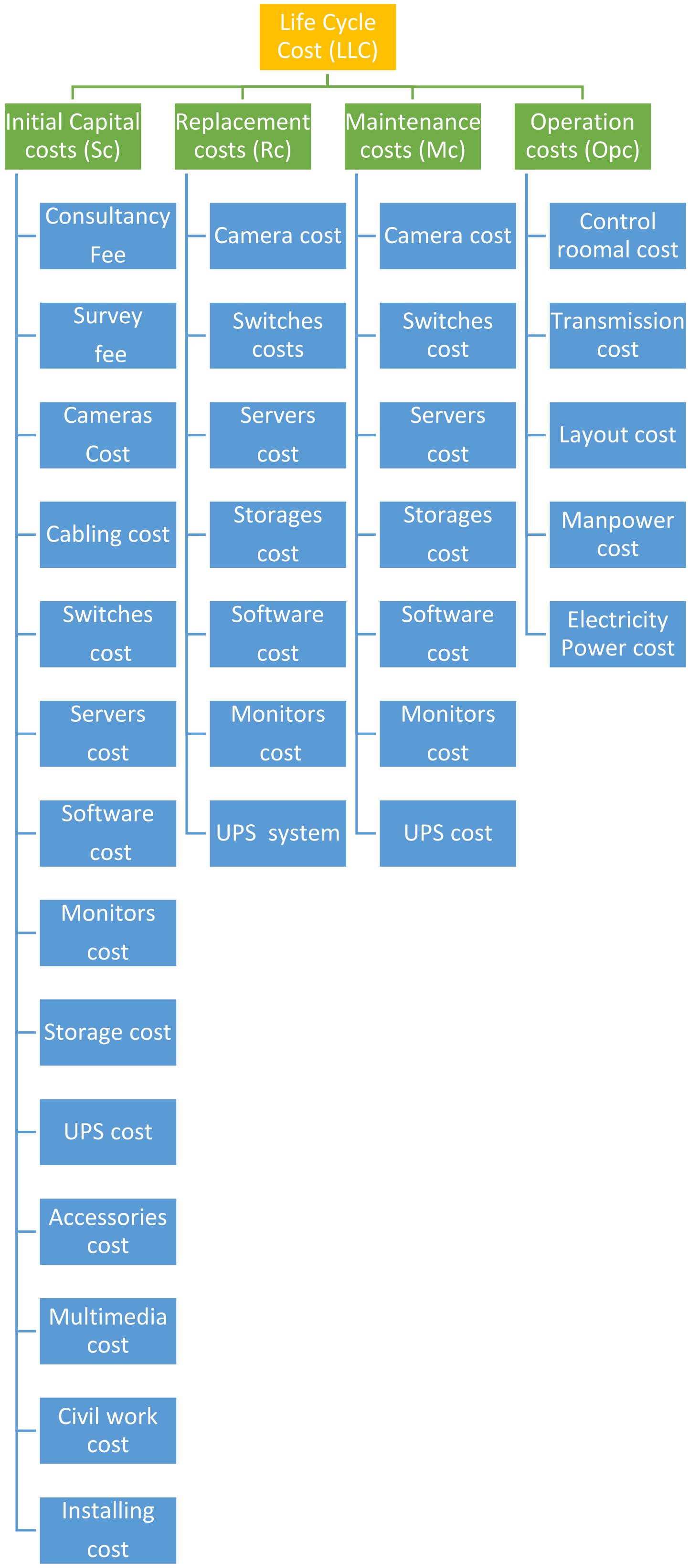


Figure 5-1: Organizational structure of security systems' life cycle costs.

The above classification serves to predict and manage the total security system costs while analysing the cost of the product lifecycle, the types of costs defined, and the identified risk factors that may impact the final value of the cost, causing the growth. During the cost analysis, one determines the value of the cost and the size of the impact of risks factors on costs in the above categories.

Using the input probability distributions for each cost item, the annual forecasted cost (present value) is calculated in an Excel spreadsheet for a period of 10 years. This period of time has been selected based on the replacement costs of the CCTV components.

Each cost element is treated stochastically and the cost flow (PV) for each year is described as PDF. These PV cost profiles are considered to be variable from one year to another depending on the discount interest rates.

An appropriate discount and inflation rate are used in this study. Since the cash flow profile of each type of cost is known or can be stimulated, the annual PV of security cost can be estimated using the following equation:

$$PV_i = S_C + \sum_{i=1}^{n} \frac{R_C +}{(}$$

Where: $S_C = initial\ capital\ costs, R_c = replacement\ costs,\ M_c = maintenance\ costs,$ $O_{pc} = operation\ costs, r = discount\ rate, and\ n = number\ of\ years\ (time)$

The following sections describe the security system (CCTV) cost parameters and functions assumed in this life cycle cost (LCC) calculation.

5.3.1 Initiation Capital Cost (S_C)

This pertains to the cost incurred by the firm at the time of initiation of a PSA project. The survey needs to be carried out before the acquisition, where the systems have to be put up. Control room location also needs to be determined. User perceptions should be fully taken into account. Experts could be used in this, as they will independently check and validate, plus also giving their opinion on the assumptions and the judgments of the owners. Contractor costs must also be included here.

In the present study, the initial capital costs are the total initial setup costs for the security system (CCTV) over its total life, and they are assumed to be fixed and include cost items such as cameras, switches, servers, storage, software, monitors, UPS tracking systems, and consultancy fees. The amount of the total cost is adjusted adding a percentage of risk factors. These factors are initialization risk (Ri), implementation risk (Rm), and acquisition risk (Ra). The equation for the initial capital costs after the adjusted risk is as follows:

$$S_C = S_C + S_C * R_i + S_C * R_m + S_{C\square} * R_a$$

5.3.2 Replacement Costs ($\boldsymbol{R_C}$)

The replacement cost (R_C) includes cost items such as cameras, switches, servers, storage, software, monitors, and UPS systems. These costs are applied during the end-of-life year proposed by the manufacturer/supplier for each aforementioned item. Over the period of time in this LCC model, the costs are applied every 10years.

5.3.3 Maintenance Costs (M_C)

The maintenance costs (M_C) are annual recurring costs, and each of them is a percentage of the initial cost. In the present cost calculation, the first three years are zero cost, and then a cumulative 1% is added for each year until the 10thyear. After that, the maintenance cost starts from the beginning with the same cost as in the fourth year, adding 1% per year.

5.3.4 Operational Costs (O_{PC})

The operational costs (O_{PC}) are annual recurring costs, and each of them is a percentage of the operational cost adding an amount of operational risk. Operational costs include cost items such as control room cost, transmission cost, layout cost, manpower cost, and electricity and power cost. These costs are applied every year during the project life cycle. The associations between operational costs and risk factors are presented in the following table.

Variables	Cost Items	Risk Operational Factors
Cr	Control room cost	Roo
Tc	Transmission cost	Roo
Lc	Layout cost	Roo
Ma	Manpower cost	----
Ec	Electricity power cost	Rosy

Table 5-1: Operational cost items with risk operational factors

The following equations are used to determine the yearly operational costs.

$$O_{pc} = \sum_{i=1}^{n} O_{cri} + O_{Tci} + O_{Lci} + O_{Mai} + O_{Eci}$$

Where: $O_{cr} = Operational\ control\ room\ cost,\ O_{Tc} = Operational\ transmission\ cost,$ $O_{Lc} = Operational\ layout\ cost,\ O_{Ma} = Operational\ manpower\ cost,\ O_{Ec} =$ $Operational\ electricity\ cost, n = number\ of\ years.$

Each above operational cost is presented in the following equations with an inflation rate of r=5%.

Operational control room cost:

$$O_{cri} = (O_{cr} + O_{cr} * R_{oo}) + \sum_{i=2}^{n} Ocr_{i-1} + (Ocr_{i-1} * r)$$

Operational transmission cost:

$$O_{Tci} = (O_{Tc} + O_{Tc} * R_{oo}) + \sum_{i=2}^{n} O_{Tci-1} + (O_{Tci-1} * r)$$

Operational layout cost:

$$O_{Lci} = (O_{Lc} + O_{Lc} * R_{oo}) + \sum_{i=2}^{n} O_{Lci-1} + (O_{Lci-1} * r)$$

Operational manpower cost:

$$O_{Mai} = (O_{Ma}) + \sum_{i=2}^{n} O_{Mai-1} + (O_{Mai-1} * r)$$

Operational electricity cost:

$$O_{Eci} = (O_{Ec} + O_{Ec} * R_{osy}) + \sum_{i=2}^{n} O_{Eci-1} + (O_{Eci-1} * r)$$

Installation of a new CCTV system is the relevant cost here and includes cameras, monitors, brackets, and pole mounts, as well as the control room and hiring staff or training them. This must be included in the budget, with the importance that the buyer must appreciate the industry norms and different offers from vendors before committing the firm. The organization can also opt for installation of the CCTV systems by the vendors in many cases, and it can also be assured that system is functioning adequately. Downtime chances can be minimized ifthe installation is done with due care, with the ideal scenario being the vendor to install the CCTV itself.

$$WLCC_{im} = C_{im} + \sum_{t=0}^{n} \frac{C_{im}}{(1+d)^t}$$

Where $WLCC_{im}$denotes the complete costs of the PSA. Discounting would be needed here as the costs are to be paid during the life of the project too.

Operational costs are linked to the daily administration and maintenance of the PSAs. They represent a component of the operating income, which is why they are present in firms' income statements. On the other hand, maintenance costs are incurred by a business to keep its PSAs operating well. This would include the service costs of the equipment to keep it in optimal condition. Surveillance and other factors need to be factored in, such as traffic, objects, or individuals, per Dadashi, Stedmon, and Pridmore (2013).

Complete and fully systematic assessments are required regardingthe resolution of problems in case of the surveillance systems (Malmenbratt and Brooks, 2015). The operational needs of the CCTV system, along with the insurance thereof can be worked on and managed well through this. Here, it is critical that the management factors in the various advantages of the CCTV systems in order to conduct the right cost-benefit analysis.

Code of Practice and an Operating Manual must be drafted for the CCTV systems (Chen, Wu, and Hsieh, 2013). This articulates a robust internal control system and would help the users get adept at maintaining and making use of the system. Crucial tips must be included to help the operators, with due recognition of the level of authority and accountability. This will serve as a point of reference while brand management can also be worked upon, along with the structure of the control room, and matters regarding staffing levels and competencies.

5.4 PSA WLCC Risk Analysis

Decision-making is facilitated through adequate risk management practices. It factors in all elements from the beginning, incorporating various scenarios and associated outcomes to be fed into the model. So, the analyst also has to consider what would happen in case the

PSA does not function as scheduled. The judgment and experience of the analyst would be very useful, and the best solution has to be sought rather than adopting any other one that looks good. Regarding application to PSA, the conventional risk management systems as adopted in many firms fail the purpose due to their inherent inadequacies. However, formal models can be quite costly and prohibitive too. Here, it pins down to the judgment of the analyst to make use of various methods, for making the appropriate choice given the circumstances.

The categories included in this domain are deterministic, qualitative or quantitative. In the case of deterministic techniques,

$$WLCC = C_p + \sum_{t=0}^{n} \frac{C_t}{(1+d)^t}$$

Whereby, WLL includes all the present values of the related costs, including C_p which is the capital costs and of installation, C_t being the whole lifecycle costs net of the accrued cash flow benefits. D stands for the cost of capital, being the opportunity cost element. In this study, Quantitative techniques have been used, but the other two approaches have also been discussed.

.

5.4.1 Qualitative Risk Analysis

In this study, instead of being expressed in quantitative terms, the likelihood of an outcome is articulated ina quantitative manner, expressed in qualitative terms. Probability is not used here. At the start, qualitative measures are adopted, which are later converted into quantitative ones. This approach enables a valid initial check on the risks from a wider angle.

5.4.2 Risk Matrices, Risk Registers, and Other Tools

Such a risk matrix would delineate the various risk levels and financial impact on the project thereof. It helps in prioritizing risk. These are dynamic tools, which are to be updated continually as the PSA progresses through its life. Legal issues, of contingency, of environmental factors etc, have to be included therein. The matrix identifies the intensity and also the likelihood of the event happening, from which the users can derive the adequate and appropriate risk management response.

The risk registers also help in controlling the identified risk elements, with due importance given to the most pressing ones, such as for breakdown of the system. Lack of monitoring or a major exception occurring. This provides the users with a tool to chart out the extent and likelihood of the related risks and helps in determining the responses which can be standardised and put into the operating manual.

Diagrams help depict the flow, with arrows and nodes showing the sundry PSA phases. It triggers better thinking approach in the analyst regarding how to manage the uncertainties therein. This must also be kept updated for better utility, employing complex formal diagrams and symbols showing connectivity of different variables.

A SWOT analysis would include taking stock of the landscape to ascertain the related strengths, weaknesses, opportunities and threats the system has. Strengths have to be put to use whereas the weaknesses have to be protected against. Opportunities have to be exploited, and the threats have to be mitigated in an effective and efficient manner.

5.4.3 Quantitative Analysis

Statistical techniques are used which can then be categorized into statistical and other methods. Descriptive statistics can be used in order to articulate the level and extent of the risks identified, with NPV showing the practicality of the investment. The probabilistic approach is the most relevant as it is embedded into the theme of risk management.

5.4.4 Probabilistic Approach

Probability use has spiraled in use since the proliferation of risk quantification packages (Lorance and Welding, 1999). Accurate modeling is vital to theproper execution of Monte Carlo simulation. Historical data may not be of much use here especially when the dynamics of security have changed. Similarly, when the data is available, the construction of valid probabilistic distribution can pose issues. However, a way around it is to create a histogram, and then check for distribution measures, which will then lead to the specific type of distribution as identified. The assumptions regarding stochastic factors for the WLCC, and data analysis regime become critical in this respect. It has been observed that simulation errors can generally be traced to inaccurate parameter allocations regarding the choice of identified specific distribution as it was considered to be reflective of the data.

Simulation can be carried out, leading to the following WLCC equation:

$$f(PV) = f(C_p) + \sum_{t=0}^{n} \frac{f(Cti)}{\{1 + f(d)\}^t}$$

f(PV) signifies the probability density function of the total PSA WLCC in present value terms

f (Cti) is the probability distribution of whole life cost element of a segment *i* in period *t*, and includes the capital costs and future costs; *t* is the numbers of years relating to the PSA investment in its entirety

f(d) is the probability distribution of the discount rate to adjust the cash flows to the present values;

and, $f(C_p)$ is the probability distribution of the initial capital cost of the PSA.

When data is available and stochastic models are used include trace-driven simulations, empirical distributions, and theoretical distributions, per Maio et al. (2000). Frequency histograms can be plotted and result in input into the simulation model. A good fit model has the advantage of catering for extreme values too.

5.5 *Development of the WLCC Model*

A chain of interconnected processes is to be considered where assumptions need to be made and in the following figure. Cost data are calculated and presented in the previous chapter 5. For the risk data analysis, chapter 7 presents a risk model and risk factor analysis, defining the PDF's risk distributions.

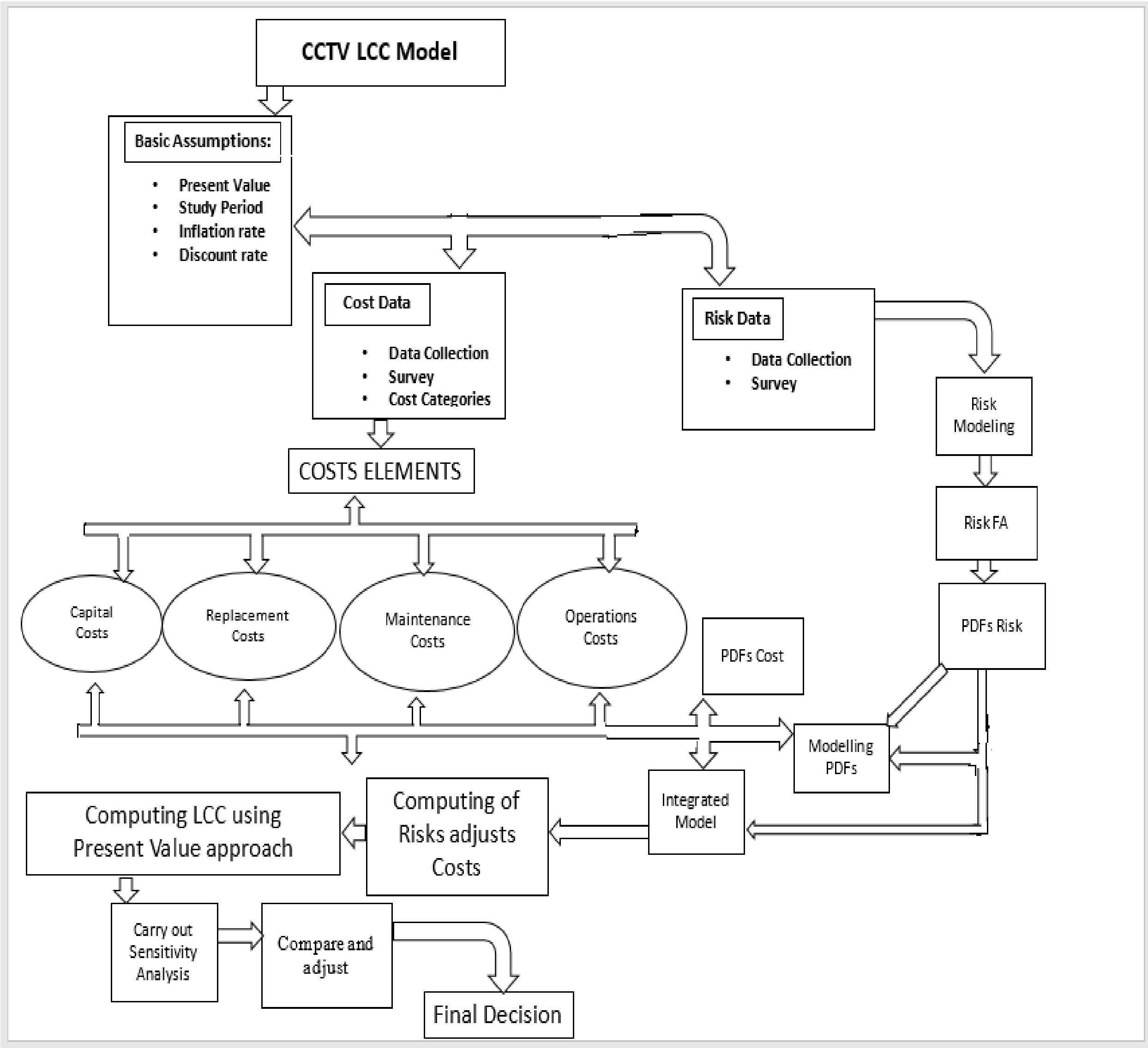


Figure 5-2: WLCC model development process

Following are the steps:

- Identification, manipulation, and adjustment of cost assumptions
- Computation and risk adjustment of LCC cost centers.
- The simulated annual forecast presents the obtained values,
- Forecasts to be modeled as input probability distributions to simulate the WLCC model.
- Specific economic performance measurement parameters are established
- Sensitivity analysis was done
- Comparison carried out and final evaluation of decision

An appropriate discount rate to be used is the firm's cost of capital. Iteratively, the cash flows are obtained and discounted to the present value, as churned out by the simulation software against the distribution fit input. The steps are discussed in detail below.

5.5.1 Sensitivity Analysis

In order to ascertain and validate the theoretical probability distribution for the various segments, sensitivity analysis is carried out In the Monte Carlo simulation, the various risks and the related assumptions are factored in and result in different spreads of the present values therewith. The simulation has the advantage of providing for prioritising of risks through identifying the various elements with their related impacts on the results. Correlated assumptions, however, can render this exercise not that useful. Also, it can happen when the assumptions therewith are not monotonic, and hence a change in assumptions does not carry a related change in the forecasts.

The model eventually shows summation of the present values of all the related costs. Here, the discount rate used for the cash flows can have a large bearing, and thus the calculations can provide for the results under various rates of discount. The discount rates are considered to be normally distributed. The analyst can then decide on the viability of the exercise given the results.

5.5.2 Performance Measurement in the PSA WLCC Model

Impact of the WLCC outputs has to be a tie with the economic performance indicators. The exercise can be carried out through making a cumulative distribution of the associated cost flows and then by comparing with the PSA costs across various entities. Benchmarking would add value to this exercise, with analysis needed to ascertain the reasons for the cost differentials, thereby providing the managers with valuable input regarding the acquisition, maintenance, and operation of the PSAs.

.

5.5.3 Updating the PSA WLCC Model

The WLCC model should be updated annually at least, with factoring in for the relevant developments and technological changes, in order to keep it relevant. The analyst can employ performance indicators to be aware and incorporate the changes needed.

5.6 Summary

This chapter has presented the LCC model cost with a robust method of modeling the input probability distribution assumptions. The WLCC model brings together the service life costs for PSAs such as CCTV cameras. A systematic procedure was adopted to transform the input probabilities (PDF) into useful assumptions for the simulated model. These were then used to simulate the present value cost for the CCTV cameras over a period of 10 years. The sensitivity analysis was assessed and then the results were used to forecast the final WLCC output probability distribution.

CHAPTER 6. RESEARCH DESIGN AND METHODOLOGY

6.1 *Introduction*

Research could simply be explained as the process which investigates a certain hypothesis, suggests anew interpretation of data, and finally, it posesa new set of questions which could be explored by future researchers, to explain the topic in-depth. Garner and Scott, (2013) explained research as a systematic investigation conducted for studying the sources, and material with the aim of establishing certain facts and reachinga new set of conclusions. The purpose of this study is to determine an ideal mechanism, which could aid the process of risk modelling of the PSAs so as to aid in development and operation for high-value UAE retailers. However, before selecting a research method for the collection of data for the study, it is essential to develop a research design which could facilitate the overall research process, and enable the researcher to achieve the overall research objectives.

Hence, this chapter of the study starts by providing an overview of the theoretical approach which would be utilized by the researcher while conducting this study. Thus, the researcher will begin with the research philosophy which will be adopted for the study; next the researcher will provide an overview of the research methodology, research approach, research instrument which will be used for conducting the research, along with the data collection and data analysis techniques which would be used by the researcher to determine the overall research outcomes.

6.2 *Research Philosophy*

While conducting a research study the researcher might possessa varied level of beliefs when it comes to the collection of knowledge regarding the study. This belief of the researcher could eventually have an impact on the creation and interpretation of the knowledge (Saunders, and Lewis, 2014). Research philosophy is critical for any research and it is important for the researcher to make sure that relevant research philosophy is used for data analysis. In this research, the researcher has specifically focused upon identifying a correct research philosophy hence all three research philosophies are given below as it helps in providing information with regards to each of these techniques and how they can be successfully utilized by the researcher.

6.2.1 Epistemology

Epistemology could simply be explained as the method used by the research to acquire knowledge regarding a certain phenomenon. It helps the researcher in finding the answers to the questions like, how do we go to know about a certain phenomenon? Hence, epistemology is composed of nature of concepts, the manner in which those concepts are constructed, validation of the senses, and more importantly logical reasoning (Bryant, 2016). Thus, epistemology is more concerns regarding how our minds are linked to reality, and whether these relationships are valid or not. Hence, epistemology enabled the researchers to provide an explanation of how we think; it allows the researcher to determine the truth regarding a certain phenomenon, through the utilization of an effective evaluation method. Furthermore, it is essential as it helps the researcher in gaining knowledge regarding the world around us, and without epistemology, we would not be able to think. Additionally, we might not have a reason to believe in the fact that our thinking was neither correct nor productive, as opposed to some of the random images flashing infront of our mind.

6.2.2 Ontology

Ontology could simply be referred to as the philosophical knowledge of nature of being, existence, or reality. Along, with that, it could also be referred to as the basic categories of being, and their relations. Hence, this philosophy concentrates more towards the view of the researcher towards nature of existence of knowledge among the social entities (Ritchie et.al, 2013). It further enables the researcher to determine how an individual could develop an understanding regarding the existence of a certain phenomenon, and how the nature of that phenomenon's existence could have an impact over the perception of the knowledge creation. Through adoption of ontology philosophy, the researcher can establish a solid ground to subjectivism, and the researcher could create a design for their research process based on the ontological knowledge.

6.2.3 Axiology

The philosophy of axiology basically deals with the explanation of the value which a researcher process while conducting a research. These values might include the personal values possessed by the researcher, and ethical values, both of could have an influence over the decision making process during a research, furthermore, it could also have an impact over the manner in which the data is collected and the results of the study are interpreted by the researcher. In case there are certain personal values which a researcher holds more close to him or herself than it would prove to be difficult for the researcher to determine conclusive evidence regarding a certain phenomenon (Creswell, 2013).

Hence, for this study the process of identification, as well as thedetermination of the risks to the PSA development and operation needed. Hence, for this study, the philosophy of axiology will prove to be more suitable, as it will enable the researcher to conduct a researcher in a manner which would not be hindered by the personal values possessed by the researcher, neither the ethical values will hinder the overall progress of the research. In this research, the researcher has successfully used axiology as a research philosophy as this technique seems to be an ideal fit for this research project.

6.3 *Research Paradigm*

Stingone et.al, (2016) explained research paradigm, as the example or the patent consisting of self-contained, simplified, and small examples, which are used for the illustration of the theoretical facts, and processes. In another study by Moreton-Robinson, (2016) research paradigm was explained as the world view, a strategy of breaking down the complexity of the real world. Hence, it could be stated that research paradigm is an interpretative framework, which is specifically guided by a certain set of beliefs possessed by the researcher regarding the world, and the manner in which it should be studied and understood. There are three basic researcher paradigms which are applicable to this research study are (i) Positivism; (ii) Realism, and (iii) Interpretivism.

6.3.1 Positivism

Positivism holds the view that the only knowledge which is highly authentic is the scientific knowledge, and it further stated that such sort of knowledge could only come through the positive affirmation of the theories which are formed through the scientific method these are basically the techniques used for conducting investigations of the phenomenon based on gathering of measurable, empirical, and the observable evidence (Halfpenny, 2014). Hence, in the epistemological sense, positivism indicates towards an objective approach towards the study of humanity which is quite close to the natural sciences methods. Hence, as far as the current research is concerned this philosophy is quite important since the researcher is aiming to analyze the risks to the PSA throughout the life cycle.

In this research paper, the researcher has successfully utilized personal knowledge, information, and experience. This research philosophy of positivism was an ideal match for this research topic as it allowed the researcher to successfully collect information from various data sources and interpret it according to the requirements of the research topic. In this paper, the researcher has successfully collected data form research participants and used the information to form meaningful analysis with regards to the research question.

6.3.2 Realism

Realism could simply be explained as the philosophy which rests over the realist belief. It looks at a certain phenomenon which based on their knowledge, which enabled the researcher to arrive at a more realistic view. Smart, (2014) conducted a study in which they concluded that realism enabled the researchers to refer to their consciousness, and it helps them to provide a reflection over the issue based on their needs and desires. Hence, it could be stated that realism is heavily associated with the level of exposure which a researcher has regarding a certain phenomenon. However, when it comes to determine deeper knowledge regarding a certain phenomenon this approach ha prove to be inappropriate, because the knowledge collected would be quite vast and it would become impossible for the researcher to achieve the overall research objectives, hence, this approach will not be adopted by the researcher for analyzing the risks associated. This approach doesn’t seem to be a perfect technique for data collection and analysis under this research because there are concerns over its applicability within the context or area of this research.

6.3.3 Interpretivism

It is also known as the Interpretivism approach, this approach involved the researchers to interpret certain elements of the study. Hence, Interpretivism is used for integrating the human interest within the study. Goldkuhl, (2012) stated that interpretive researchers assume that the access to the reality could only be gained through various social constructs such as instruments, consciousness, and social meaning. Therefore, the development of the Interpretivism philosophy is based strictly on the critique of positivism in social sciences. It was important for the researcher to successfully collect data and analyze it by keeping under consideration views and opinions of research participants who were part of the data collection activity performed during the research. In this regard, usage of Interpretivism philosophy was essential as it allowed the researcher to accumulate and analyze information from participants and combine it with knowledge which already exists with the researcher.

6.4 *Approaches to Reasoning behind the Research Process*

In a study conducted by Creswell, (2013) it was determined that the approach adopted by the researcher towards conducting a research study is more and less determined through the manner in which the researcher conducts reasoning about the phenomenon under study. Therefore, this provides an indication towards the fact that in cases a certain process is developed by the researcher before undertaking the research, then under such circumstances, the results of the study would simply be assessed against the theory which is more close the phenomenon under study. However, in case the researcher does not possess a theory at the beginning of the research and is relying on the information which has to be gathered for the research prior to the development of the theory, then under such circumstances, the researcher should opt towards adopting a different reasoning approach. Basically, there are two types of reasoning approach which are followed by the researcher while conducting a research; both of these approaches are explained below.

6.4.1 Inductive Theory of Reasoning

Inductive reasoning moves from a specific set of observation toward much broader theories and generalizations. Inductive reasoning is also known as the bottom-up approach, as in inductive approach the researcher process initially begins through a set of specific observations and measurements. After which the researcher starts to detect certain irregularities and patterns based on which the researcher then formulates a number of tentative hypotheses which could be further explored, and the researcher finally ends up with certain theories, as well as general conclusions (Molnár et.al, 2013). Despite of the fact that inductive reasoning might sound ideal for some of the research projects, but it still might be quite complex to be applied to the current study, because of the variations involved in the retail sector of the UAE, specifically due to the particular view of scope, quality, cost, and time of the research study. This approach or theory doesn't fit into this research paper and there can be concerns with regards to applicability and usage of this technique in this research paper as there are numerous differences that might exist between data that is collected specifically for UAE market. There are factors which are able to have an impact on cost, scope and time of research study.

6.4.2 Deductive Theory of Reasoning

As compared to inductive reasoning, deductive reasoning takes a more specific approach rather than a general approach which is followed by the inductive approach. This is the reason why the deductive approach is also known as the top-down approach. Hence, in deductive reasoning the researcher initially begins with a theory regarding the topic under study, next the researcher narrows down the theory through the generation of specific hypothesis which could be tested by the researcher. Afterwards, the researcher further narrows down the focus of the study; this is the phase where the researcher collects data regarding a certain set of observations for addressing the researcher hypotheses (Evans, 201;3). Thus, this, in turn, leads towards testing of the hypotheses with the specific data which has been collected by the researcher over the researcher topic, which gives the researcher a confirmation of the original theories.

Hence, after conducting an in-depth analysis it could be concluded that the deductive approach is more suitable for this study, due to the impact of the variation in the retail sector of UAE specifically due to the scope, time, cost, as well as the quality of the research. Furthermore, the researcher initially started with the development of a theory, which made it possible for the researcher to further development arguments related to the number of factors which the researcher has identified as critical for the overall outcomes of the study. In this research paper, the perfect or most suited theory of reasoning was deductive approach as it was able to successfully take into account various factors which are different according to a specific location where research is conducted.

6.5 *Research Strategy or Methodology*

According to Ryan, Scapens, and Theobald, (2002), the research design identifies the overall research methodology that is undertaken by the researcher in carrying out any research work. The research methodology signifies the overarching approach that is required to be implemented in the research on the basis of the philosophical notion, i.e. Interpretivism and positivism. However, the philosophical underpinnings indicate the way in which knowledge can be incorporated as well as the reason for the research, which can be both inductive and deductive. There are three main strategies that are widely used in research. According to Ryan, Scapens, and Theobald, (2002) they are qualitative, quantitative and mixed method research. However, the mixed method of research allows using both the quantitative and qualitative research methodologies at the same time.

6.5.1 Qualitative Research Methodology

Qualitative research methodology refers to a strategy that is basically dependent on the qualitative data, for instance, symbols, signs, and words. According to Taylor, Bogdan, and DeVault, (2015), the qualitative data is the type of data that cannot easily be presented in terms of numbers or can be quantified. In addition to this, Silverman, (2016) indicated that qualitative research methodology presents the data within which it is gathered and it can also revolve around the contextualization of the overall research process to ascertain social interaction. On the other hand, Marshall, and Rossman, (2014) have added that qualitative research methodology only focuses on the collection of qualitative data i.e. words and not the numeric data. The qualitative data is mainly analyzed in such a manner that it includes the context within which the words clarify the reasons behind conveying and sharing the message. The qualitative research approach is best suitable for Interpretivism philosophical form, whereas the evaluation of the social world can be described in several other ways beyond the numbers. According to Silverman, (2016), the main difference between the quantitative and qualitative research methodology is that the qualitative data does not only rely on the primary information, instead, it can also be based on alphanumeric or only non-numerical data. Therefore, in relation to the current research work, the numerical values are considered as the characters therefore, they can be used in the analysis for this research.

6.5.2 Quantitative Research Methodology

Quantitative research methodology refers to a strategy of carrying out research that is mainly based on the collection of quantitative data which is normally numeric data only. However, the numbers presented from the data gathered are used for the analysis. According to Neuman and Robson, (2012), the researcher is required to design appropriate data collection process that facilitates in collecting quantitative data for the analysis purpose of the research. Flick, (2015) in the same manner stated that the data collected through quantitative means actually organize the overall system of collection of data. In relation to the current research work, the numeric data is generated from the survey based on assigning ranks to the risks that are used for the evaluation of deviations in retails sector in UAE.

6.6 Survey sample and Data Collections:

6.6.1 Selecting Respondents

The research was planned and executed from the beginning to accommodate a rich diversity of opinion from specialists and related parties, so that valuable inferences and conclusions could be drawn therefrom. It was impractical to ascertain the population size of the personnel involved in designing, managing and operating the apparatuses and landscape for the CCTV security systems. Sampling techniques were thus deployed. Sampling results provide valuable basis for inferring results about the population. The notion of inferential statistics was employed as the idea being that the inferences can be drawn about the population from the samples, per KuZEL (1992) andNaoum (2013).

6.6.2 Selective (or Stratified) Sampling Technique

Stratified random sampling technique enables the researcher to select random samples from layers of population as identified. It is a two-phased research, whereby first the potential participants need be chosen, and then selections for inclusion in the research is taken therewith. The first phase or step was deemed impractical and too costly i.e. to choose the right type of participant, as done by Naoum (2013). As the sampling approach could be biased from the outset due to issues of impracticality, the researcher did not employ stratified sampling.

6.6.3 Simple Random Sampling Technique

Random sampling results in each item in the population a statistically equal chance of being selected n the sample, according to Suri (2011). This has also been elaborated on by Brase and Brase (2009). However, it was impractical to include the names of all related experts and operators for CCTV surveillance; it helps in understanding the approach by referring to existing research. Researchconducted by Albanna (2005) included all employees working in a company in the UAE, in three emirates of Dubai, Abu Dhabi and Sharjah. Hence, the study was able to focus on all the employees of the firm in those locations. In other research, 28 project managers were chosen from across the Canadian non-governmental sector, by using the simple random method. This approach can take the shape of allocating a number to each participant, and the numbers are chosen through a spreadsheet or some other method. In case the number of participants is large, this method can result in a high level of responses, as high as 52% experienced during research done by Spalek (2014), and 82% in the case of Elbanna (2015). To enhance the response rate, the time duration of the survey can be increased or the methods of primary data collection can be adjusted accordingly, according to Naum (2013). If it takes considerably long, but the number of respondents is proportionately high, then the results are acceptable (de Carvalho et al., 2015).

6.7 Risk impact on cost estimation survey

6.7.1 Design of the Questionnaire and Data Coding

The primary objective of the questionnaire was to ascertain how different groups of respondents would rate or rank the various factors that may potentially lead to variations. The factors were neatly summarised in table form for the respondents to rank, as derived from literature.

6.7.2 Pilot Study (Primary Questionnaire)

A Pilot Study was drafted initially which could be evaluated by a select number of people initially from the industry. This was the preparation for the full survey using the analysis and comments of those who had worked on answering the pilot questionnaire. Bryman and Bell (2011) employed this method to test the strength and improve the data-gathering mechanism, so as to achieve as much mitigation as possible of any faults and weaknesses. The select group of participants were initially provided the questionnaire to get their feedback regarding completeness and understandability. Various comments were generated as a result, that were factored into the final questionnaire. An example of such enhancements was the numbering of the questionnaire slides with a idea regarding the remaining time for completion to assist the respondents.

6.7.3 Final Form of the questionnaire

The questionnaire was designed through a systematic process taking it through three layers. The first one included the basic questionnaire evolved with the help of the supervisor, which was then reviewed by colleagues of the researcher who are area specialists and then the managers and operators of the PSA apparatus. The final questionnaire was prepared after a full review from the pilot survey. The questions were coded in a manner consistent with ease in data input later. Questions were focused on contractors, project owners, consultants and operators, with the result that eventually the respondents could work in teams to get the answers or to seek the help of others they had worked with to finish the questionnaire.

To develop the questionnaire used in this study, the following tasks were completed:

A. Reviewing the literature to extract and classify PSA risks based on life cycle stages.
B. Workshop: An initial exploration of the issues of concern to security professionals working in different organizations via a series of workshops to inform the development of the questionnaire. In addition, meetings were held with the present author’s supervisor for the final development of questions.

The workshop was used to modify the risks extracted from the literature. The participants were asked to suggest the risks that are relevant to the UAE environment. Based on this a questionnaire was developed to estimate the impact of risks on PSA WLC costs. This study uses the PMI matrix for assessing the related WLCC risk structure. An example of how this matrix is used in this study is shown in the subsequent figure.

Probability and Impact Matrix

Probability	Threats					Opportunities				
0.90	0.05	0.09	0.18	0.36	0.72	0.72	0.36	0.18	0.09	0.05
0.70	0.04	0.07	0.14	0.28	0.56	0.56	0.28	0.14	0.07	0.04
0.50	0.03	0.05	0.10	0.20	0.40	0.40	0.20	0.10	0.05	0.03
0.30	0.02	0.03	0.06	0.12	0.24	0.24	0.12	0.06	0.03	0.02
0.10	0.01	0.01	0.02	0.04	0.08	0.08	0.04	0.02	0.01	0.01
	0.05/ Very Low	0.10/ Low	0.20/ Moderate	0.40/ High	0.80/ Very High	0.80/ Very High	0.40/ High	0.20/ Moderate	0.10/ Low	0.05/ Very Low

Impact (numerical scale) on an objective (e.g., cost, time, scope or quality)

Each risk is rated on its probability of occurring and impact on an objective if it does occur. The organization's thresholds for low, moderate or high risks are shown in the matrix and determine whether the risk is scored as high, moderate or low for that objective.

Probability and Impact Matrix

Risk Factors		Degree of Risk impact on risk cost (1 %-72%)	Risk Matrix
41	Lack of funds		
42	Running out of funds		
43	Continually changing requirements		
44	Market development pace rendering products obsolete		
45	Changing priorities		
46	Government rule changes		
47	Hardware & Software defects		
48	Integration issues		
49	Inaccurate Cost forecasts		
50	Exchange rate variability not managed well		
51	Failure to integrate with existing systems		
52	Unavailability of adequate test environment		
53	Failure to integrate components		
54	Security Asset disrupts operations		

Probability					
VH (90%)	5%	9%	18%	36%	72%
H (70%)	4%	7%	14%	28%	56%
M (50%)	3%	5%	10%	20%	40%
L (30%)	2%	3%	6%	12%	24%
VL (10%)	1%	1%	2%	4%	8%
	VL (5%)	L (10%)	M (20 %)	H (40%)	VH (80%)
	IMPACT				

Figure 6-1: Sample of the survey question

The respondent was asked to rate the influence/impact of the following acquisition risks on the cost of security systems. Thequestionnaire was distributed across different organizations with a core business of procuring PSAs. A copy of the questionnaire is included in the appendix. Respondents were assured that all information would be treated as strictly confidential to the university, and that anonymous data would be used in any reports. Participants did not have to enter any identifying details unless they wished to participate further in the research.

Due to the technicality of the research, the questionnaire was created on paper and distributed to the clients and organizations as groups or as individuals. The questionnaire could be simply answered and sent back right away. However, if respondents preferred to take the paper home, they were able to do so and send it later via email. 100 experts were solicited for completing the questionnaire. In total 91 surveys were completed but 23 were incomplete and unusable. Compared to others studies this sample was deemed adequate for estimating and developing the probability distribution for each of the risks.

6.8 *Cost estimation collection*

To estimate the cost of every item in the LCC model a data sheet was developed, see figure 6-2. Cost List: Started with "Brain Storming" between the researcher and the supervisor in the first base, then it goes up one level to the industry of security companies third parties. After that, the list been verified by a consultancy office and experts in AD police which was the final stage.

The datasheet is sent to 10 different securities companies that work in the UAE to estimate the cost and compare and used the data in different programs. Also, the researcher went back again to theconsultancy office in AD police to verify the LCC of CCTV and confirmed it with other 2 companies. The collected data was processed as shown in figure 6-2:

1- The cost of each item computed per square meter
2- The data from step is used to develop the probability disruption of each cost item
3- The best fit program was use to find the best theoretical distribution to fit the estimate costs
4- The author used Anderson test was used to select the best fit distribution
5- The fit of the distributions were assessed for goodness of fit using P-P and Q-Q plots.

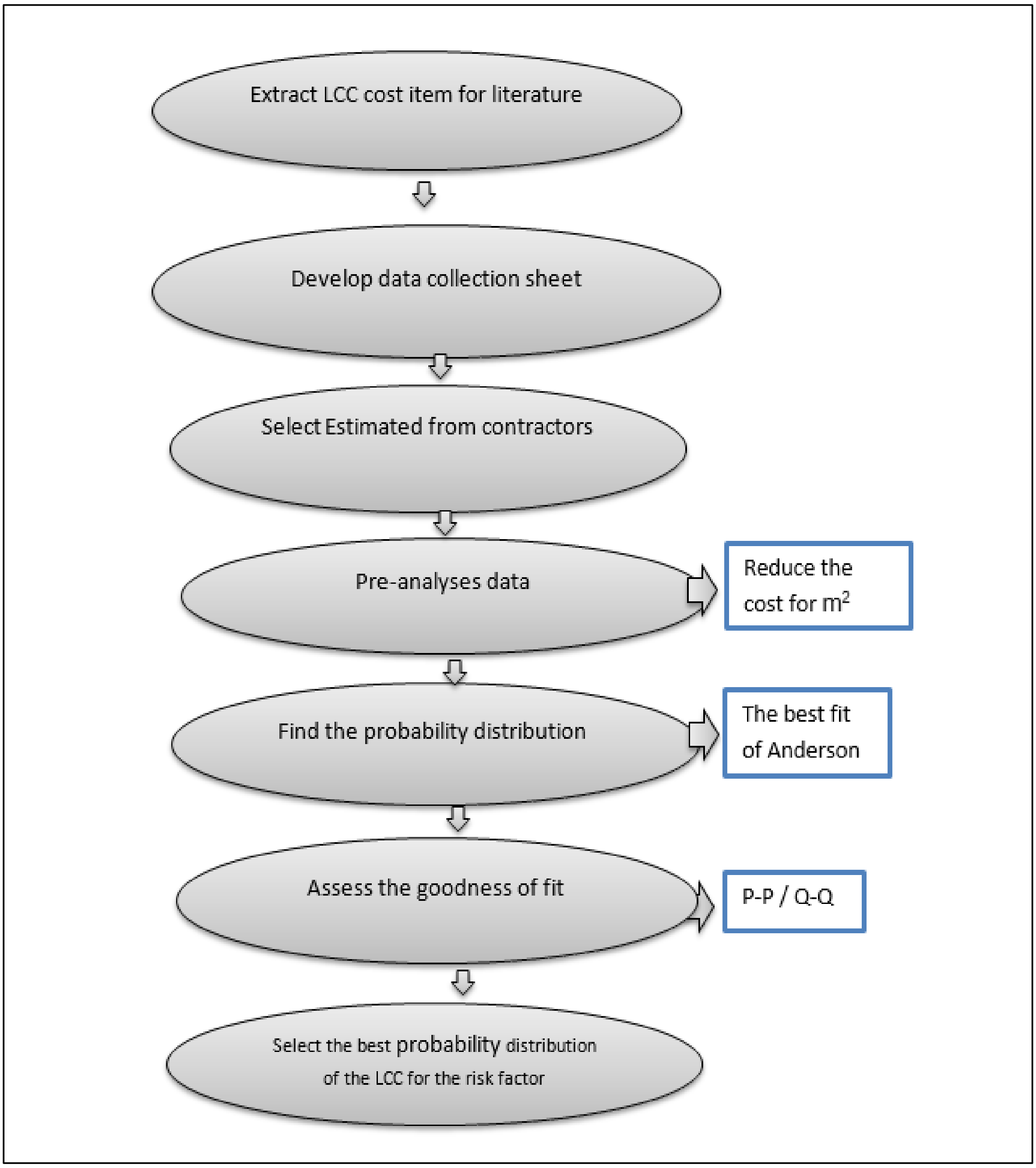


Figure 6-2: process of collecting data

6.9 Incorporating risks into PSA WLCC

The PSA WLCC methodology is presented in chapter5. This section presented the method by which the risk impact is incorporated into the relevant WLCC.

A risk is a scientific tool that helps in making decisions. It attempts to capture all the options as identified and then combines them with the impact thereon of different variables. It requiresthejudgment of the analyst and the adoption of the most suitable risk environment. Traditional methods of risk management have been known to falter when applied to PSA, whereas the more formal methods can be impractical due toa high degree of complexity or cost reasons. The analyst must choose the appropriate risk environment as applicable to the circumstances of the organization and as such no one system can be termed as the ideal one for the environment. Broadly there are the following three categories of approaches available for WLCC analysis:

a) Deterministic – on numerical computations
b) Qualitative – based on subjective system
c) Quantitative techniques – based ona statistical and probabilistic approach to quantification

In deterministic techniques, PMI matrix is used to quantify risk as shown in the previous section. The following formula is relevant:

.

$$y_{Rxc} = wlcc_{xc} * \prod_{i=1}^{i=n} Rxc$$

$$Wlcc_{Rxc} = Wlcc_{xc} + y_{Rxc}$$

Where:

Rxc = risk impact on cost from the type.

So for all stages for PSA WLC:

$$y_{Ric} = wlcc_{Ic} * \prod_{i=1}^{i=n} Ric$$

$$Wlcc_{RIc} = Wlcc_{Ic} + y_{Ric}$$

Where, Ric = risk impact on initial cost from the initial risk category

$$y_{Rimc} = wlcc_{Imc} * \prod_{i=1}^{i=n} Rimc$$

I

$$Wlcc_{RImc} = Wlcc_{Ic} + y_{Rimc}$$

Where, $Rimc$ = risk impact on Implemental cost from the Implemental l risk category

$$y_{R(op\&m)c} = wlcc_{Ic} * \prod_{i=1}^{i=n} R(op\&m)c$$

$$Wlcc_{R(op\&m)c} = Wlcc_{(op\&m)c} + y_{R(op\&m)c}$$

Where, $R(op\&m)c$= risk impact on Operational and maintenance cost from the Operational risk category

$$y_{RAc} = wlcc_{Ac} * \prod_{i=1}^{i=n} RAc$$

$$Wlcc_{RAc} = Wlcc_{Ac} + y_{RAc}$$

Where, RAc = risk impact on an acquisition cost from the a acquisition risk category

$$y_{Rdc} = wlcc_{dc} * \prod_{i=1}^{i=n} Rdc$$

$$Wlcc_{Rdc} = Wlcc_{dc} + y_{Rdc}$$

WhereRdc = risk impact on disposal cost from the disposal risk category

The approach taken in this research is the quantitative one. Regardless, the analysis is based on probabilistic methods is also combined the above formulates so that the variation of risk and costs can be captured by probability distributions. To do so this study employed risk modelling techniques including probability functions. Descriptive statistics are used for the statistical approach, where NPV is also deployed. Probabilistic techniques are the most sophisticated form of the three categories. This study approach is mainly based on Monte Carlo simulation (further details are provided chapter 4.

Total WLCC can be extracted from the following equation:

$$f(PV) = f(C_p) + \sum_{t=0}^{n} \frac{f(Cti)}{\{1 + f(d)\}^t}$$

Trace-driven simulation techniques can be used, or empirical distribution, and the theoretical distribution ones per Maio et al. (2000). Then, frequency histograms can be plotted with results taken from the model.

6.10 *Development of WLCC Model*

This requires a series of steps where initially cost assumptions are identified, later manipulated and adjusted for later inputting into the model. After that simulation is carried out to get present values, then for the whole PSA framework, after which the parameters are considered for the model. Thereupon, sensitivity measures can be conducted.

A range of techniques is available to ascertain the assumptions. The discount rate used has to be the relevant one, generally the cost of capital for the firm. An alternative procedure is carried out to generate eventually the probability functions. The model adopted bythe study is shown in the following Figure.

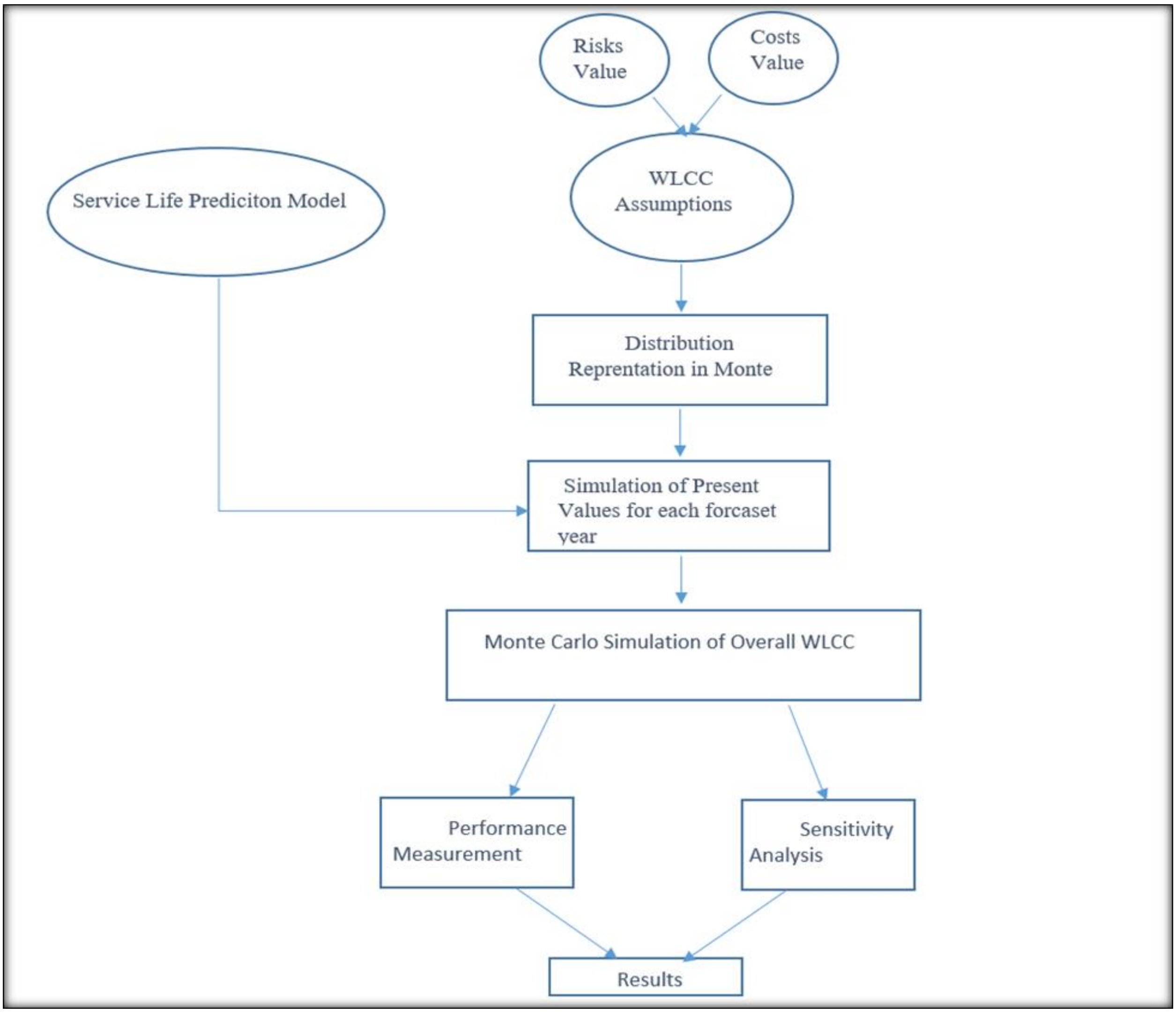


Figure 6-3: The proposed study model

CHAPTER 7. ***DATA PRESENTATION AND ANALYSIS***

7.1 Introduction

This Chapter deals with data collection and analysis. In the first part, the focus would be on the development of a questionnaire survey about the influence of risks on PSA costs and the presented initiation risks, implementation risks, acquisition risks, operation and maintenance (O&M) risks, and disposal risks. The Survey results were employed to assess the impact on risks associated with product lifecycle through statistical methods. The second part deals with the application of Factor Analysis in order to reduce the number of relevant variables in risk analysis.

7.2 PSA Risk Questionnaire

7.2.1 Methodology

To develop the questionnaire used in this study, the following tasks were completed:

- Reviewing the literature to extract and classify PSA risks based on life cycle stages.
- Workshop: Series of workshops to explore the issue amongst security professionals, to facilitate the development of the Questionnaire. In addition, meetings were held with the present author's supervisor for the final development of questions.
- Questionnaire: The questionnaire was developed and distributed across different organizations with a core business of procuring PSAs. A copy of the questionnaire is included in the appendix.

The main themes of the questionnaire were:

- General information about participants
- The influence and impact of risks on PSAs for the following life cycle phases:
- Initiation phase
- Implementation phase
- Acquisition phase
- Operations and maintenance phase
- Disposition phase

The respondents were given the assurance of confidentiality and that anonymity would be used in applying the data collected. Moreover, that the data collected would be strictly confidential to the university.

Due to the technicality of the research, the questionnaire was created on paper and distributed to the clients and organizations as groups or as individuals. The questionnaire could be simply answered and sent back right away. However, if respondents preferred to take the paper home, they were able to do so and send it later via email.

7.2.2 Questionnaire Results– the Organisation

In total, 100 questionnaires were distributed to the PSA organizations. Only 90 responses were received by the deadline, 68 of which were found to be usable.

Therefore, although the 100 questionnaires are analyzed, only 68 are used in this research study. In this questionnaire, the term ‘organization ‘refers to an organization whose main business is PSAs.

In the analysis of the results, 15 values and answers were found to be missing from the respondents. Field (2013) lists a number of reasons why participants miss questions. For instance, this can occur in long questionnaires, where participants accidentally miss questions. However, participants can also sometimes do this on purpose just to annoy a researcher, or to avoid delicate topics to show their right not to answer such questions. However, Field stresses that some missing data in a survey does not mean that the researcher should have to ignore the rest of the collected data (Field 2013, pp. 107-108).

7.2.2.1 Respondents’ Employment Status

Most of the respondents, 43 out of 69 (62%),are employed in the private sector. The rest, 26 out of 69 (38%), are in the public sector. Figure 1illustrates the respondents’ answers.

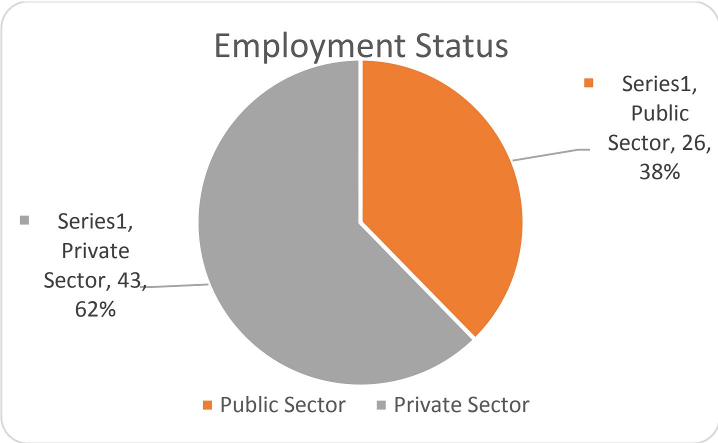


Figure 7-1: Respondents' employment status

7.2.2.2 Respondents' Job Title

The questionnaire was distributed across different levels of the organizations, such as the operational and tactical levels, to ensure the integrity and consistency of the results. A total of 32 respondents work as security engineers for an organization; 16 respondents are project managers; 14 respondents are cost engineers; 4 are control room operators, and 3 are estimators. Figure 2 presents the respondents' answers.

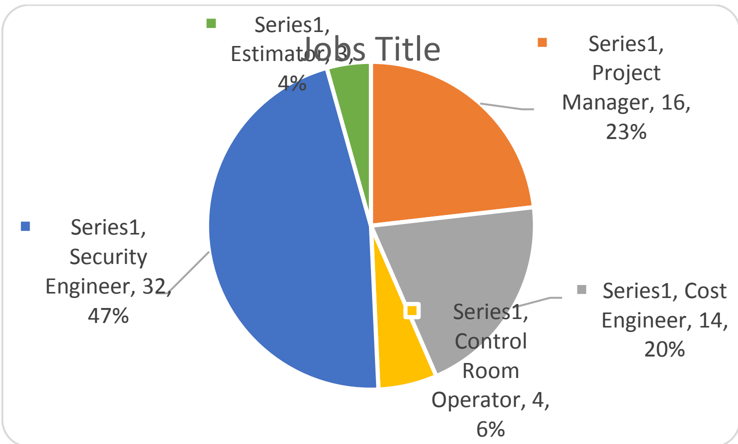


Figure 7-2: Jobs title in an organization

7.2.2.3 Respondents' Experience

A total of 53 (77%) of the respondents reported having 5to10 years' experience, compared to 12 (17%) respondents with more than 10 years' experience, and only 4 (6%)with 3-to-5 years' experience. Figure 3illustrates the respondents' answers.

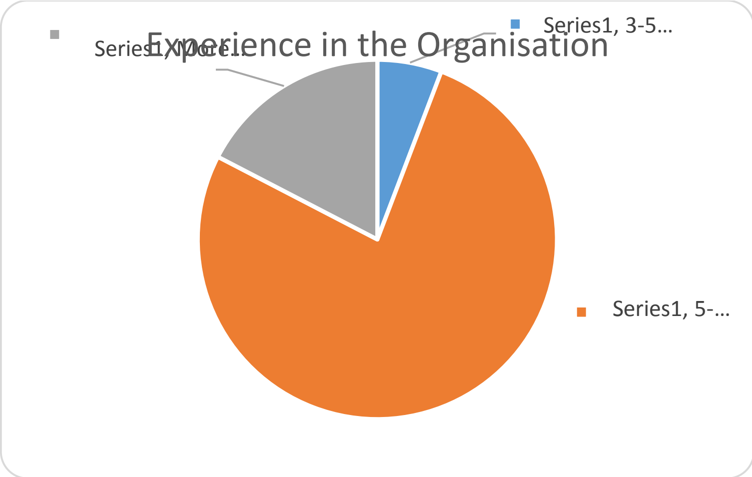


Figure 7-3: Respondents' experience in the organization

7.2.2.4 Size of Projects

Most respondents, 59 (86%),work in an organization that participates in projects making revenues of more than 5million AED, and 5 (7%) participate in projects with a value of less than 5million AED. Only 2 (3%) and 3 (4%) are involved in small projects worth less than 1million AED and less than 500,000 AED, respectively. Figure 4 shows the respondents' answers.

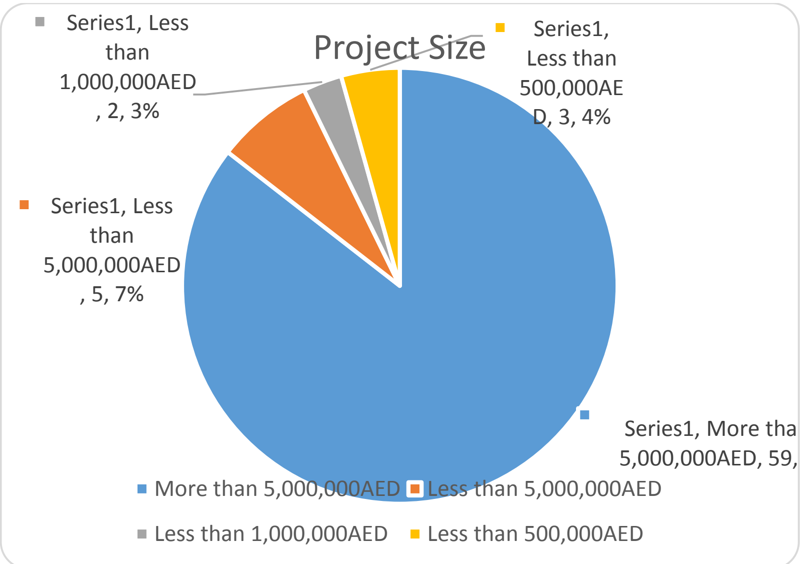


Figure 7-4: Size of projects in value [AED]

7.3 PSA Risks

This section presents the statistical calculations of riskfor different phases of the life cycle. There are five types of risks factors: initiation, implementation, acquisition, operation and maintenance, and disposition risks factors. Given that a high number of risk factors are taken from a source that spans a long period of time, it is expected that there are only statistically insignificant differences between the risk factors. However, the analysis reveals that there is a statistically significant difference in the means and the standard deviations. Therefore, kurtosis and Skewness are calculated for each risk factor using the risk matrix impact and probability.

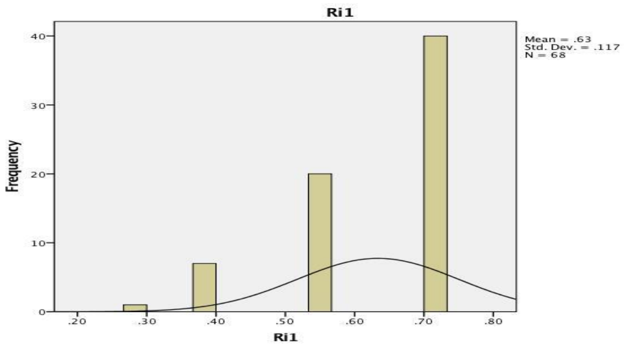
Kurtosis is a measure of the peakedness of the distribution. Skewness is a measure of how much lack of symmetry occurs in the distribution. In times of increased uncertainty, kurtosis is greater than three and has a fatter tail. In times of lower uncertainty, the kurtosis figure is less than three with a thinner tail. Skewness similarly gets highly significant N times of uncertainty, and in cases can mean that there is a large probability of negative results. In low uncertainty, the Skewness measure is close to zero. Hence, the two measures provide for factoring in times of uncertainty and can be carried out for each life cycle element. Risk Matrix can then be formed with probability and the impact showing for each factor.

Probability	Threats				
0.90	0.05	0.09	0.18	0.36	0.72
0.70	0.04	0.07	0.14	0.28	0.56
0.50	0.03	0.05	0.10	0.20	0.40
0.30	0.02	0.03	0.06	0.12	0.24
0.10	0.01	0.01	0.02	0.04	0.08
	0.05	0.10	0.20	0.40	0.80

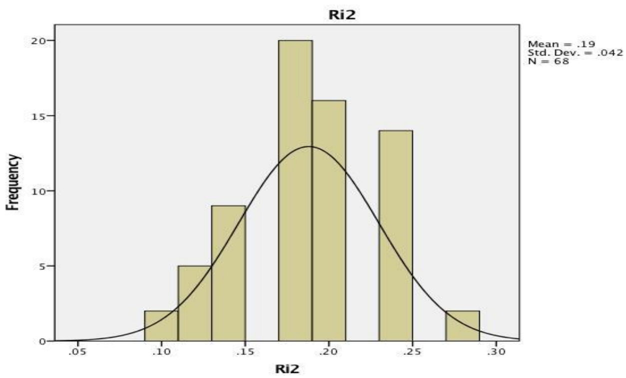
Figure 7-5 Risk Matrix

7.3.1 Influence of Risks on Initiation Costs (Ri)

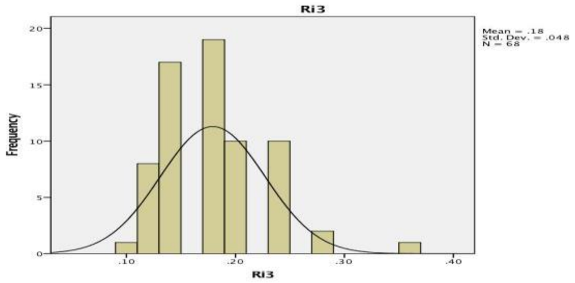
The survey results are presented regarding the impact of the initiation risks on the cost of security systems. The likelihood of each risk factor is presented. A total of40 out of the 68 respondents indicated that **the risk factor (Ri1) 'wrong budget estimation'** is 72%likely to occur as a result of initiation risks related tothe cost of the security system, 20 out of 68 chose 56%, 7 chose 40%, and only 1 through 28%.

Histogram	Mean & Standard Deviation
 Figure 7-6 Histogram for Ri1	The likelihood of Ri1 ranging from 0-80% on **initiation risk** has a mean of 0.63.The distribution curve of this variable shows that it is negatively skewed, with a Skewness of -1.114. It has a standard deviation of 0.117. This is an indication that the respondents agreed that Ri1 is highly likely to occur.

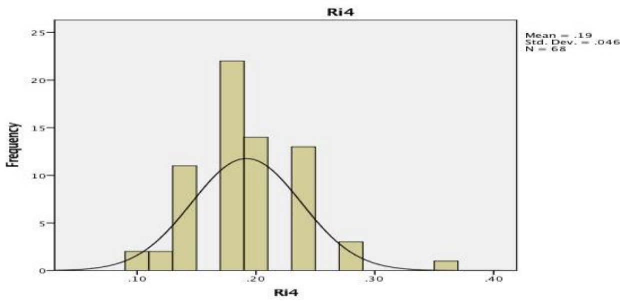
Furthermore, 2 out of the 68 respondents indicated that **risk factor (Ri2) 'cost overruns due to change of scope'** is 10% likely to occur as a result of initiation risks related to the cost of the security system, 5 chose12%, 9 indicated 14%, 20 chose 18%, 16 chose 20%, 14 indicated 28% and only 2 out of 68 thought 28%.

Histogram	Mean & Standard Deviation
 Figure 7-7 Histogram for Ri2	The likelihood of Ri2 ranging from 0-30% on **initiation risk** has a mean of 0.19.The distribution curve of this variable shows that it is negatively skewed, with a skewness of -.077. It has a standard deviation of .042. This is an indication that the respondents agreed that Ri2 is highly likely to take place.

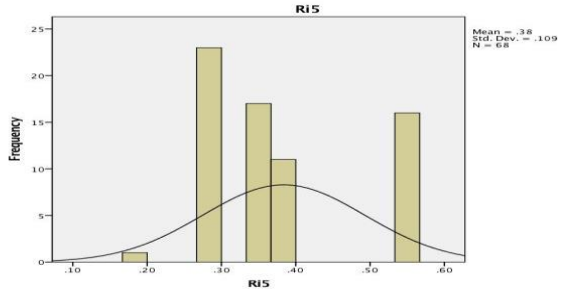
A single respondent indicated that **risk factor (Ri3) 'continual project scope expansion'** is 10%likely to occur as a result of initiation risks related to the cost of the security system, 8 out of 68 indicated12%, 17 chose 14%, 19 chose 18%, 10 through20%, 10 out of 24 indicated 24%, 2 chose 28%, and only 1 out of 68 thought 36%.

Histogram	**Mean & Standard Deviation**
 Figure 7-8 Histogram for Ri3	The likelihood of Ri3 ranging from 0-40% on **initiation risk** has a mean of 0.18.The distribution curve of this variable shows that it is positively skewed, with a skewness of 0.991. It has a standard deviation of .48.

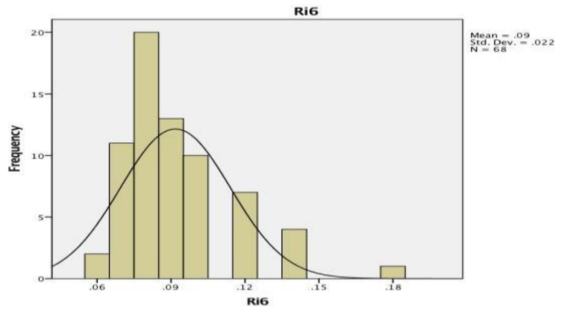
A single respondent indicated that **risk factor (Ri4) 'delayed approval'** is 10% likely to occur as a result of initiation risks related to the cost of the security system, 2 out of 68 indicated 12%, 11 chose 14%, 22 chose 18%, 14 indicated 20%, 13 thought24%, 3 chose 28%, and only 1 out of 68 thought 36%.

Histogram	**Mean & Standard Deviation**
 Figure 7-9 Histogram for Ri4	The likelihood of Ri4 ranging from 0-40% on **initiation risk has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a Skewness of 0.677. It has a standard deviation of .046

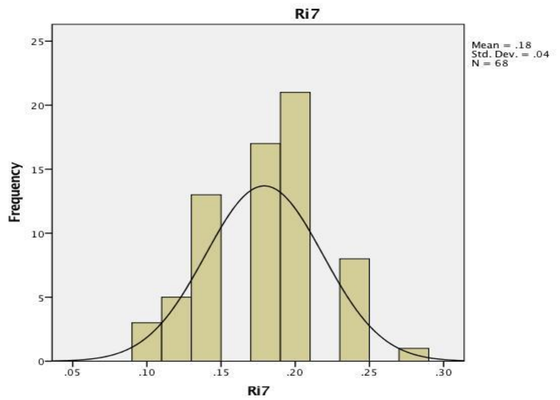
Only 1 out of the 68 respondents indicated that **risk factor (Ri5) 'lack of defined scope'**is 18% likely to occur as a result of initiation risks related to the cost of the security system, 23 out of 68 indicated 28%, 17 chose 36%, 11 indicated 40%, and 16 chose 56%.

Histogram	Mean & Standard Deviation
 Figure 7-10 Histogram for Ri5	The likelihood of Ri5 ranging from 0-60% on **initiation risk has** a mean of 0.38.The distribution curve of this variable shows that it is positively skewed, with a Skewness of 0.627. It has a standard deviation of .109.

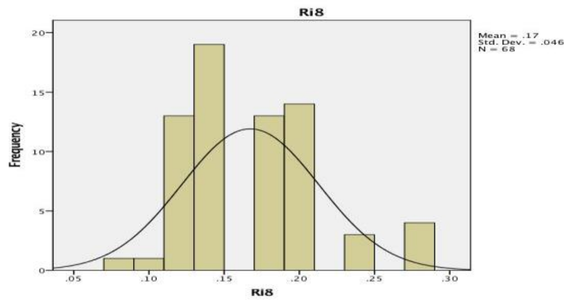
Two respondents indicated that **risk factor (Ri6)'scope creep**' is 6% likely to occur as a result of initiation risks related to the cost of the security system, 11 out of 68 indicated 7%, 20 through8%, 13 chose 9%, 10 indicated 10%, 7 out of 68 thought 12%, 4 chose 14%, and only 1 out of 68 thought 18%.

Histogram	Mean & Standard Deviation
 Figure 7-11 Histogram for Ri6	The likelihood of Ri6 ranging from 0-20% on **initiation risk has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed, with a Skewness of 1.505. It has a standard deviation of .022.

A total of 3 out of the 68 respondents who participated in the survey indicated that **risk factor (Ri7) 'gold plating** 'is 10% likely to occur as a result of initiation risks related to the cost of the security system, 5 indicated 12%, 13 chose 14%, 17 through18%, 21 indicated 20%, 8 24%, and 1 out of 68 chose 28%.

Histogram	**Mean & Standard Deviation**
 Figure 7-12 Histogram for Ri7	The likelihood of Ri7 ranging from 0-30% on **initiation risk has** a mean of 0.18.The distribution curve of this variable shows that it is negatively skewed, with a Skewness of -0.668. It has a standard deviation of .04. This is an indication that the respondents agreed that **Ri7**is highly likely to occur.

A single respondent indicated that **risk factor (Ri8) 'inter-dependencies are not defined well** 'is 8% likely to occur as a result of initiation risks related to the cost of the security system, 1 out of 68 chose 10%, 13 indicated 12%, 19 indicated 14%, 13 thought18%, 14 chose 20%, 3 indicated 24%, and only 4 out of 68 thought28%.

Histogram	**Mean & Standard Deviation**
 Figure 7-13 Histogram for Ri8	The likelihood of Ri8 ranging from 0-80% on **initiation risk has** a mean of 0.17.The distribution curve of this variable shows that it is positively skewed, with a Skewness of 0.754. It has a standard deviation of .046.

Nine respondents indicated that **risk factor (Ri9) 'inter-dependencies are not coordinated and approved** 'is 28% likely to occur as a result of initiation risks related to the cost of the security system, 26 out of 68 indicated 36%, 19 chose 40%, and only 14 thought 56%.

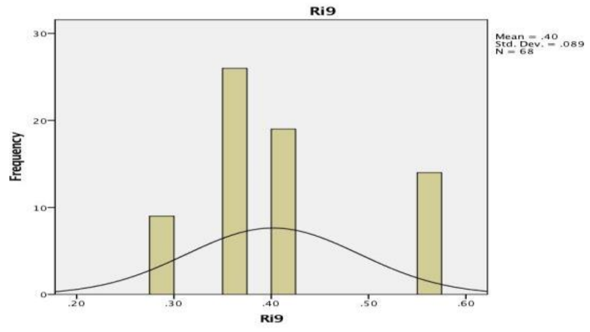
<table>
<tr><th>Histogram</th><th>Mean & Standard Deviation</th></tr>
<tr><td>

Figure 7-14 Histogram for Ri9</td><td>The likelihood of Ri9 ranging from 0-60% on initiation risk has a mean of 0.40.The distribution curve of this variable shows that it is positively skewed, with a Skewness of 0.817. It has a standard deviation of .089.</td></tr>
</table>

One respondent indicated that **risk factor (Ri10) 'missing critical activities from scope** 'is 12% likely to occur as a result of initiation risks related to the cost of the security system, 13 out of 68 indicated 14%, 22 thought18%, 18 chose 20%, 7 indicated 24%, 3 believed 28%, 2 indicated 36%, and another 2 out of 68 thought 40%.

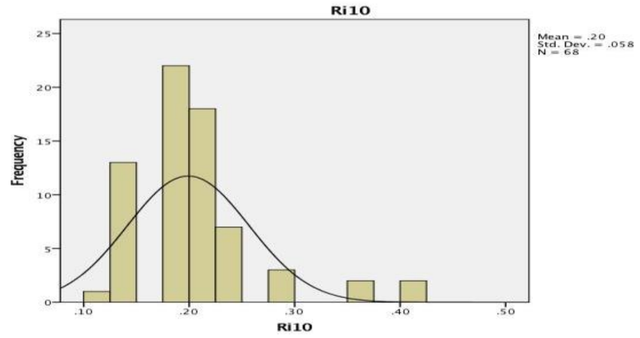
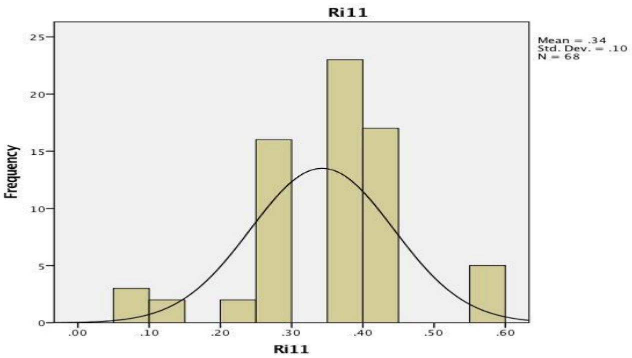
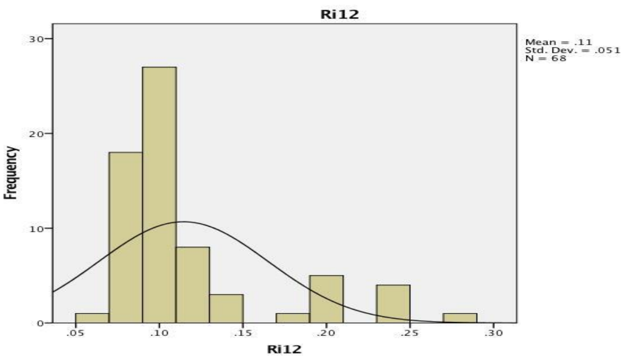
<table>
<tr><th>Histogram</th><th>Mean & Standard Deviation</th></tr>
<tr><td>

Figure 7-15 Histogram for Ri10</td><td>The likelihood of Ri10 ranging from 0-50% on initiation risk has a mean of 0.30.The distribution curve of this variable shows that it is positively skewed, with a Skewness of 1.857. It has a standard deviation of .058.</td></tr>
</table>

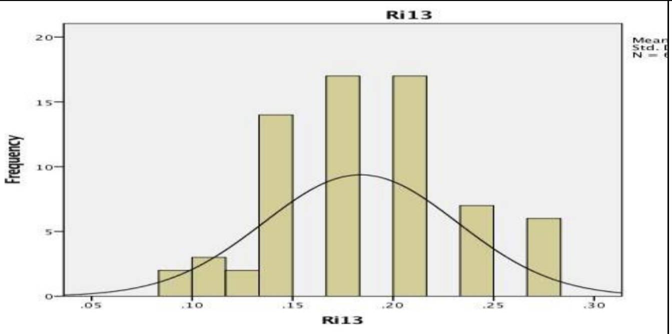
Three respondents indicated that **risk factor (Ri11) 'unknownstakeholders** 'is 9% likely to occur as a result of initiation risks related to the cost of the security system, 2 out of 68 thought 14%, 2 chose 20%, 16 believed 28%, 23 indicated 36%, 17 chose 40%, and 5 out of 68 indicated 56%.

Histogram	Mean & Standard Deviation
 Figure 7-16 Histogram for Ri11	The likelihood of Ri11 ranging from 0-60% on **initiation risk has** a mean of 0.34.The distribution curve of this variable shows that it is negatively skewed, with a Skewness of -.309. It has a standard deviation of .10. This is an indication that the respondents agreed that **Ri11** is highly likely to occur.

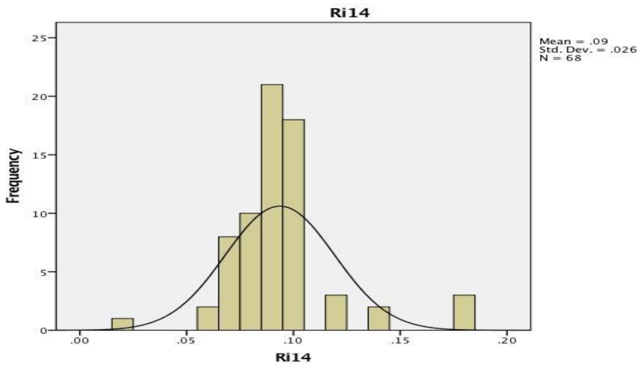
One respondent indicated that **risk factor (Ri12) ‘technology design failures**‘is 6% likely to occur as a result of initiation risks related to the cost of the security system, 2 out of 68 chose 7%, 16 answered 8%, 20 thought9%, 7 indicated10%, 8 answered 12%, 3 chose 14%, 1 answered 18%, 5 through20%, 4 believed 24%, and only 1 out of 68 thought 28%.

Histogram	Mean & Standard Deviation
 Figure 7-17 Histogram for Ri12	The likelihood of Ri12 ranging from 0-30% on **initiation risk has** a mean of 0.11.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.717. It has a standard deviation of .051.

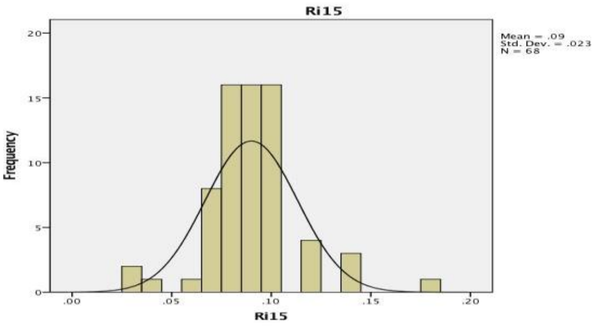
A total of 2 out of the 68 respondents indicated that **risk factor (Ri13) ‘risks in specification breakdown**‘is 9% likely to occur**,** 3 indicated 10%, 2 chose 12%, 14 answered 14%, 17 thought18%, 17 indicated 20%, 7 believed 24%, and 6 out of 68 thought 28%.

Histogram	Mean & Standard Deviation
 Figure 7-18 Histogram for Ri13	The likelihood of Ri13 ranging from 0-80% on **initiation risk has** a mean of 0.18.The distribution curve of this variable shows that it is positively skewed, with a skewness of 0.210. It has a standard deviation of .048.

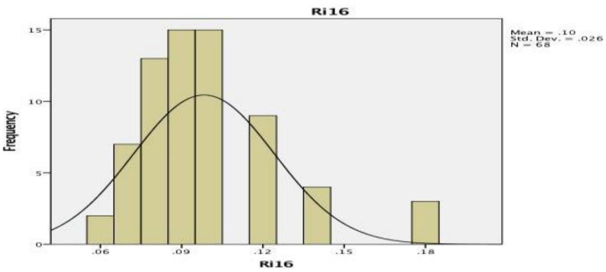
Just 1 out of the 68 respondents indicated that **risk factor (Ri14) ‘unrealistic expectations of stakeholders**’ is 2%likely to occur as a result of initiation risks related to the cost of the security system, 2 answered 6%, 8 thought7%, 10 chose 8%, 21 indicated 9%, 18 chose 10%, 3 believed 12%, 2 answered 14%, and 3 out of 68 thought 18%.

Histogram	Mean & Standard Deviation
 Figure 7-19 Histogram for Ri14	The likelihood of Ri14 ranging from 0-30% on **initiation risk has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.453. It has a standard deviation of .035.

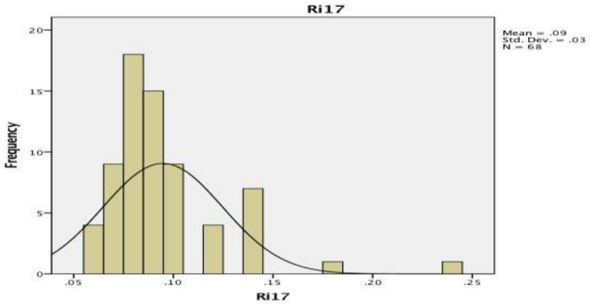
Only 2 out of the 68 respondents indicated that **risk factor (Ri15) ‘schedule flaws** ‘is 3% likely to occur as a result of initiation risks related to the cost of the security system, 1 out of 68 indicated 4%, 1 chose 6%, 8 answered 7%, 16 out of 68 thought 8%, 16 indicated 9%, 16 believed 10%, 4 answered 12%, 3 indicated 14%, and 1 out of 68 believed 18%.

Histogram	**Mean & Standard Deviation**
 Figure 7-20 Histogram for Ri15	The likelihood of Ri15 ranging from 0-80% on **initiation risk** has a mean of 0.09.The distribution curve of this variable shows that it is positively skewed, with a skewness of .691. It has a standard deviation of .023.

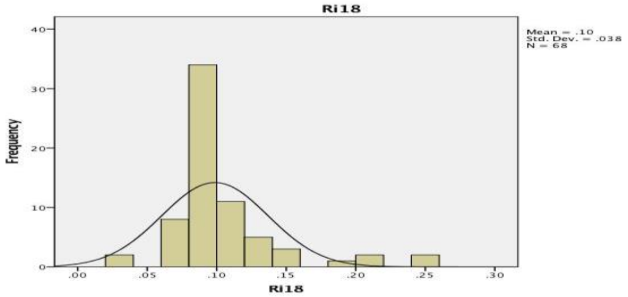
Two respondents indicated that **risk factor (Ri16) 'quality management issues** 'is 6% likely to occur as a result of initiation risks related to the cost of the security system, 7 out of 68 answered 7%, 13 chose 8%, 15 answered 9%, 15 thought10%, 9 indicated 12%, 4 believed 14%, and 3 out of 68 thought 18%.

Histogram	**Mean & Standard Deviation**
 Figure 7-21 Histogram for Ri16	The likelihood of Ri16 ranging from 0-20% on initiation risk has a mean of 0.10.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.464. It has a standard deviation of .026.

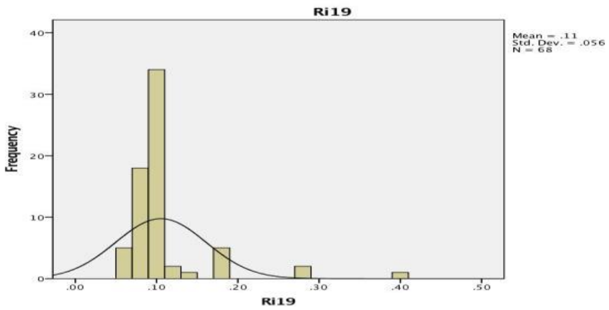
A total of 4 out of the 68 respondents indicated that **risk factor (Ri17) 'human resources management issues** 'is 6%likely to occur as a result of initiation risks related to the cost of the security system, 9 out of 68 indicated 7%, 18 thought8%, 15 chose 9%, 9 answered 10%, 4 thought12%, 7 believed 14%, 1 indicated 18%, and another 1 out of 68 answered 24%.

Histogram	Mean & Standard Deviation
 Figure 7-22 Histogram for Ri17	The likelihood of Ri17 ranging from 0-30% on **initiation risk has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.314. It has a standard deviation of .03.

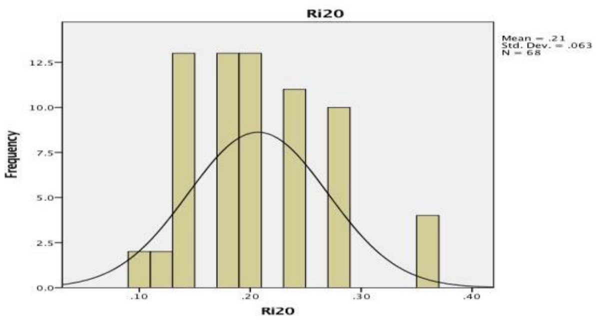
Two respondents indicated that **risk factor (Ri18) ‘procurement management issues** ‘is 3%likely to occur as a result of initiation risks related to the cost of the security system, 2 out of 68 thought 6%, 6chose 7%, 13 answered 8%, 21 indicated 9%, 11 answered 10%, 5 12%, 3 out of 68 thought 14%, 1 believed 18%, 1 answered 20%, and 2 out of 68 answered 24%.

Histogram	Mean & Standard Deviation
 Figure 7-23 Histogram for Ri18	The likelihood of Ri18 ranging from 0-30% on initiation risk has a mean of 0.10.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.068. It has a standard deviation of .038.

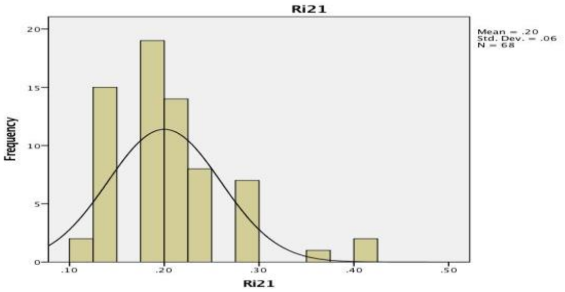
A total of 5 out of the 68 respondents indicated that **risk factor (Ri19) ‘time management issues** ‘is 6%likely to occur as a result of initiation risks related to the cost of the security system, 6 answered 7%, 12 indicated 8%, 16 chose 9%, 18 thought10%, 2 answered 12%, 1 thought14%, 5 indicated 18%, 2 believed 28%, and only 1 out of 68 indicated 40%.

Histogram	Mean & Standard Deviation
 Figure 7-24 Histogram for Ri19	The likelihood of Ri19 ranging from 0-50% on **initiation risk has** a mean of 0.11.The distribution curve of this variable shows that it is positively skewed, with a skewness of 3.348. It has a standard deviation of .056.

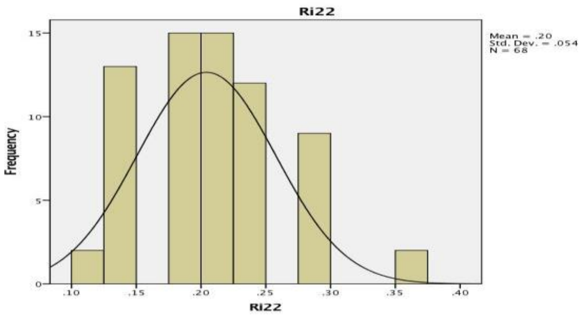
Just 2 out of the 68 respondents indicated that **risk factor (Ri20) ‘poor workmanship quality** ‘is 10%likely to occur as a result of initiation risks related to the cost of the security system, 2 answered 12%, 13 chose 14%, 13 thought20%, 11 answered 24%, 10 believed 28%, and 4 out of 68 chose 36%.

Histogram	Mean & Standard Deviation
 Figure 7-25 Histogram for Ri20	The likelihood of Ri20 ranging from 0-50% on **initiation risk has** a mean of 0.21.The distribution curve of this variable shows that it is positively skewed, with a skewness of .655. It has a standard deviation of .063.

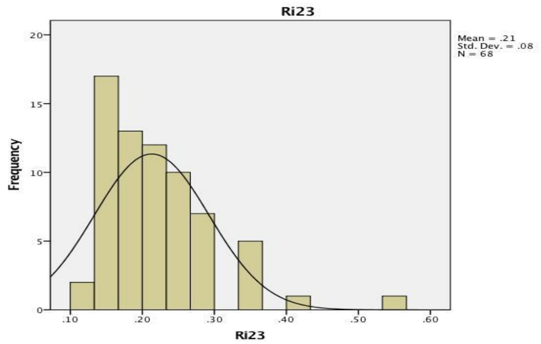
Only 2 out of the 68 respondents indicated that **risk factor (Ri21) ‘frequent delay design change** ‘is 12%likely to occur as a result of initiation risks related to the cost of the security system, 15 indicated 14%, 19 chose 18%, 14 answered 20%, 8 thought24%, 7 chose 28%, 1 believed 36%, and 2 out of 68 indicated 40%.

Histogram	**Mean & Standard Deviation**
 Figure 7-26 Histogram for Ri21	The likelihood of Ri21 ranging from 0-50% on **initiation risk has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.440. It has a standard deviation of .06.

A total of 2 out of the 68 respondents indicated that **risk factor (Ri22) ‘contractor factor to platform** ‘is 12%likely to occur as a result of initiation risks related to the cost of the security system, 13 answered 14%, 15 thought18%, 15 indicated 20%, 12 chose 24%, 9 answered 28%, and 2 out of 68 thought 36%.

Histogram	**Mean & Standard Deviation**
 Figure 7-27 Histogram for Ri22	The likelihood of Ri22 ranging from 0-50% on **initiation risk has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of .470. It has a standard deviation of .054. This is an indication that the respondents agreed that **Ri22**is highly likely to occur.

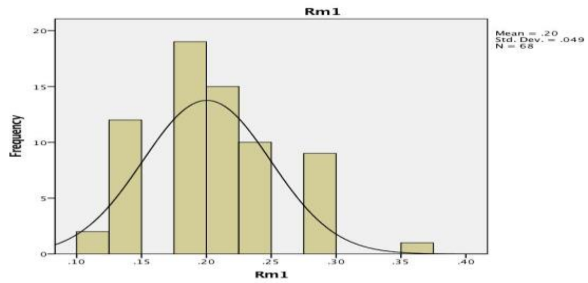
Two respondents answered that **risk factor (Ri23) ‘poor negotiation between different stakeholders** ‘is 12%likely to occur as a result of initiation risks related to the cost of the security system, 17 out of 68 indicated 14%, 13 chose 18%, 12 answered 20%, 10 thought24%, 7 indicated 28%, 5 believed 36%, 1 thought 40%, and 1 out of 68 indicated 56%.

Histogram	**Mean & Standard Deviation**
 Figure 7-28 Histogram for Ri23	The likelihood of Ri23 ranging from 0-60% on **initiation risk has** a mean of 0.21.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.754. It has a standard deviation of .08.

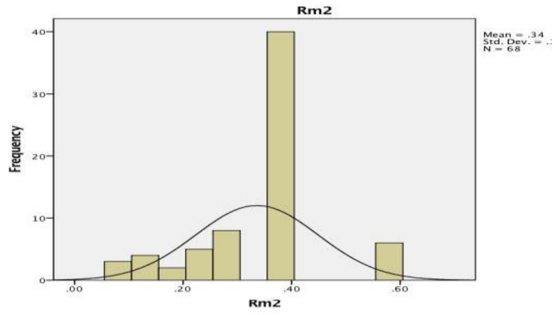
7.3.2 Influence of Risks on the ImplementationCosts (Rmx)

This section presents the survey results for the impact of the implementation risks on the cost of security systems. The likelihood of each risk factor is indicated.

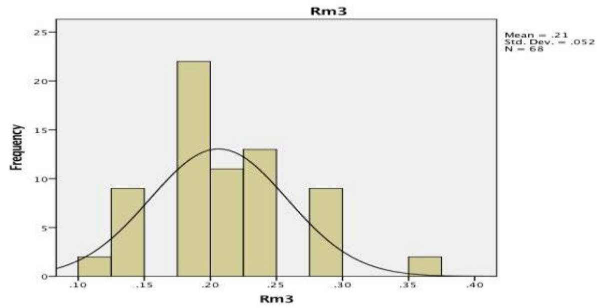
Two respondents thought that **risk factor (Rm1) 'change in management'** is 12%likely to occur as a result of implementation risks related to the cost of the security system, 12 out of 68 indicated 14%, 19 chose 18%, 15 answered20%, 10 thought24%, 9 indicated 28%, and 1 out of 68 answered 36%.

Histogram	**Mean & Standard Deviation**
 Figure 7-29 Histogram for Rm1	The likelihood of Rm1 ranging from 0-40% on **implementation risk has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of .697. It has a standard deviation of .049.

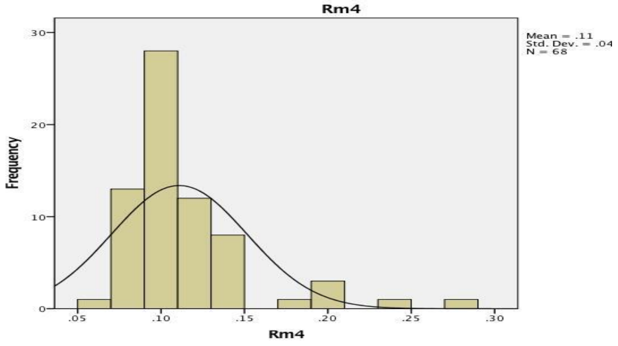
Only 1 out of the 68 respondents indicated that **risk factor (Rm2) 'wrong timeframe estimation** 'is 8%likely to occur as a result of implementation risks related to the cost of the security system, 1 out of 68 thought 9%, 1 answered 10%, 14 indicated 12%, 1 answered 18%, 1 chose 20%, 5 thought24%, 8 indicated 28%, 27 believed 36%, 13 chose 40%, and 6 out of 68 answered 56%.

Histogram	Mean & Standard Deviation
 Figure 7-30 Histogram for Rm2	The likelihood of Rm2 ranging from 0-80% on **implementation risk has** a mean of 0.34.The distribution curve of this variable shows that it is negatively skewed, with a skewness of -.280. It has a standard deviation of .113 This is an indication that the respondents agreed that **Rm2** is highly likely to occur.

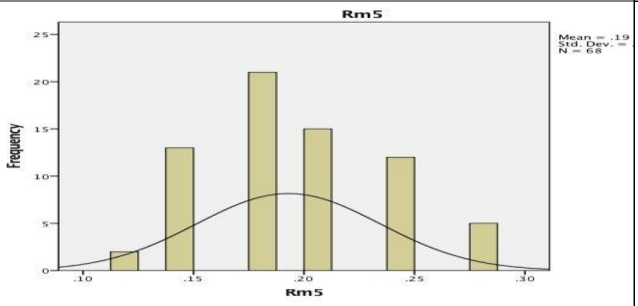
A total of 2 out of the 68 respondents answered that **risk factor (Rm3) 'change in laws /rules**' is 12%likely to occur as a result of implementation risks related to the cost of the security system, 9 indicated 14%, 22 out of 68 chose 18%, 11 believed 20%, 13 answered 24%, 9 thought 28%, and 2 indicated 36%.

Histogram	Mean & Standard Deviation
 Figure 7-31 Histogram for Rm3	The likelihood of Rm3 ranging from 0-80% on **implementation risk has** a mean of 0.21.The distribution curve of this variable shows that it is positively skewed, with a skewness of .780. It has a standard deviation of .052.

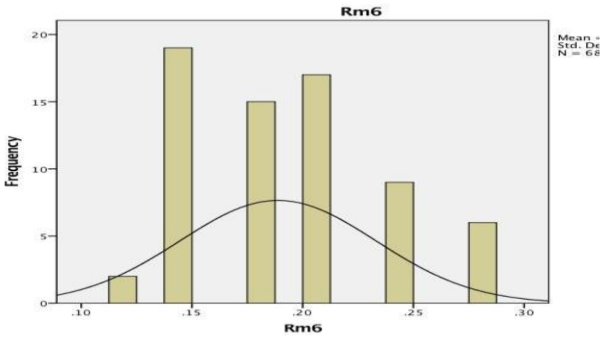
One respondent indicated that **risk factor (Rm4) 'poor projectmanagement's** 6%likely to occur as a result of implementation risks related to the cost of the security system, 8 out of 68 answered7%, 5 indicated 8%, 14 chose 9%, 14 thought10%, 12 answered 12%, 8 chose 14%, 1 indicated 18%, 3 thought20%, 1 believed 24%, and only 1 out of 68 answered 28%.

Histogram	Mean & Standard Deviation
 Figure 7-32 Histogram for Rm4	The likelihood of Rm4 ranging from 0-30% on **implementation risk has** a mean of 0.11.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.002. It has a standard deviation of .117.

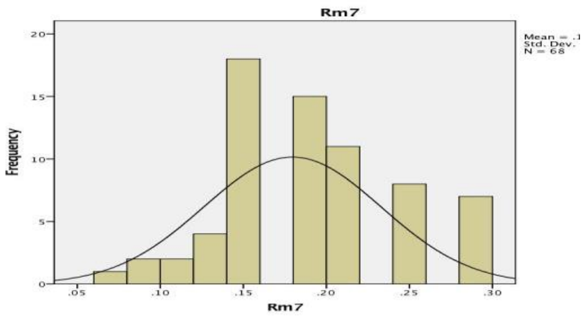
Just 2 out of the 68 respondents thought that **risk factor (Rm5) 'delays due to coordinates with other contractors**' is 12%likely to occur as a result of implementation risks related to the cost of the security system, 13 out of 68 indicated 14%, 21 answered18%, 15 chose 20%, 12 thought 24%, and 5 indicated 28%.

Histogram	Mean & Standard Deviation
 Figure 7-33 Histogram for Rm5	The likelihood of Rm5 ranging from 0-30% on **implementation risk has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of .386. It has a standard deviation of .042.

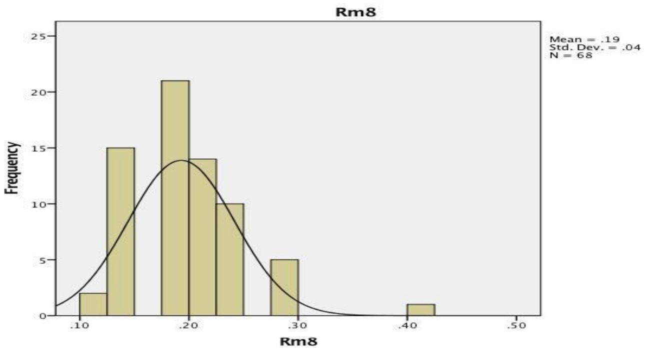
Two respondents indicated that **risk factor (Rm6) 'Failure to identify complex functionalities and time required to develop those functionalities**' is 12%likely to occur as a result of implementation risks related to the cost of the security system, 19 out of 68 thought 14%, 15 answered 18%, 17 believed 20%, 9 thought 24%, and 6 out 68 indicated 28%.

Histogram	Mean & Standard Deviation
 Figure 7-34 Histogram for Rm6	The likelihood of Rm6 ranging from 0-30% on **implementation risk has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of .514.It has a standard deviation of .044.

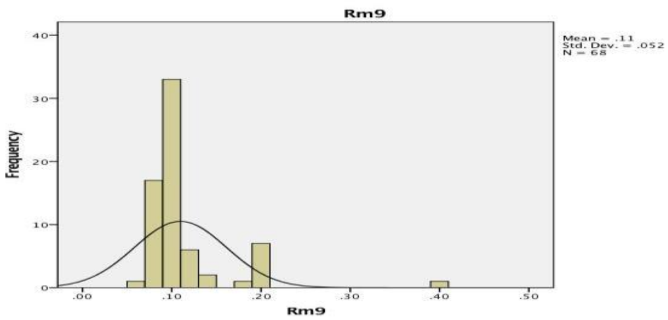
Just 1 out of the 68 respondents indicated that **risk factor (Rm7) 'information security incidents'** is 7%likely to occur as a result of implementation risks related to the cost of the security system, 2 out of 68 thought8%, 2 indicated 10%, 4 answered 12%, 18 chose 14%, 15 believed 18%, 11 indicated 20%, 8 chose 24%, and 7 out of 68 answered 28%

Histogram	Mean & Standard Deviation
 Figure 7-35 Histogram for Rm7	The likelihood of Rm7 ranging from 0-30% on **implementation risk has** a mean of 0.18.The distribution curve of this variable shows that it is positively skewed, with a skewness of .272. It has a standard deviation of .053.

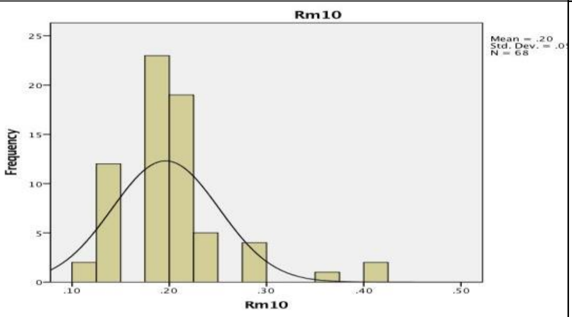
Two respondents indicated that **risk factor (Rm8) 'legacy components lack adequate documentation'** is 12%likely to occur as a result of implementation risks related to the cost of the security system, 15 out of 68 chose 14%, 21 thought18%, 14 answered 20%, 10 thought24%, 5 indicated 28%, and 1 out of 68 chose 40%.

Histogram	Mean & Standard Deviation
 Figure 7-36 Histogram for Rm8	The likelihood of Rm8 ranging from 0-50% on **implementation risk has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.343. It has a standard deviation of .049.

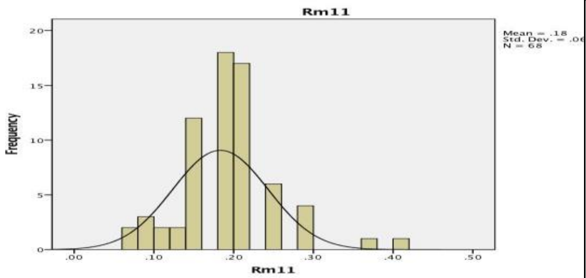
Only 1 out of the 68 respondents answered that **risk factor (Rm9) 'security assets are not maintainable'** is 6%likely to occur as a result of implementation risks related to the cost of the security system, 6 out of 68 indicated 7%, 11 thought8%, 18 answered 9%, 15 chose 10%, 6 believed 12%, 2 indicated 14%, 1 chose 18%, 7 answered 20%, and 1 out of 68 indicated 40%.

Histogram	Mean & Standard Deviation
 Figure 7-37 Histogram for Rm9	The likelihood of Rm9 ranging from 0-50% on **implementation risk has** a mean of 0.11.The distribution curve of this variable shows that it is positively skewed, with a skewness of 3.245. It has a standard deviation of .052.

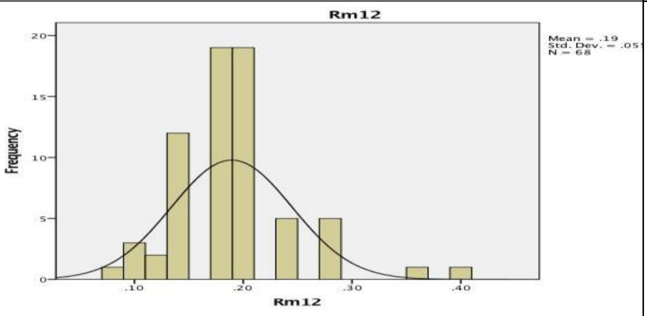
Two respondents answered that **risk factor (Rm10) 'lack of operationalisation'** is 12%likely to occur as a result of implementation risks related to the cost of the security system, 12 out of 68 thought 14%, 23 indicated 18%, 19 thought20%, 5 chose 24%, 4 indicated 28%, 1 thought 36%, and 2 out of 68 believed 40%.

Histogram	Mean & Standard Deviation
 Figure 7-38 Histogram for Rm10	The likelihood of Rm10 ranging from 0-50% on **initiation risk has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.931. It has a standard deviation of .055.

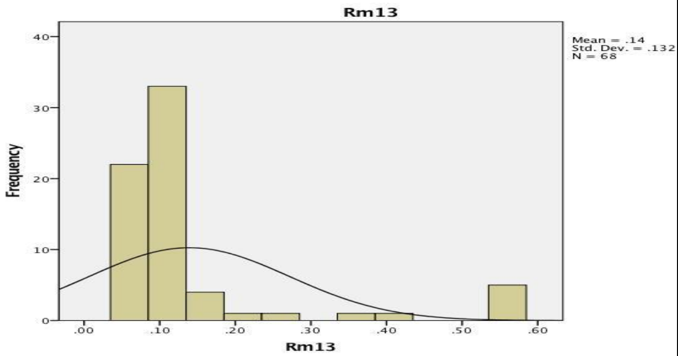
Two respondents thought that **risk factor (Rm11) 'delays due to physical infrastructure'** is 7%likely to occur as a result of implementation risks related to the cost of the security system, 2 out of 68 indicated 8%, 1 answered 9%, 2 thought10%, 2 chose 12%, 12 indicated 14%, 18 believed 18%, 17 answered 20%, 6 chose 24%, 4 thought 28%, 1indicated 36%, and 1 out of 68 answered 40%.

Histogram	Mean & Standard Deviation
 Figure 7-39 Histogram for Rm11	The likelihood of Rm11 ranging from 0-50% on **implementation risk has** a mean of 0.18.The distribution curve of this variable shows that it is positively skewed, with a skewness of .851. It has a standard deviation of .06.

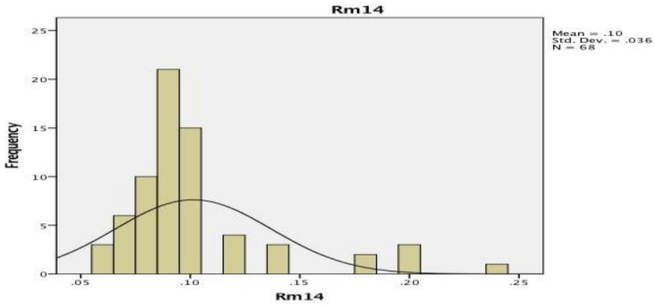
A single respondent indicated that **risk factor (Rm12) 'unexpected project scope expansions**' is 8%likely to occur as a result of implementation risks related to the cost of the security system, 3 out of 68 indicated 10%, 2 chose 12%, 12 thought14%, 19 answered 18%, 19 indicated20%, 5 believed 24%, 5 thought28%, 1 chose 36%, and 1 out of 68 indicated 40%.

Histogram	Mean & Standard Deviation
 Figure 7-40 Histogram for Rm12	The likelihood of Rm12 ranging from 0-40% on **implementation risk has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.182. It has a standard deviation of .055.

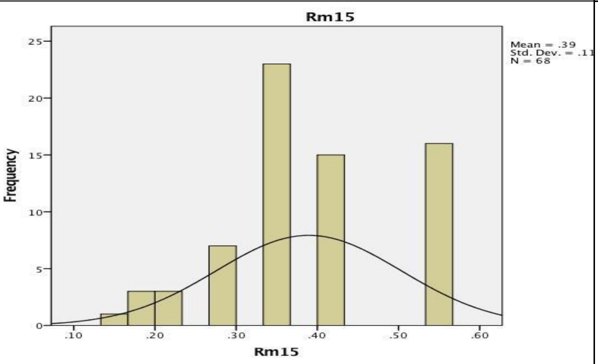
Just 1 out of the 68 respondents indicated that **risk factor (Rm13) 'product solution is complex to implement** 'is 6%likely to occur as a result of implementation risks related to the cost of the security system, 11 out of 68 thought 7%, 10 answered 8%, 15 chose 9%, 14 indicated 10%, 4 out of 68 believed 12%, 3 chose 14%, 1 answered 18%, 1 thought 20%, 1indicated 24%, 1 chose 36%, 1 answered 40%, and 5 out of 68 indicated 56%.

Histogram	Mean & Standard Deviation
 Figure 7-41 Histogram for Rm13	The likelihood of Rm13 ranging from 0-60% on **implementation risk has** a mean of 0.14.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.621. It has a standard deviation of .132.

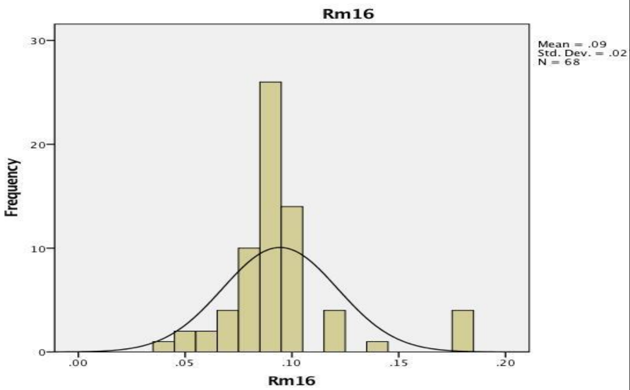
A total of 3 out of the 68 respondents indicated that **risk factor (Rm14)** 'staff turnover' is 6%likely to occur as a result of implementation risks related to the cost of the security system, 6 out of 68 indicated 7%, 10 thought8%, 21 answered 9%, 15 thought10%, 4 chose 12%, 3 believed 14%, 2 indicated 18%, 3 thought 20% and only 1 out 68answered 24%.

Histogram	Mean & Standard Deviation
 Figure 7-42 Histogram for Rm14	The likelihood of Rm14 ranging from 0-30% on **implementation risk has** a mean of 0.10.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.110. It has a standard deviation of .036.

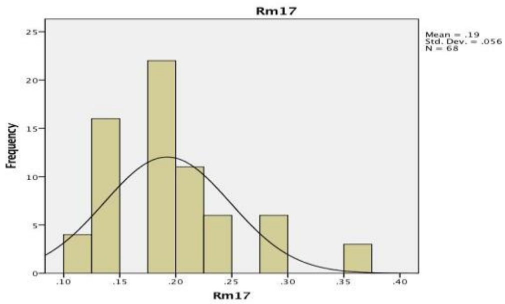
A single respondent indicated that **risk factor (Rm15**) '**insufficient financial resources**' is 14%likely to occur as a result of implementation risks related to the cost of the security system, 3 out of 68 thought 18%, 3 indicated 20%, 7 answered 28%, 23 chose 36%, 15 believed 40%, and 16 out of 68 thought 56%.

Histogram	Mean & Standard Deviation
 Figure 7-43 Histogram for Rm15	The likelihood of Rm15 ranging from 0-60% on **implementation risk has** a mean of 0.39.The distribution curve of this variable shows that it is positively skewed, with a skewness of .065. It has a standard deviation of .114.

Only one respondent answered that **risk factor (Rm16) 'lack of training on the system** 'is 4%likely to occur as a result of implementation risks related to the cost of the security system, 2 out of 68 indicated 5%, 2 thought6%, 4 chose 7%, 10 thought8%, 26 answered 9%, 14 indicated 10%, 4 believed 12%, 1 chose 14%, and 4 out of 68 indicated 18%.

Histogram	Mean & Standard Deviation
 Figure 7-44 Histogram for Rm16	The likelihood of Rm16 ranging from 0-20% on **implementation risk has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.699. It has a standard deviation of .027.

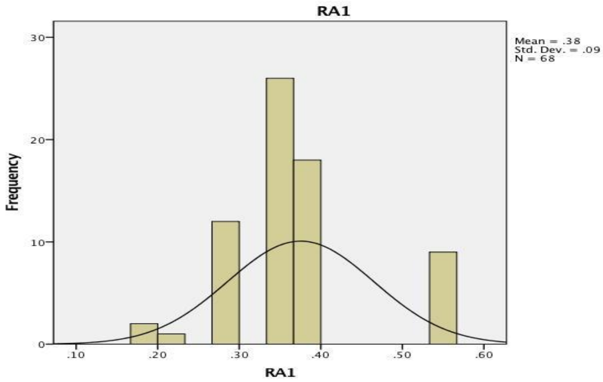
A total of 4 out of the 68 respondents indicated that **risk factor (Rm17) 'poor quality management's** 12%likely to occur as a result of implementation risks related to the cost of the security system, 16 out of 68 thought14%, 22 answered 18%, 11 chose %, 6 indicated 24%, 6 answered 28%, and 3 out of 68 thought 36%.

Histogram	Mean & Standard Deviation
 Figure 7-45 Histogram for Rm17	The likelihood of Rm17 ranging from 0-40% on **implementation risk has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.286. It has a standard deviation of .056.

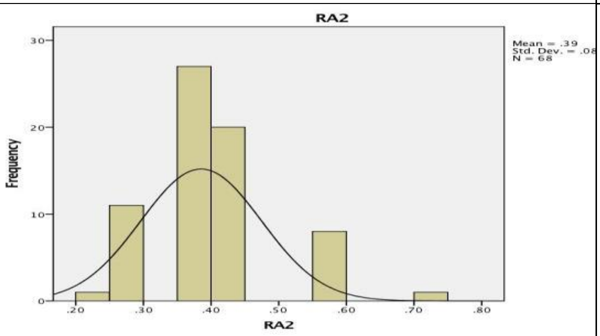
7.3.3 Influence of Risks o*n* the Acquisition *Cost* (RAx*)*

This section provides the survey results for the impact of the acquisition risks on the cost of security systems. The likelihood of each risk factor is presented.

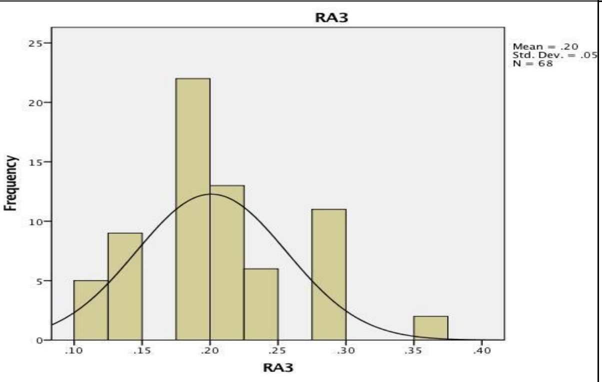
Two respondents indicated that **risk factor (RA1) 'lack of funds**' is 18%likely to occur as a result of acquisition risks related to the cost of the security system, 1 out of 68 answered 20%, 12 thought28%, 26 chose 36%, 18 answered 40%, and 9 out of 68 thought 56%.

Histogram	Mean & Standard Deviation
 Figure 7-46 Histogram for RA1	The likelihood of RA1 ranging from 0-50% on **acquisition risk has** a mean of 0.38.The distribution curve of this variable shows that it is positively skewed, with a skewness of .557. It has a standard deviation of .09.

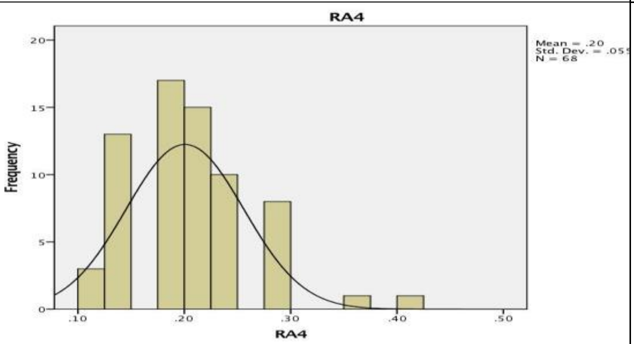
Only one respondent thought that **risk factor (RA2) 'running out of funds'**is20%likely to occur as a result of acquisition risks related to the cost of the security system, 11 out of 68 indicated 28%, 27 answered 36%, 20 chose 40%, 8 thought 56%, and only 1 out of 68 answered 72%.

Histogram	Mean & Standard Deviation
 Figure 7-47 Histogram for RA2	The likelihood of RA2 ranging from 0-80% on **acquisition risk has** a mean of 0.39.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.309. It has a standard deviation of .089.

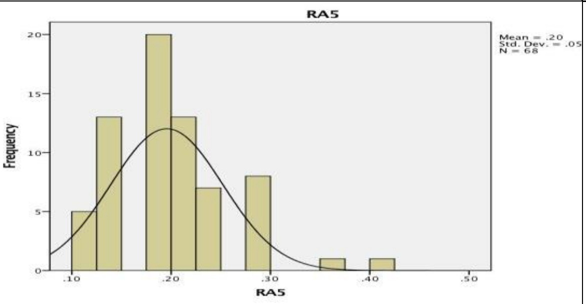
Five respondents indicated that **risk factor (RA3) 'continually changing requirements**' is 12%likely to occur as a result of acquisition risks related to the cost of the security system, 9 out of 68 indicated 14%, 22 thought18%, 13 answered 20%, 6 chose 24%, 11 thought 28%, and 2 out 68 indicated 36%.

Histogram	Mean & Standard Deviation
 Figure 7-48 Histogram for RA3	The likelihood of RA3 ranging from 0-40% on **acquisition risk has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of .820. It has a standard deviation of .055.

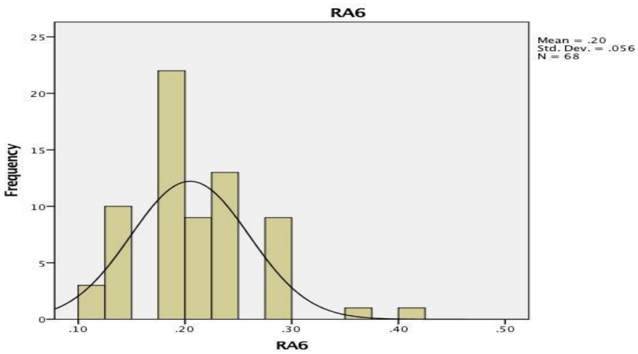
A total of 3 out of the 68 respondents indicated that **risk factor (RA4) 'market development pace rendering products obsolete** 'is 12%likely to occur as a result of acquisition risks related to the cost of the security system, 13 out of 68 answered 14%, 17 thought18%, 15 chose 20%, 10 believed 24%, 8 thought28%, 1 indicated 36%, and only 1 out of 68 answered 40%.

Histogram	Mean & Standard Deviation
 Figure 7-49 Histogram for RA4	The likelihood of RA4 ranging from 0-50% on **acquisition risk has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.085. It has a standard deviation of .055.

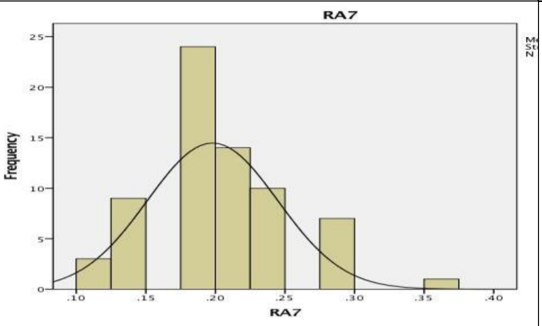
A total of 5 out of the 68 respondents thought that **risk factor (RA5) 'changing priorities** 'is 12%likely to occur as a result of acquisition risks related to the cost of the security system, 13 out of 68 indicated 14%, 20 chose 18%, 13 answered 20%, 7 thought24%, 8 answered 28%, 1 chose 36%, and only 1 out of 68 indicated 40%.

Histogram	Mean & Standard Deviation
 Figure 7-50 Histogram for RA5	The likelihood of RA5 ranging from 0-50% on **acquisition risk has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.192. It has a standard deviation of .056.

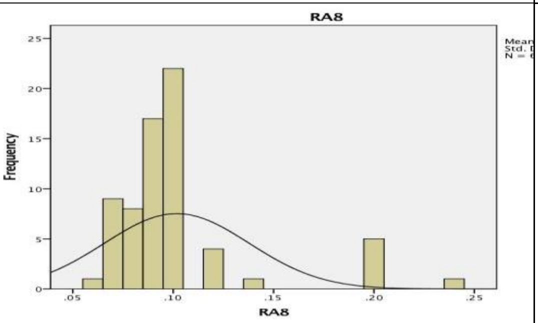
Three respondents indicated that **risk factor (RA6) 'government rule changes'** is 12%likely to occur as a result of acquisition risks related to the cost of the security system, 10 out of 68 indicated 14%, 22 chose 18%, 9 thought20%, 13 indicated 24%, 9 answered 28%, 1 chose 36%, and only 1 out of 68 thought 40%.

Histogram	Mean & Standard Deviation
 Figure 7-51 Histogram for RA6	The likelihood of RA6 ranging from 0-50% on **acquisition risk has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of .965. It has a standard deviation of .056.

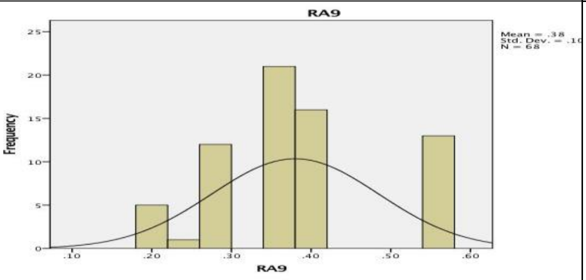
Three respondents indicated that **risk factor (RA7) 'hardware and software defects** 'is 12%likely to occur as a result of acquisition risks related to the cost of the security system, 3 out of 68 thought 14%, 24 answered 18%, 14 chose 20%, 10 believed 24%, 7indicated 28%, and only 1 out of 68 thought 36%.

Histogram	Mean & Standard Deviation
 Figure 7-52 Histogram for RA7	The likelihood of RA7 ranging from 0-40% on **acquisition risk has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of .829. It has a standard deviation of .047.

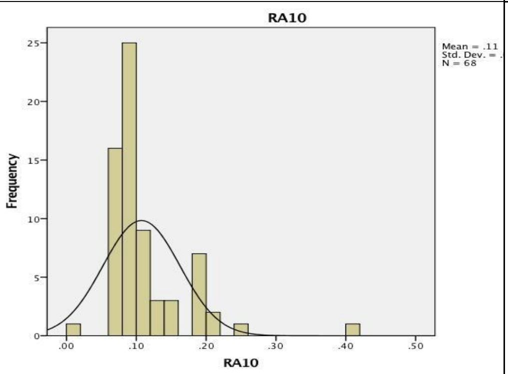
Only 1 out of the 68 respondents thought that **risk factor (RA8) ‘integration issues** ‘is 6%likely to occur as a result of acquisition risks related to the cost of the security system, 9 out of 68 indicated 7%, 8 chose 8%, 17 answered 9%, 22 thought10%, 4 indicated 12%, 1 believed 14%, 5 chose 20%, and only 1 out of 68 thought 24%.

Histogram	Mean & Standard Deviation
 Figure 7-53 Histogram for RA8	The likelihood of RA8 ranging from 0-30% on **acquisition risk has** a mean of 0.10.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.290. It has a standard deviation of .036.

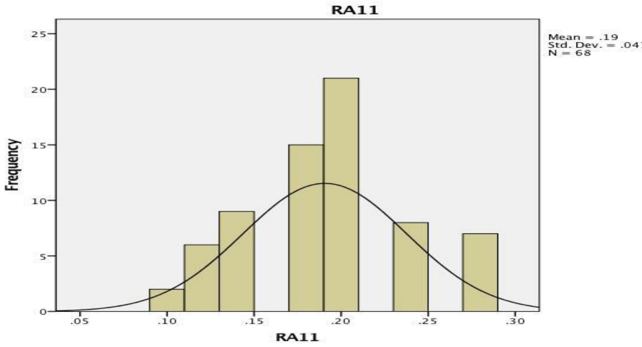
A total of 5 out of the 68 respondents indicated that **risk factor (RA9) ‘inaccurate cost forecasts** ‘is 20%likely to occur as a result of acquisition risks related to the cost of the security system, 1 out of 68 thought 24%, 12 answered 28%, 21 chose 36%, 16 thought 40%, and 13 out of 68 indicated 56%.

Histogram	Mean & Standard Deviation
 Figure 7-54 Histogram for RA9	The likelihood of RA9 ranging from 0-60% on **acquisition risk has** a mean of 0.38.The distribution curve of this variable shows that it is positively skewed, with a skewness of .424. It has a standard deviation of .105.

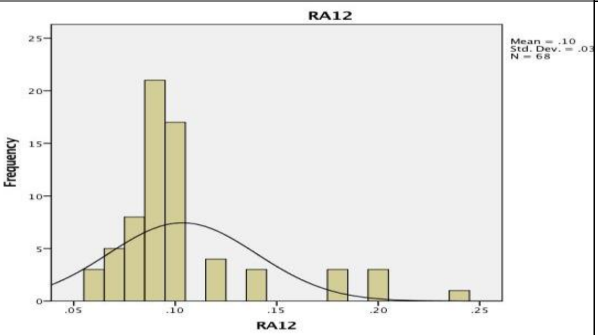
Just one respondent indicated that **risk factor (RA10) 'exchange rate variability not managed well** 'is 1%likely to occur as a result of acquisition risks related to the cost of the security system, 1 out of 68 chose 6%, 15 answered 7%, 5 thought 8%, 20 indicated 9%, 9 chose 10%, 3 believed 12%, 3 out of 68 thought 14%, 7 answered 18%, 2 indicated 20%, 1 thought 24% and only 1 out of 68 chose 40%.

Histogram	Mean & Standard Deviation
 Figure 7-55 Histogram for RA10	The likelihood of RA10 ranging from 0-50% on **acquisition risk has** a mean of 0.11.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.725. It has a standard deviation of .055.

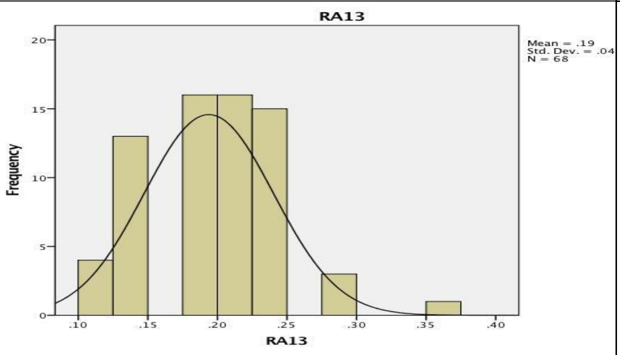
Two respondents indicated that **risk factor (RA11) 'failure to integrate with existing systems** 'is 10%likely to occur as a result of acquisition risks related to the cost of the security system, 6 out of 68 thought 12%, 9 answered 14%, 15 chose 18%, 21 thought20%, 8 indicated 24%, and 7 out 68 answered 28.

Histogram	Mean & Standard Deviation
 Figure 7-56 Histogram for RA11	The likelihood of RA11 ranging from 0-30% on **acquisition risk has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of .178. It has a standard deviation of .047.

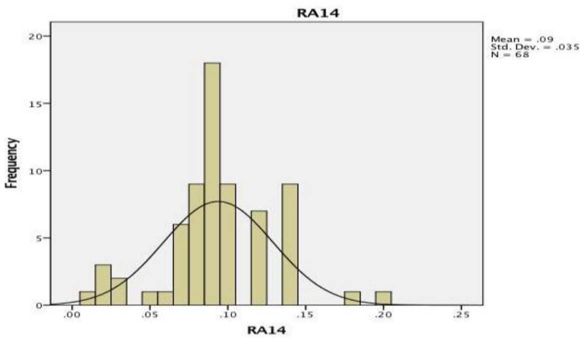
A total of 3 out of the 68 respondents indicated that **risk factor (RA12) ‘unavailability of adequate test environment** ‘is 6%likely to occur as a result of acquisition risks related to the cost of the security system, 5 out of 68 answered 7%, 8 believed 8%, 21 thought9%, 17 answered 10%, 4 indicated 12%, 3 chose14%, 3 thought18%, 3 answered 20%, and only 1 out of 68 chose 24%.

Histogram	Mean & Standard Deviation
 Figure 7-57 Histogram for RA12	The likelihood of RA12 ranging from 0-30% on **acquisition risk has** a mean of 0.10.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.954. It has a standard deviation of .036.

Four respondents indicated that **risk factor (RA13) ‘failure to integrate components** ‘is 12% likely to occur as a result of acquisition risks related to the cost of the security system, 13 out of 68 answered 14%, 16 thought18%, 16 chose 20%, 15 indicated 24%, 3 answered 28%, and only 1 out of 68 thought 36%.

Histogram	Mean & Standard Deviation
 Figure 7-58 Histogram for RA13	The likelihood of RA13 ranging from 0-40% on **acquisition risk has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of .058. It has a standard deviation of .047.

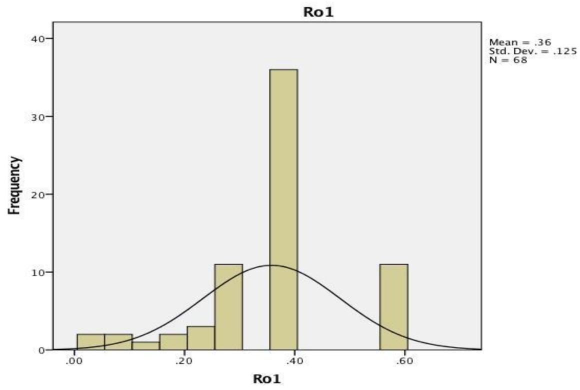
Only 1 out of the 68 respondents indicated that **risk factor (RA14) 'security asset disrupts operations** 'is 1%likely to occur as a result of acquisition risks related to the cost of the security system, 3 out of 68 chose 2%, 2 answered 3%, 1 thought 5%, 1 indicated 6%, 6 answered 7%, 9 believed 8%, 18 chose 9%, 9 indicated 10%, 7 answered 12%, 9 thought 14%, 1 chose18%, and only 1 out of 68 believed 20%.

Histogram	Mean & Standard Deviation
 Figure 7-59 Histogram for RA14	The likelihood of RA14 ranging from 0-30% on **acquisition risk has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed, with a skewness of .108. It has a standard deviation of .035.

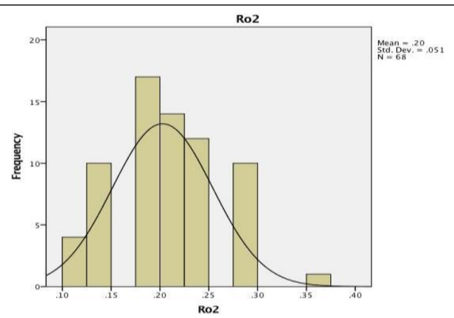
7.3.4 Influence of Risks o*n* the Operations and Maintenance *Costs* (Rox*)*

Survey results regarding the impact of the operations and maintenance risks on the cost of security systems are presented here. The likelihood of each risk factor is indicated.

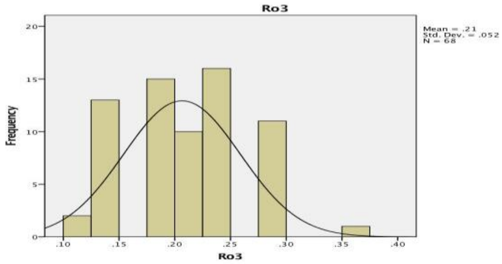
Only 1 out of the 68 respondents indicated that **risk factor (Ro1) 'lack of poor policy performance for monitoring the system** 'is 3%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 1 out of 68 answered 5%, 1 thought 8%, 1 answered 9%, 1 chose 12%, 2 indicated 20%, 3 believed 24%, 11chose 28%, 20 thought 36%, 16 answered 40%, and 11 out of 68 indicated 56%.

Histogram	Mean & Standard Deviation
 Figure 7-60 Histogram for Ro1	The likelihood of Ro1 ranging from 0-60% on **operations and maintenance risks has** a mean of 0.63, the distribution curve of this variable shows that it is negatively skewed, with a skewness of -.350. It has a standard deviation of .125.This is an indication that the respondents agree that **Ro1**has a high tendency of taking place

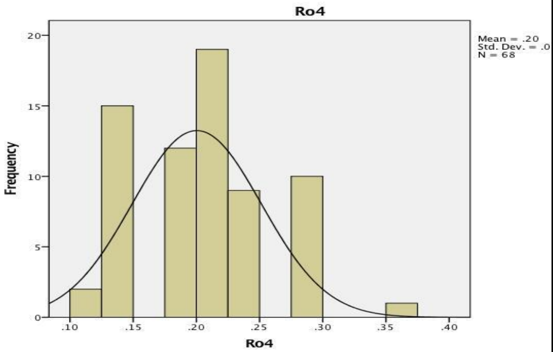
A total of 4 out of the 68 respondents indicated that **Risk Factor (Ro2) 'poor implementation which leads to technical risks** 'is 12%likely to occur as a result of operations and maintenance risks related to the cost of the security system,10 out of 68 answered 14%, 17 chose 18%, 14 thought20%, 12 indicated 24%, 10 believed 28%, and only 1 out of 68 thought 36%.

Histogram	Mean & Standard Deviation
 Figure 7-61 Histogram for Ro2	The likelihood of Ro2 ranging from 0-40% on **operations and maintenance risks has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of .481. It has a standard deviation of .051.

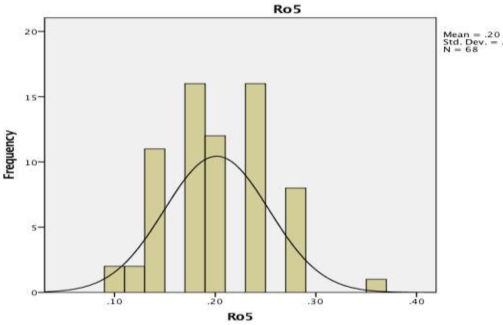
Two respondents indicated that **risk factor (Ro3) 'failure to address priority conflicts** 'is 12%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 13 out of 68 thought 14%, 15 answered 18%, 10 thought20%, 16 chose 24%, 11 answered 28%, and only 1 out of 68 indicated36%.

Histogram	Mean & Standard Deviation
 Figure 7-62 Histogram for Ro3	The likelihood of Ro3 ranging from 0-40% on **operations and maintenance risks** has a mean of 0.21.The distribution curve of this variable shows that it is positively skewed, with a skewness of .341. It has a standard deviation of .052.

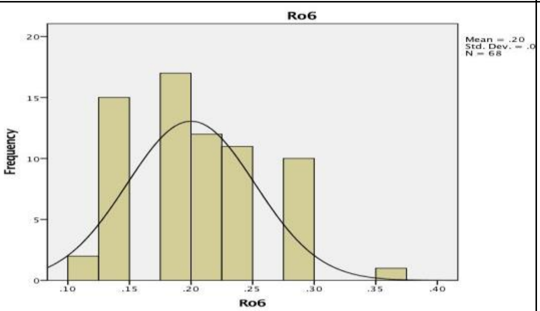
Just 2 out of the 68 respondents indicated that **risk factor(Ro4) 'failure to allocate and resolve the responsibilities** 'is 12%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 15 out of 68 thought 14%, 12 chose 18%, 19 indicated 20%, 9 answered 24%, 10believed 28% and only 1 out of 68 thought 36%.

Histogram	Mean & Standard Deviation
 Figure 7-63 Histogram for Ro4	The likelihood of Ro4 ranging from 0-40% on **operations and maintenance risks** has a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of .605. It has a standard deviation of .051.

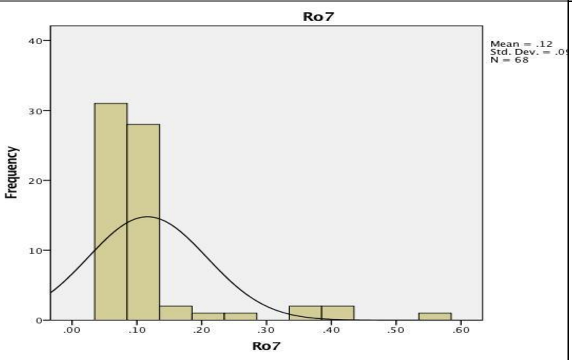
Two respondents indicated that **risk factor(Ro5) 'insufficient human and financial resources** 'is 10%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 2 out of 68 believed 12%, 11 answered 14%, 16 indicated 18%, 12 thought20%, 16 chose 24%, 8 answered 28%, and only 1 out of 68 indicated 36%.

Histogram	Mean & Standard Deviation
 Figure 7-64 Histogram for Ro5	The likelihood of Ro5 ranging from 0-40% on **operations and maintenance risks has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of .316. It has a standard deviation of .052.

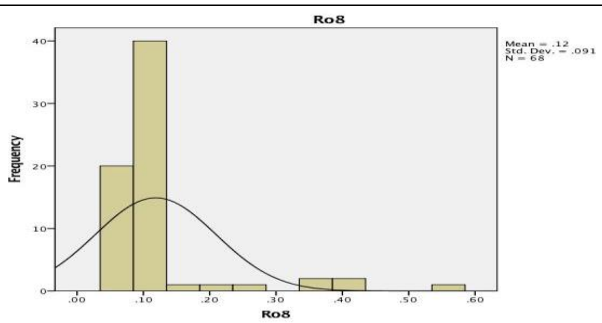
Only 2 out of the 68 respondents thought that **risk factor(Ro6) 'inadequate subject training** 'is 12%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 15 out of 68 indicated 14%, 17 thought18%, 12 answered 20%, 11 chose 24%, 10 believed 28%, and only 1 out of 68 indicated 36%.

Histogram	Mean & Standard Deviation
 Figure 7-65 Histogram for Ro6	The likelihood of Ro6 ranging from 0-40% on **operations and maintenance risks has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of .606. It has a standard deviation of .052.

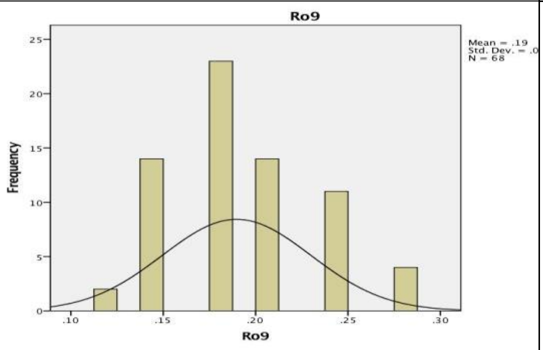
Just 2 out of the 68 respondents indicated that **risk factor(Ro7) 'inadequate resource planning** 'is 6%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 9 out of 68 chose 7%, 20 answered 8%, 12 indicated 9%, 12 thought 10%, 4 indicated 12%, 2 chose 14%, 1 out of 68 believed 20%, 1 indicated 24%, 2 answered 36%, 2 thought 40% and only 1 out of 68 chose 56%.

Histogram	Mean & Standard Deviation
 Figure 7-66 Histogram for Ro7	The likelihood of Ro7 ranging from 0-60% on **operations and maintenance risks has** a mean of 0.12. The distribution curve of this variable shows that it is positively skewed, with a skewness of 3.228. It has a standard deviation of .092.

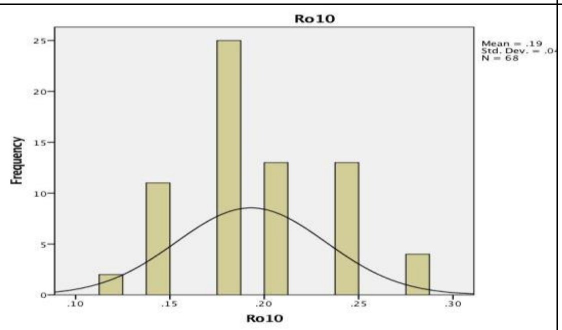
A total of 4 out of the 68 respondents indicated that **risk factor(Ro8) 'poor communication in team's** 6%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 8 out of 68 answered 7%, 8 out of 68 thought 8%, 16 chose 9%, 18 answered 10%, 6 believed 12%, 1 indicated 14%, 1 answered 20%, 1 chose 24%, 2 thought 36%, 2 indicated 40%, and only 1 out of 68 answered 56%.

Histogram	Mean & Standard Deviation
 Figure 7-67 Histogram for Ro8	The likelihood of Ro8 ranging from 0-60% on **operations and maintenance risks has** a mean of 0.12.The distribution curve of this variable shows that it is positively skewed, with a skewness of 3.229. It has a standard deviation of .091.

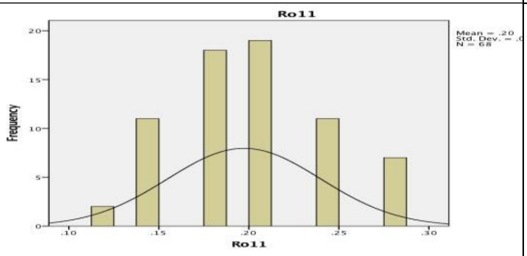
Two respondents indicated that **risk factor(Ro9) 'security assets not fit for purpose** 'is 12%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 14 out of 68 indicated 14%, 23 chose 18%, 14 thought20%, 11 chose 24%, and 4 out 68 answered 28%.

Histogram	Mean & Standard Deviation
 Figure 7-68 Histogram for Ro9	The likelihood of Ro9 ranging from 0-30% on **operations and maintenance risks has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of .0459. It has a standard deviation of .04.

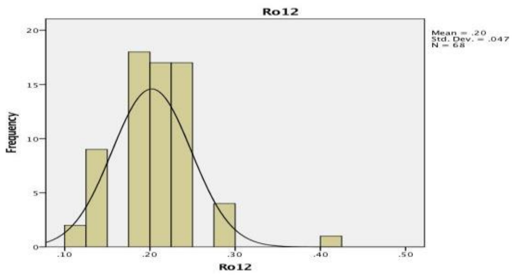
Only 2 out of the 68 respondents indicated that **risk factor(Ro10) 'un-scalability of system** 'is 12%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 11 out of 68 chose14%, 25 answered 18%, 13 thought20%, 13 chose 24%, and 4 out 68 indicated 28%.

Histogram	Mean & Standard Deviation
 Figure 7-69 Histogram for Ro10	The likelihood of Ro10 ranging from 0-30% on **operations and maintenance risks has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of .379. It has a standard deviation of .04.

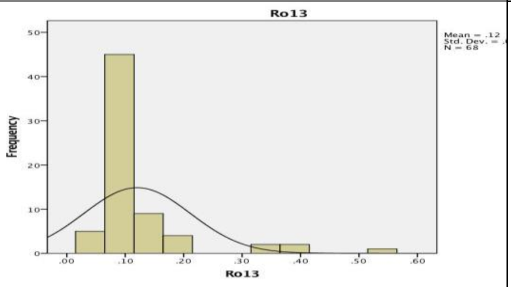
Two respondents answered that **risk factor(Ro11) 'lack of interoperability** 'is 12%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 11 out of 68 indicated 14%, 18 thought18%, 19 chose 20%, 11 indicated 24%, and 7 out 68 thought28%.

Histogram	Mean & Standard Deviation
 Figure 7-70 Histogram for Ro11	The likelihood of Ro11 ranging from 0-30% on **operations and maintenance risks has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of .340. It has a standard deviation of .043.

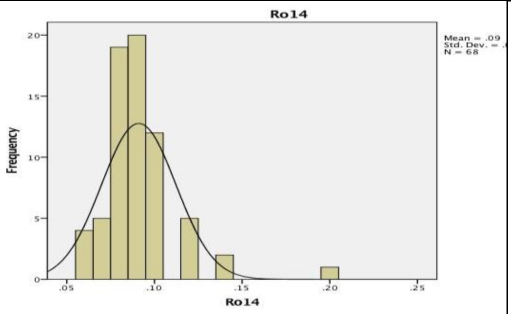
Just 2 out of the 68 respondents thought that **risk factor (Ro12) 'physical security assets are not compliant with regulatory standards and best practices**' is 12%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 9 out of 68 indicated 14%, 18 chose 18%, 17 answered 20%, 17 believed 24%, 4 chose 28%, and only 1 out of 68 indicated 40%.

Histogram	Mean & Standard Deviation
 Figure 7-71 Histogram for Ro12	The likelihood of Ro12 ranging from 0-50% on **operations and maintenance risks has** a mean of 0.20.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.090. It has a standard deviation of .047.

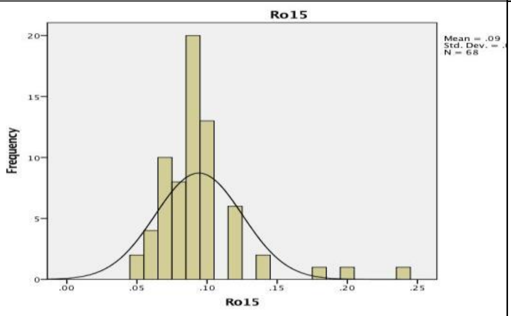
A single respondent indicated that **risk factor(Ro13) 'lack of quality team's** 4%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 4 out of 68 thought 6%, 8 chose 7%, 7 chose 8%, 20 answered 9%, 10 believed 10%, 5 indicated 12%, 4 thought 14%, 3 chose 18%, 1 out of 68 indicated 20%, 2 answered 36%, 2 chose 40%, and only 1 out of 68 indicated 56%.

Histogram	Mean & Standard Deviation
 Figure 7-72 Histogram for Ro13	The likelihood of Ro13 ranging from 0-60% on **operations and maintenance risks has** a mean of 0.12.The distribution curve of this variable shows that it is positively skewed, with a skewness of 3.112. It has a standard deviation of .091.

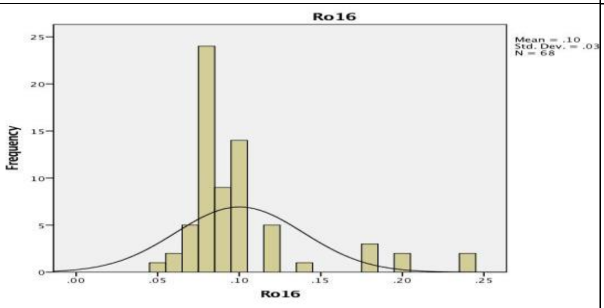
A total of 4 out of the 68 respondents thought that **risk factor(Ro14) 'lack of stability** 'is 6%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 5 out of 68 indicated 7%, 19 answered 8%, 20 thought9%, 12 believed 10%, 5 chose 12%, 2 answered 14%, and only 1 out of 68 indicated 20%.

Histogram	Mean & Standard Deviation
 Figure 7-73 Histogram for Ro14	The likelihood of Ro14 ranging from 0-30% on **operations and maintenance risks has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.355. It has a standard deviation of .021.

Just 2 out of the 68 respondents thought that **risk factor(Ro15) 'no support from manufacture** 'is 5%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 4 out of 68 indicated 6%, 10 thought7%, 8 answered 8%, 20 chose 9%, 13 answered 10%, 6 indicated 12%, 2 believed 14%, 1 chose 18%, 1 indicated 20%, and only 1 out of 68 answered 24%.

Histogram	Mean & Standard Deviation
 Figure 7-74 Histogram for Ro15	The likelihood of Ro15 ranging from 0-30% on **operations and maintenance risks has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.416. It has a standard deviation of .031.

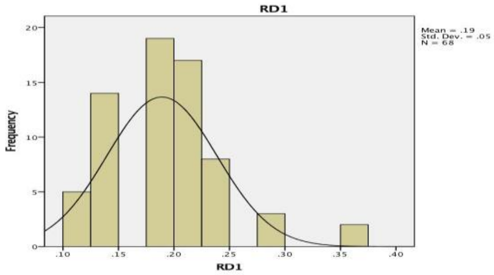
Only 1 out of the 68 respondents indicated that **risk factor(Ro16) ‘change in operation process and policy** ‘is 5%likely to occur as a result of operations and maintenance risks related to the cost of the security system, 2 out of 68 thought 6%, 5 chose 7%, 24answered 8%, 9 chose 9%, 14 out of 68 believed 10%, 5 answered 12%, 1 indicated 14%, 3 thought 18%, 2 chose 20%, and 2 out of 68 indicated 24%.

Histogram	Mean & Standard Deviation
 Figure 7-75 Histogram for Ro16	The likelihood of Ro16 ranging from 0-30% on **operations and maintenance risks has** a mean of 0.10.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.176. It has a standard deviation of .039.

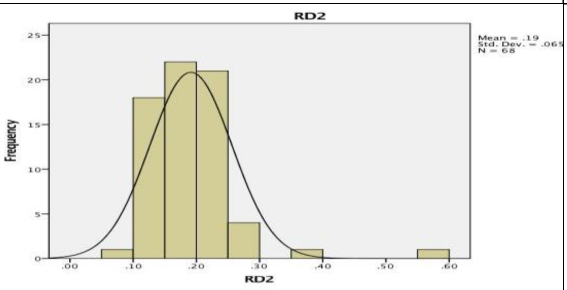
7.3.5 Influence of Risks on the Disposal Costs (RDX)

This section provides the survey results regarding the impact of the disposal risks on the cost of security systems. The likelihood of each risk factor is presented.

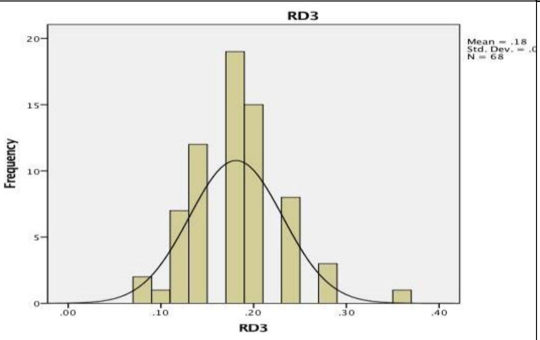
A total of 5 out of the 68 respondents indicated that **risk factor (RD1) ‘health and safety risks during process** ‘is 12% likely to occur as a result of disposal risks related to the cost of the security system, 14 answered 14%, 19 thought18%, 17 chose 20%, 8 indicated 24%, 3 believed 28%, and 2 out of 68 chose 36%.

Histogram	Mean & Standard Deviation
 Figure 7-76 Histogram for RD1	The likelihood of RD1 ranging from 0-40% on **disposal risks has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.254. It has a standard deviation of .05.

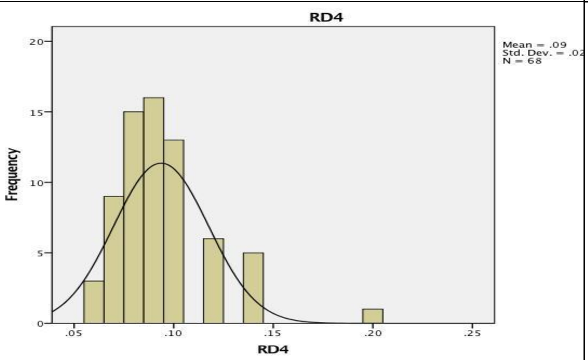
A single respondent indicated that **risk factor(RD2) 'selling costs not feasible'** is 9% likely to occur as a result of disposal risks related to the cost of the security system, 4 out of 68 answered 12%, 14 believed14%, 22 thought18%, 14 indicated 20%, 7 answered 24%, 4 chose 28%, 1 thought 36%, and 1 out of 68 answered 56%.

Histogram	Mean & Standard Deviation
 Figure 7-77 Histogram for RD2	The likelihood of RD2 ranging from 0-60% on **disposal risks has** a mean of 0.19.The distribution curve of this variable shows that it is positively skewed, with a skewness of 3.018. It has a standard deviation of .065.

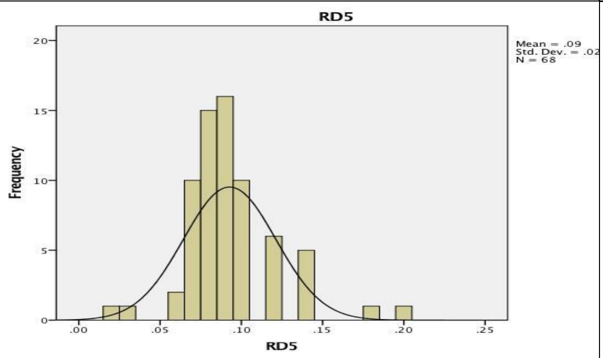
Only 2 out of the 68 respondents thought that **risk factor(RD3) 'environment risks '**is 8%likely to occur as a result of disposal risks related to the cost of the security system, 1 out of 68 indicated 9%, 7 answered 12%, 12 chose 14%, 19 thought18%, 15 indicated 20%, 8 chose 24%, 3 answered 28%, and only 1 out of 68 thought 36%.

Histogram	Mean & Standard Deviation
 Figure 7-78 Histogram for RD3	The likelihood of RD3 ranging from 0-40% on **disposal risks has** a mean of 0.18.The distribution curve of this variable shows that it is positively skewed; with a skewness of .621 It has a standard deviation of .05.

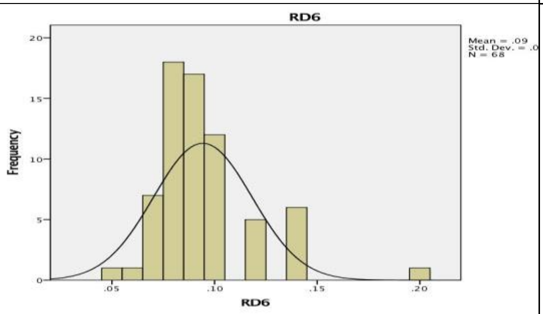
A total of 3 out of the 68 respondents thought that **risk factor(RD4) 'out-dated and damaged equipment'** is6%likely to occur as a result of disposal risks related to the cost of the security system, 9 out of 68 answered 7%, 15 chose 8%, 16 believed 9%, 13 indicated 10%, 6 chose 12%, 5 answered 14%, and only 1 out of 68 thought 20%.

Histogram	Mean & Standard Deviation
 Figure 7-79 Histogram for RD4	The likelihood of RD4 ranging from 0-30% on **disposal risks has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed; with a skewness of 1.739 It has a standard deviation of .024.

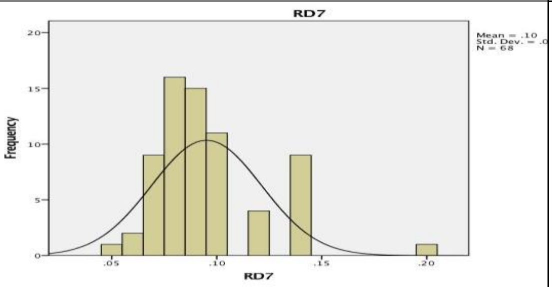
Just 1 out of the 68 respondents indicated that **risk factor(RD5) 'recycling cost risks**' is 2%likely to occur as a result of disposal risks related to the cost of the security system, 1 out of 68 answered 3%, 2 thought6%, 10 indicated 7%, 15 chose 8%, 16 answered 9%, 10 believed 10%, 6 chose 12%, 5 indicated 14%, 1 answered 18%, and 1 out of 68 thought 20%.

Histogram	Mean & Standard Deviation
 Figure 7-80 Histogram for RD5	The likelihood of RD5 ranging from 0-30% on **disposal risks has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed; with a skewness of 1.125 It has a standard deviation of .028.

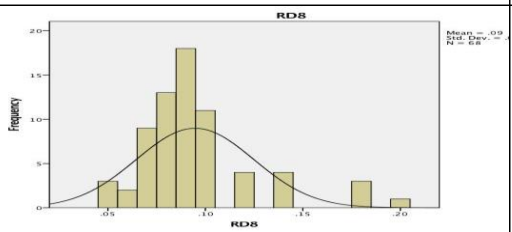
A single respondent answered that **risk factor(RD6) 'environmental management costs** 'is 5%likely to occur as a result of disposal risks related to the cost of the security system, 1 out of 68 chose 6%, 7 indicated 7%, 18 believed 8%, 17 chose9%, 12 answered 10%, 5 thought12%, 6 indicated 14%, and only 1 out of 68 answered 20%.

Histogram	Mean & Standard Deviation
 Figure 7-81 Histogram for RD6	The likelihood of RD6 ranging from 0-30% on **disposal risks has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.734. It has a standard deviation of .024.

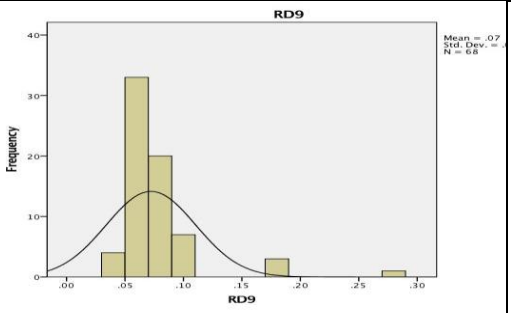
Only 1 out of the 68 respondents indicated that **risk factor(RD7) 'lack of information on disposal of equipment costs'** is 5%likely to occur as a result of disposal risks related to the cost of the security system, 2 out of 68 chose 6%, 9 indicated 7%, 16 thought8%, 15 answered 9%, 11 chose 10%, 4 believed 12%, 9 indicated 14%, and only 1 out of 68 thought 20%.

Histogram	Mean & Standard Deviation
 Figure 7-82 Histogram for RD7	The likelihood of RD7 ranging from 0-20% on **disposal risks has** a mean of 0.10.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.404. It has a standard deviation of .026.

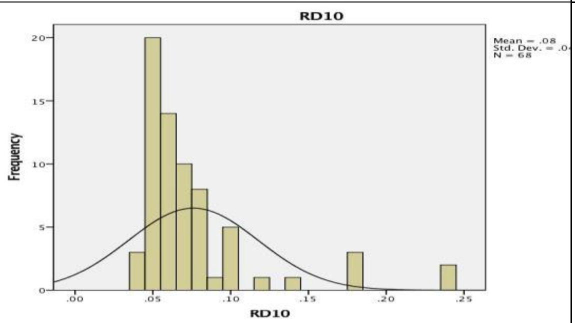
Three respondents indicated that **risk factor(RD8) ‘batteryrisks**’ is 5%likely to occur as a result of disposal risks related to the cost of the security system, 2 out of 68 thought 6%, 9 out of 68 answered 7%, 13 indicated 8%, 18 answered 9%, 11 thought10%, 4 chose 12%, 4 believed 14%, 3 indicated 18%, and only 1 out of 68 chose 20%.

Histogram	Mean & Standard Deviation
 Figure 7-83 Histogram for RD8	The likelihood of RD8 ranging from 0-20% on **disposal risks has** a mean of 0.09.The distribution curve of this variable shows that it is positively skewed, with a skewness of 1.640. It has a standard deviation of .03.

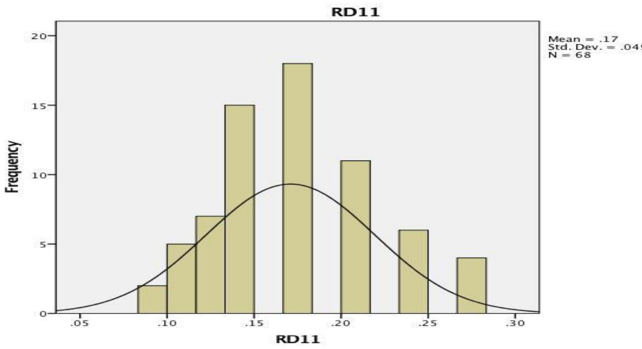
In total, 4 out of the 68 respondents thought that **risk factor(RD9) ‘failure to align with systems** ‘is 4%likely to occur as a result of disposal risks related to the cost of the security system, 21 out of 68 thought 5%, 12 indicated 6%, 10 answered 7%, 10 chose 8%, 4 believed 9%, 3 indicated 10%, 3 thought 18% and only 1 out of 68 answered 28%.

Histogram	Mean & Standard Deviation
 Figure 7-84 Histogram for RD9	The likelihood of RD9 ranging from 0-30% on **disposal risks has** a mean of 0.07.The distribution curve of this variable shows that it is positively skewed, with a skewness of 3.389. It has a standard deviation of .038.

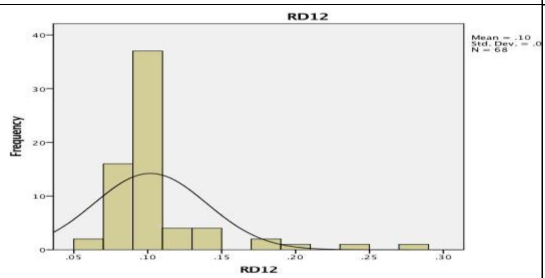
A total of 3 out of the 68 respondents indicated that **risk factor(RD10) 'compliance issues** 'is 4%likely to occur as a result of disposal risks related to the cost of the security system, 20 out of 68 answered 5%, 14 thought6%, 10 chose 7%, 8 indicated 8%, 1 believed 9%, 5 chose 10%, 1 answered 12%, 1 thought14%, 3 chose 18%, and 2 out of 68 indicated 24%.

Histogram	Mean & Standard Deviation
 Figure 7-85 Histogram for RD10	The likelihood of RD10 ranging from 0-30% on **disposal risks has** a mean of 0.08.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.546. It has a standard deviation of .042.

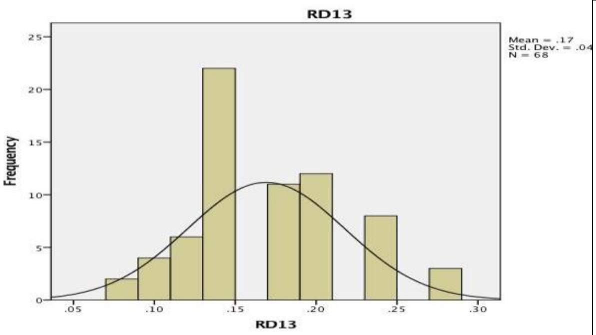
Two respondents answered that **risk factor(RD11) 'ambiguity in process** 'is 9%likely to occur as a result of disposal risks related to the cost of the security system, 5 out of 68 thought 10%, 7out of 68 indicated 12%, 15 chose 14%, 18 answered 18%, 11 believed 20%, 6 indicated 24%, and 8 out of 68 thought 28%.

Histogram	Mean & Standard Deviation
 Figure 7-86 Histogram for RD11	The likelihood of RD11 ranging from 0-30% on **disposal risks has** a mean of 0.17.The distribution curve of this variable shows that it is positively skewed, with a skewness of .439. It has a standard deviation of .049.

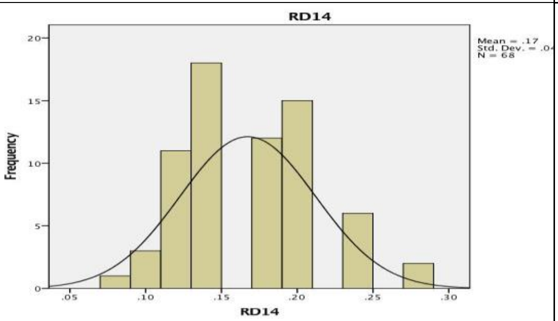
Just 2 out of the 68 respondents indicated that **risk factor(RD12) 'contaminated waste costs**' is 6%likely to occur as a result of disposal risks related to the cost of the security system, 6 out of 68 thought 7%, 10 chose 8%, 24 chose 9%, 13 answered 10%, 4 indicated 12%, 4 believed 14%, 2 thought18%, 1 answered 20%, 1 chose 24%, and 1 out of 68 indicated 28%.

Histogram	Mean & Standard Deviation
 Figure 7-87 Histogram for RD12	The likelihood of RD12 ranging from 0-30% on **disposal risks has** a mean of 0.10.The distribution curve of this variable shows that it is positively skewed, with a skewness of 2.760. It has a standard deviation of .038.

Two respondents indicated that **risk factor (RD13) 'civic amenity sites costs** 'is 8%likely to occur as a result of disposal risks related to the cost of the security system, 4 out of 68 thought 10%, 6 answered 12%, 22 thought14%, 11 chose 18%, 12 believed 20%, 8 indicated 24%, and 3 out of 68 thought 28%.

Histogram	Mean & Standard Deviation
 Figure 7-88 Histogram for RD13	The likelihood of RD13 ranging from 0-30% on **disposal risks has** a mean of 0.17.The distribution curve of this variable shows that it is positively skewed, with a skewness of .446. It has a standard deviation of .049.

Only 1out of the 68 respondents answered that **risk factor(RD14) 'civic amenity sites costs**' is 8%likely to occur as a result of disposal risks related to the cost of the security system, 3 out of 68 indicated 10%, 11 thought12%, 18 chose 14%, 12 believed 18%, 15 answered 20%, 6 thought 24%, and 2 out of 68 indicated 28%.

Histogram	Mean & Standard Deviation
 Figure 7-89 Histogram for RD14	The likelihood of RD14 ranging from 0-30% on **disposal risks has** a mean of 0.17. The distribution curve of this variable shows that it is positively skewed, with a skewness of .443. It has a standard deviation of .045.

7.4 Factor Analysis

Primary and secondary data are evaluated, with factor analysis evolving through many steps in the case of small sample sizes. The groups, (Ri, Rm, Ra, Ro) and factors were sketched for each group independently. Factor analysis was undertaken then over the factors until the final factors emerged. The basic utility of this analysis is to reduce the number of questions for the survey. The questionnaire made of 84 questions in the 1st group "initiation risks (Ri)"; 23 questions in the 2nd group "implementation risks (Rm)"; 16 questions for the third group "acquisition risks (Ra)", and 17 questions in the fourth group "Operations and Maintenance Risks (Ro)".Eighty-four questions have been used thus, despite some questions of the 5th group “Disposition Risks” (Rd) which not been used for this study and also regardless the questions in the front which is the Demographic Questions. Various tests can be used to validate this:

- Kaiser-Meyer-Olkin (KMO)
- Bartlett Test,
- Reliability Test (Cronbach Alpha).

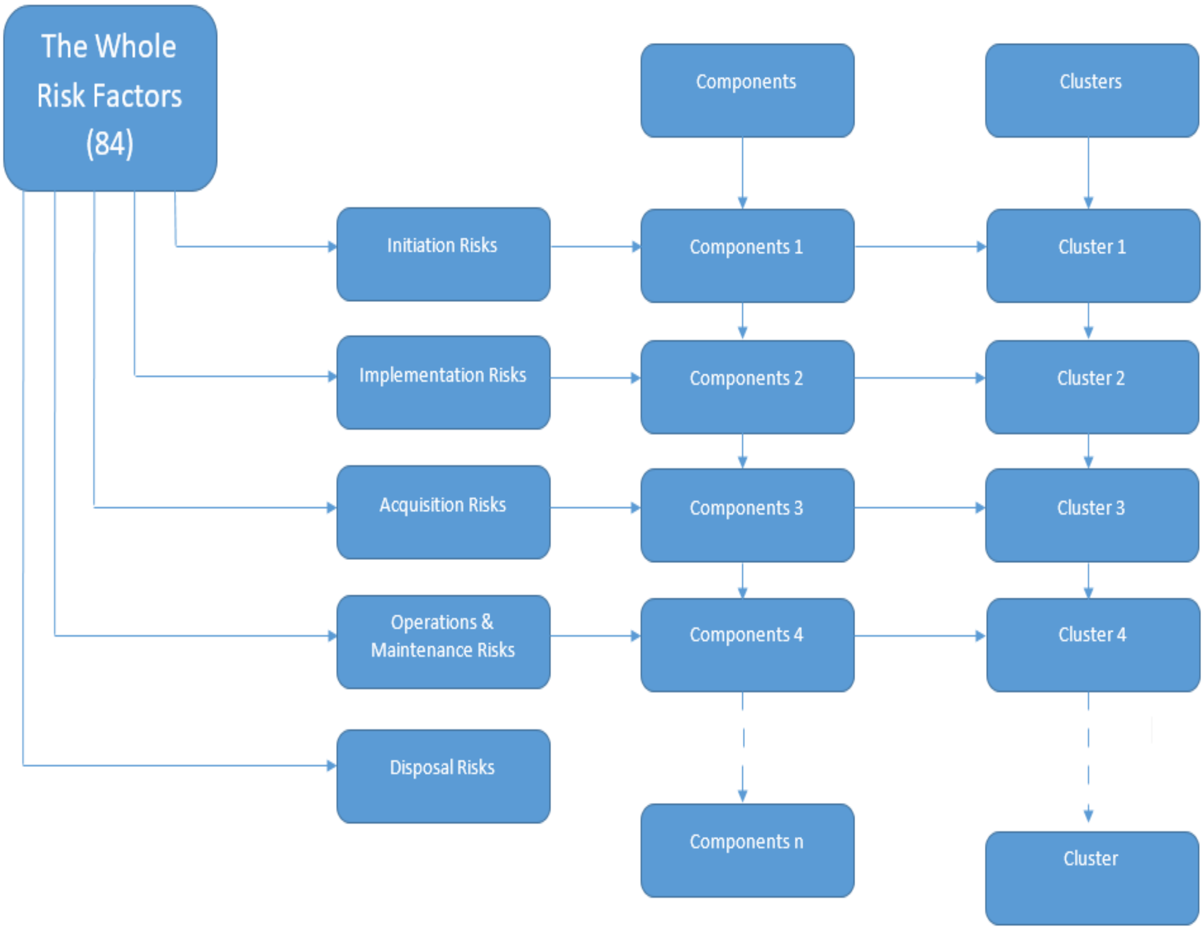


Figure 7.90.The process of factor analysis

DATA SET (Ri)

The researcher for instant selected Initiation risks (Ri) for this analysis of the dataset. The set has a high number of variables a total of 23 variables. For this reason, the decision was made to reduce the number of variables using a factor analysis. Factor analysis follows the principle that the number of observable variables can be reduced to fewer ones that share common variances (Bartholomew, Knott, and Moustaki, 2011).

Exploratory factor analysis (EFA) and Confirmatory factor analysis (CFA) are the two main methods. CFA employs path analysis diagrams whereas the EFA uses testing and dataset predictions (Child, 2006).

The present study considered only the descriptive approach with the selection of principal components. The main reason is that latent (hidden) variables were explored and identified, but the goal was not to confirm or deny any hypothesis concerning the reality of their existence. The analysis was run on SPSS v.23.

Several options were available to run the factor analysis. The desired variables were chosen to include in the analysis. Then, the descriptive dialogue box was chosen with several options. The coefficients option was selected to produce the R-matrix, to produce a matrix for each of the associated correlations. The determinant therewith has to be greater than 0.00001. If it turns out to be lesser than this, then high levels of correlation are assumed and thereafter one of the variables is removed. This can be an arbitrary exercise too as exploring for multicollinearity in the data can raise a few issues of choice. In the next step, KMO and Bartlett's test was chosen, whereupon the value of the KMO should be greater than 0.5 in cases where the sample is adequate.

Then onwards, the “Factor Extraction box” is chosen through component analysis. Although this is not specifically factored analysis, the results obtained from this are usually the same. The display box provides for two measures – the un-rotated factor solution and the scree plot, with the latter being used to determine how many factors to be kept eventually in the analysis.

Thereupon, the model provides a choice regarding the number of factors, which can be either according to a fixed number or with Eigenvalues greater than a specified number by the user. Kaiser recommendation is to use Eigenvalues over one. A Scree plot can then be selected, using such Eigenvalue factors and the results analyzed. If the same number of factors emerge, then the analysis can carry on. If, however, the results are different, then analysis will require input regarding the number of factors required.

Rotation Box provides for interpretation. It maximizes loading of each factor on one of the previously extracted factors, keeping other loadings as the same. Rotation works through changing the absolute values, whilst the differential ones are kept constant. Varimax, equamax, and quartimax are orthogonal rotations, whereas the oblique rotations are direct oblimin and Promax. The decision regarding which ones to use depends on whether the factors are to be related. In case of independent factors, orthogonal rotations should be used, and if the factors are correlated strongly, then direct oblimin may be the choice. In this study, the Varimax option was selected for the factor analysis. In addition, an orthogonal rotation was chosen.

There are some options to be discussed in the options box. SPSS will churn out variables in the same order in which they have been entered. However, a better method would be to sort the variables by size, with another option to suppress the absolute values lesser than a pre-specified value. The default value, in this case, is 0.1. Hence, the values lesser than 0.1 do not feature in the outputs. Given the sample size, this can be changed, and in this research 0.5 was used. In this study, the value was set at 0.5.

Labels have been used for convenience to refer to the variables in the output (e.g. Ri1). SPSS should use the value label (the question itself) in all of the output. Thus, Ri1 represents question 1, Ri2 represents question 2, and Ri23 represents question 23, and so on.

7.4.1 Preliminary Analysis

The Correlation R Matrix shows two crucial segments. The KMO measures the adequacy of the sample whereas the other one is the Bartlett test of sphericity. KMO varies between 0 and 1, thus indicating diffusion in correlations and hence factor analysis can be considered to be inappropriate. Whereas, a value closer to one would indicate that patterns are relatively compact and thus factor analysis would be useful. According to Kaiser(1974), values greater than 0.5 should be used. The values between 0.7 and 0.8 are considered good, and between 0.8 and 0.9 to be excellent, with any values over 0.9 as extremely relevant.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.631
Bartlett's Test of Sphericity	Approx. Chi-Square	896.531
	df	253
	Sig.	.000

Table 7-1: KMO results For Ri

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.665
Bartlett's Test of Sphericity	Approx. Chi-Square	869.166
	df	136
	Sig.	.000

Table 7-2: KMO results For Rm

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.768
Bartlett's Test of Sphericity	Approx. Chi-Square	633.987
	df	91
	Sig.	.000

Table 7-3: KMO results For Ra

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.703
Bartlett's Test of Sphericity	Approx. Chi-Square	1222.899
	df	120
	Sig.	.000

Table 7-4: KMO results For Ro

Bartlett’s measure is for testing the original supposition (the null hypothesis) that the correlation matrix is an identity matrix. Factor analysis would be useful only if there is some relationship between the variables. In case of an identity matrix, all the correlations would be zero. A significance level of 0.05 is used. In this case, the test indicates that this is not an identity matrix and significant relationships do exist. Bartlett’s test is highly significant as the p-value is less than 0.001, and this factor analysis is highly appropriate.

7.4.2 Factor Extraction

7.4.2.1 Initial risks cluster

SPSS picked up, in this case, 23 different linear components at the beginning, with the Eigenvalues depicting the variances that are explained by that component. SPSS also features the values in percentage terms, so Facto 1 explains 21.815% of the total variance, for example. The first few factors account for a large share of the total variance, which progressively then decreases as the output continues. Four remaining factors are picked up then; as they relate to Eigenvalues of more than 1, with the results displayed with the associated count of the variances explained in the column headed Extraction Sums of Squared Loadings. The values of the discarded factors are not included, and thus the table gets blank after the fourth factor. Eigenvalues are shown in the final column regarding the factors after rotation. Factor structure gets optimized due to the rotation and hence the relative impact and importance of the four factors is equalized.

The rotated matrix thus shows the factor loadings for each of the variables onto each factor involved. It's the same information as before, but after rotation. From our findings, some themes emerge. Factor loadings of less than 0.5 have been suppressed and thus do not feature in the output. As output is sorted by size, the variables have listed the order of factor loadings. For all the other sections of the output, labels are suppressed but show up here in order to aid interpretation. Comparing and contrasting this with the un-rotated solution, most of the factors loaded highly onto the first one. Moreover, it can be seen that three factors load very highly onto a single factor, except for two of the questions. Substantive loadings can be checked conveniently due to suppressing loadings of less than 0.5 and ordering the variables by size.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.018	21.815	21.815	5.018	21.815	21.815	3.785	16.455	16.455
2	3.418	14.861	36.676	3.418	14.861	36.676	3.502	15.228	31.683
3	2.829	12.299	48.975	2.829	12.299	48.975	3.233	14.058	45.740
4	1.907	8.290	57.265	1.907	8.290	57.265	2.048	8.905	54.645
5	1.565	6.806	64.070	1.565	6.806	64.070	1.829	7.952	62.597
6	1.385	6.024	70.094	1.385	6.024	70.094	1.433	6.230	68.827
7	1.014	4.409	74.503	1.014	4.409	74.503	1.306	5.676	74.503
8	.878	3.816	78.320						
9	.752	3.271	81.591						
10	.689	2.995	84.586						
11	.592	2.575	87.161						
12	.549	2.386	89.547						
13	.424	1.845	91.391						
14	.407	1.768	93.159						
15	.368	1.598	94.758						
16	.256	1.114	95.872						
17	.221	.962	96.834						
18	.173	.754	97.588						
19	.162	.704	98.292						
20	.140	.607	98.899						
21	.111	.485	99.383						
22	.090	.390	99.773						
23	.052	.227	100.000						

Extraction Method: Principal Component Analysis.

Table 7-5: Factor Extraction for Ri

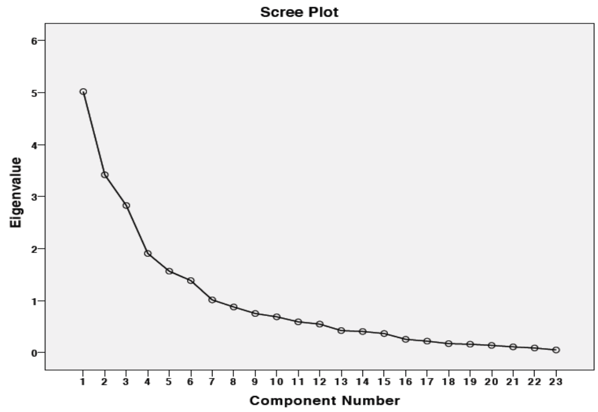


Figure 7-91: Scree Plot for Ri

Before rotation, factor 1 provided for significantly large variance than the other six (21.815% compared to 14.481, 12.290, 8.290, 6.800, 6.024, and 4.409%). However, afterwards, it provides for only 16.455% of the variance (compared to 15.228, 14058, 8.905, 7.952, and 5.670% respectively) which is the case in the Ri.

Rotated Component Matrix[a]

	Component		
	1	2	3
Ri19	.857		
Ri10	.840		
Ri12	.820		
Ri11	-.756		
Ri23	.727		
Ri16		.835	
Ri14		.792	
Ri18		.722	
Ri15		.683	
Ri17		.654	
Ri2		.572	
Ri3			
Ri6			
Ri5			
Ri22			.852
Ri21			.757
Ri20			.742
Ri8			.630
Ri13			.532
Ri7			
Ri9			
Ri4			
Ri1			

Table 7-6: Number of factors after rotation for Ri

The next step is to define the factor scoring for the initiation risk factor (Ri) to assess the individual score on a factor. The analysis uses a simple method called unit-weighted composite, and each variable on the factor contributes according to the weights in figure 7. To achieve this, the mean is taken of only those variables that load on that factor/component. Subsequently, the computation produces unit-weighted composite factor scores (NRi1, NRi2, NRi3) that are not identical to the factors after rotation, as described in figure 7.

- NRi1:

    Ri19: Time management issues

    Ri10: Missing critical activities fromthe scope

    Ri11: Not knowing stakeholders

    Ri12: Technology design failures

    Ri23: Poor negotiation between different stakeholders

- NRi2:

    Ri16: Quality management issues

    Ri14: Unrealistic expectations of stakeholders

    Ri18: Procurement management issues

    Ri15: Schedule flaws

    Ri17: Human resource management issues

    Ri2: Cost overruns due to change of scope

- NRi3:

    Ri22: Contractor factor to the platform

    Ri21: Frequent or Delay design change

    Ri20: Poor workmanship quality

    Ri8:Inter-dependencies are not defined well

    Ri13: Risks in Specification Breakdown

Their tables in the appendix present the correlation between the unit-weighted composite NRi1 and the initiation risk factor variables (Ri23, Ri12, Ri10, and Ri19), which tend to be fairly well related to regression-based factor scores. Also, their tables show the correlation between unit-weighted composite NRi2 and the initiation risk factor variables (Ri16, Ri14, Ri18, Ri15, Ri17, and Ri2),which tend to be fairly well related to regression-based factor scores. There shows the correlation between unit-weighted composite NRi3 and the initiation risk factor variables (Ri22, Ri21, Ri20, Ri8, and Ri13), which tend to be fairly well related to regression-based factor scores except for the risk factors Ri8 and Ri13 however by looking at them, and consider they not related to each other it been suggested further step before jump to the simulation.

7.4.2.2 Interpretation of the emerged initial risk clusters

0	P1 Weights	P2	P3	Alpha	New to the new cluster
Ri3					NRi1 = owner/ stakeholders
Ri4					
Ri5					
Ri6					
Ri8	0.630				
Ri9					
Ri11	-0.756				
Ri14	0.792				
Ri21	0.757				
Ri23	0.727				
Ri15		0.683			NRi2 = management
Ri16		0.835			
Ri17		0.654			
Ri18		0.722			
Ri19		0.857			
Ri20		0.742			
Ri1					NRi3 = contractor/project
Ri2			0.572		
Ri7					
Ri12			0.820		
Ri13			0.532		
Ri22			0.852		

Projects can get off to a highly undesirable and ineffective start because there didn't exist a clear understanding of what had to be done(Wysocki, 2014). A completeness definition has to be articulated and recorded. Generally, it is considered that the clients invariably expect more than project managers can or are willing to deliver. Expectation gap arises due to this gulf in perception and understanding and is generally a result of lack of proper communication. It can be a result of either or both sides assuming that the other has understood or knows completely what the requirement for them is.

The misunderstandings can also arise from the difference between what a client needs and what they want. Correction costs may become significant when this gulf in perception arises. In cases, it may well be that the client gets too hooked or readily sold on a new technology and makes up their mind without any due consideration(Wysocki, 2014). The "wants" of a client are generally connected to a solution to an issue that they can imagine. Needs, however, relate to the actual specific position where the project manager may be in a better position to decide on the solution. However, in cases where this solution – the one that is needed is not communicated effectively, expectation gaps occur. A task of the project manager is to convince the client that what they want is truly what they need too.

There needs to be a dynamic agreement that must become part of a continual process to lead to better project monitoring. Situations generally arise throughout a project's lifecycle that necessitates change resulting froma change in the needs of the client. Hence, the understanding has to be further solidified and agreed on in each milestone meeting for a better way forward.

The influence of design on overall lifecycle costs is usually great. Carefully considering and evaluating at the early stages of design processes can help avoid errors that can form as much as 70% of the overall costs (Wysocki, 2014). Here, DFM (Design for Manufacturing) is a technique that can be deployed which assesses the manufacturability, designing, cost estimation elements in the product development stage.

Latent owner/ stakeholders:

These risks arise due to the owners, whereby they are unable to define to the project manager the total scope of the project, and keep adding or dropping elements from it. This can result in scope creep too where the project manager will be genuinely concerned about the practicality and commerciality of the project, leading to legal wrangling and overall work stoppages (Kerzner, 2001). The owners may fail to explain well the interdependencies and protocols needed to carry out various parts of the project, thus leading to misunderstandings and inefficiencies. Design changes, after agreement earlier, will also pose their own risk elements.

Latent management:

These risks related to management issues during the initial stage. For example, schedule flaws, quality management issues, HRM issues, procurement management issues, time management issues, and poor workmanship quality. Not having the right team composition renders planning to be ineffective (Wysocki, 2014). Stoppages may occur if the vendors are not managed well, as quality issues can result in wrong cost estimation and will lead to knock-on effects. Poor quality work, not only creates issues of performance overall but can also lead to cost overruns and ineffective project completion.

Latent Contractor/project:

These risks related to contractors or the project in general. For example, wrong budget estimation, gold plating, technology design failures, risks in specification breakdown, and other contractor issues. Wrong budget estimation can be due to inaccurate calculations, scheduling, wrong choice of contractors made due to inadequate internal control and checks.

7.4.2.2 Implementation risks cluster

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.458	32.106	32.106	5.458	32.106	32.106	5.203	30.605	30.605
2	3.804	22.376	54.482	3.804	22.376	54.482	3.771	22.184	52.789
3	1.705	10.028	64.610	1.705	10.028	64.610	1.993	11.721	64.610
4	1.197	7.043	71.653						
5	.896	5.271	76.926						
6	.736	4.327	81.152						
7	.633	3.723	84.876						
8	.599	3.522	88.398						
9	.470	2.764	91.160						
10	.382	2.247	93.407						
11	.291	1.711	95.118						
12	.276	1.623	96.742						
13	.255	1.502	98.244						
14	.129	.761	99.005						
15	.089	.524	99.529						
16	.058	.341	99.869						
17	.022	.131	100.000						

Extraction Method: Principal Component Analysis.

Table 7-7: Factor Extraction for Rm

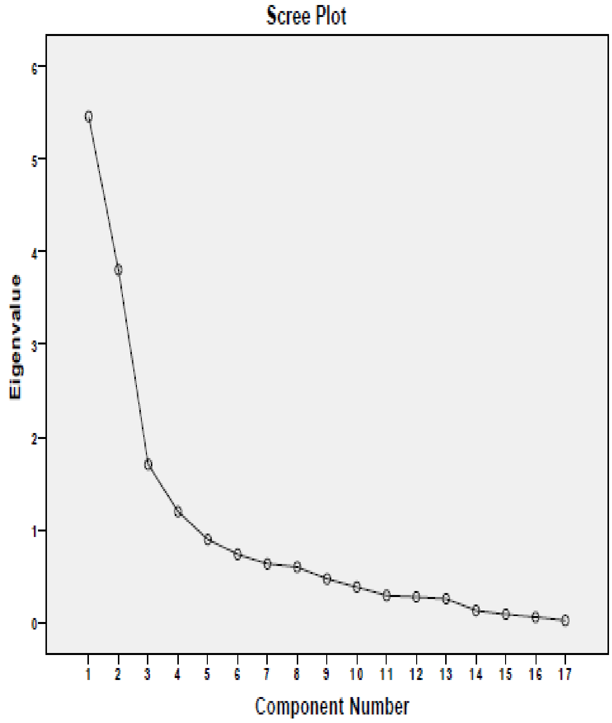


Figure 7-92: Scree Plot for RM

Rotated Component Matrix[a]

	Component		
	1	2	3
Rm8	.821		
Rm6	.815		
Rm5	.782		
Rm10	.774		
Rm12	.706		
Rm1	.692		
Rm3	.690		
Rm7	.665		
Rm11	.663		
Rm13		.894	
Rm9		.864	
Rm2		-.761	
Rm4		.761	
Rm15		-.500	
Rm14			.839
Rm17			.511
Rm16			.510

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 4 iterations.

Table 7-8: Number of factors after rotation for Rm

7.4.2.2 Interpretation of the emerged implementation risk clusters

0	P1 Weights	P2	P3	Alpha	New to the new cluster
Rm1	0.692				NRm1= change and management
Rm2	-0.761				
Rm3	0.890				
Rm4	0.761				
Rm5	0.782				
Rm12	0.706				
Rm14		0.839			NRm2= staffing & RESOURCES
Rm15		- 0.500			
Rm16		0.510			
Rm17		0.511			
Rm6			0.815		NRm3 = system/product issues
Rm7			0.665		
Rm8			0.821		
Rm9			0.864		
Rm10			0.774		
Rm11			0.663		
Rm13			0.894		

Latent change and management:

These risks related to the concept of change and also the management issues during the implementation stage. For example, change in Management, wrong timeframe estimation, change in rules and regulation, poor planning in project management, and delays due to coordination with other contractors.

As the country's rules and regulations have to be adhered to, any changes in the governmental provisions will have to be factored per Kerzner, Project Management: A Systems Approach to Planning, Scheduling, and Controlling(2013). This gets acuter when a new regime or government comes in with its own propensities for commerce and trade, and own stances regarding sustainability initiatives which may be markedly different from those of its predecessor government. Such risks may not be able to be substantially foreseen but need to be factored in somehow into the planning, for only then can the dynamics of the project be leveraged to accommodate the changes required by changing regulations.

Wrong timeframe estimation, resulting from, say inadequate understanding of the scope and extent of work, will lead to losses in the implementation stage and may lead to money being retained by the owners and sponsors due to the delay in implementation stages(Wysocki, 2014). Contractors' timeframes and availability schedules have to be coordinated carefully, as during the implementation stage if the contractors have a shortage of workforce at different levels of expertise, it will hold up the progress of the project.

Latent staffing & Resources:

These risks related to the human resource risks. For examples Staff turnover, insufficient financial resources, lack of training regarding implementation of the systems(Kirkpatrick & Kirkpatrick, 2006), and poor quality management. Budgeting has to be done at the outset, but in cases where during the implementation stage, resources are stretched due to reasons unanticipated, for example, an increase in acquisition prices for the parts of the system being installed, the progress will suffer. Staff involved in setting up the systems must be adequately trained and developed, otherwise, technical issues will arise which will detract from proper implementation according to the plans.

Latent system/product issues:

These risks related directly to the system. For example, the inability or simple lack of identification of the complex functionalities and the associated time required to manage them, information security incidents, legacy components lack adequate documentation, security assets are not maintainable, lack of Operationalization, delays due to physical infrastructure, and product solution is complex to implement. Here, the risks can be mitigated by having backup plans and through strong deals made with the vendors and the contractors that will reduce the potential losses.

7.4.2.2 Operation risks cluster

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.611	41.320	41.320	6.611	41.320	41.320	5.112	31.951	31.951
2	2.952	18.453	59.773	2.952	18.453	59.773	3.105	19.408	51.359
3	1.743	10.896	70.669	1.743	10.896	70.669	2.491	15.568	66.927
4	1.277	7.984	78.653	1.277	7.984	78.653	1.876	11.726	78.653
5	.968	6.047	84.700						
6	.688	4.298	88.998						
7	.492	3.075	92.072						
8	.465	2.903	94.976						
9	.301	1.881	96.857						
10	.151	.943	97.800						
11	.122	.764	98.564						
12	.081	.506	99.069						
13	.067	.418	99.487						
14	.041	.258	99.745						
15	.034	.213	99.958						
16	.007	.042	100.000						

Extraction Method: Principal Component Analysis.

Table 7-9: Factor Extraction for Ro

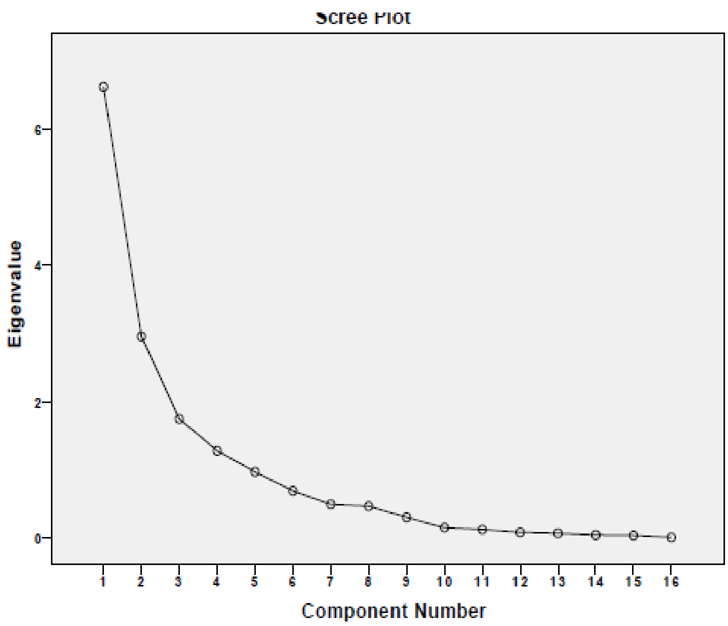


Figure 7-93: Scree Plot for Ro

Rotated Component Matrix[a]

	Component			
	1	2	3	4
Ro6	.952			
Ro4	.916			
Ro5	.915			
Ro2	.911			
Ro3	.707			
Ro9	.645		.580	
Ro8		.984		
Ro7		.982		
Ro13		.954		
Ro12	.429		.755	
Ro10	.574		.713	
Ro11	.457		.694	
Ro1			.615	
Ro14				.839
Ro15				.786
Ro16				.673

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 6 iterations.

Table 7-10: Number of factors after rotation for Ro

7.4.2.2 Interpretation of the emerged operation risk clusters

0	P1 Weights	P2	P3	Alpha	New to the new cluster
RO5	0.615				NRo1 = staffing
RO6	0.952				
RO8	0.984				
RO13	0.954				
RO1		0.615			NRo2 = operation issues
RO2		0.911			
RO3		0.707			
RO4		0.984			
RO7		0.982			
RO16		0.673			
RO9			0.645		NRo3 = systems
RO10			0.713		
RO11			0.694		
RO12			0.755		
RO14			0.839		
RO15			0.786		
RO17					

Latent staffing:

These risks related directly to staffing at Operations &Maintenance stage. For example, insufficient human and financial resources, inadequate subject training, Poor communication in the team and lack of quality team will also lead to cost inefficiencies and ineffective operations and maintenance.

Latentoperation:

These risks related directly to the operations at this stage. For example, lack of, or poor policy performance for monitoring the system, poor implementation which leads to technical risks, priority conflicts not addressed, inadequate allocation of responsibilities, inadequate resource planning, and change in operation process and policy, per Kerzner, Strategic Planning for Project Management Using a Project Management Maturity Model (2001). This requires the planners to give due consideration to the quality of human resources being deployed for maintenance, as well as setting the internal controls adequately.

Latent systems:

These risks related directly to the system or product issues at this stage. For example, security assets not fit for purpose, un-scalability of the system, lack of interoperability, physical security assets not being compliant with regulatory standards and best practices, lack of stability, no support from the manufacturer, and physical security assets not extensible. Dealing only with reputable vendors and spending the required resources and time when making the acquisition and maintenance deals will mitigate these risks. Another way about this is the choice of operating leases instead of outright purchase, which puts the onus on the vendor for replacement according to the needs of the user.

7.4.2.2 Acquisition risks cluster

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.611	41.320	41.320	6.611	41.320	41.320	5.112	31.951	31.951
2	2.952	18.453	59.773	2.952	18.453	59.773	3.105	19.408	51.359
3	1.743	10.896	70.669	1.743	10.896	70.669	2.491	15.568	66.927
4	1.277	7.984	78.653	1.277	7.984	78.653	1.876	11.726	78.653
5	.968	6.047	84.700						
6	.686	4.288	88.988						
7	.492	3.075	92.072						
8	.465	2.903	94.976						
9	.301	1.881	96.857						
10	.151	.943	97.800						
11	.122	.764	98.564						
12	.081	.505	99.069						
13	.067	.418	99.487						
14	.041	.258	99.745						
15	.034	.213	99.958						
16	.007	.042	100.000						

Extraction Method: Principal Component Analysis.

Table 7-11: Factor Extraction for Ra

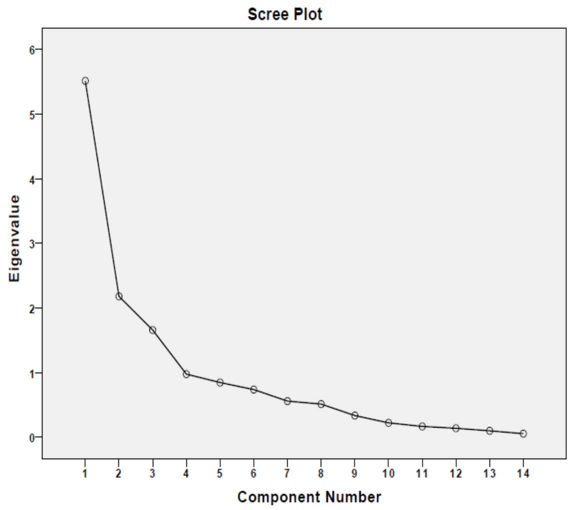


Figure 7-94: Scree Plot for Ra

Rotated Component Matrix[a]

	Component		
	1	2	3
RA7	.926		
RA4	.923		
RA5	.899		
RA6	.894		
RA3	.839		
RA11	.637		
RA13	.563		
RA8		.858	
RA12		.844	
RA14		.677	
RA10		.597	
RA2			.762
RA1			.722
RA9			.690

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

Table 7-11: Number of factors after rotation for Ro

7.4.2.2 Interpretation of the emerged acquisition risk clusters

0	P1 Weights	P2	P3	Alpha	New to the new cluster
RA1	0.722				NRA1 = financial issues
RA2	0.762				
RA9	0.690				
RA10	0.597				
RA3		0.839			NRA2 = change issues
RA4		0.923			
RA5		0.899			
RA6		0.894			
RA14			0.926		NRA3 = systems/product
RA10			0.858		
RA11			0.637		
RA12			0.844		
RA13			0.563		
RA14			0.677		

Latent financial issues:

These risks related to the financial issues at this stage. For example, lack of funds, running out of funds, inaccurate cost forecasts, and exchange rate variability not managed well(Roper & Payant, 2014). The costs budgeting should be a robust exercise and must provide for inflation and other changes due to technology and upgrading. More than a few quotes from vendors should be used, and the estimates must be based on credible and relatively recent transactions. Regarding the availability of funds, the right sources must be tapped, and allocation must be agreed upon well before the acquisitions of the PSA start. Good working capital management and overall robust deals with the banks can help an organization in mitigating these risks.

Latent change issues:

These risks related to the changing concept again but for this stage. For example, continually changing requirements, market development pace rendering products obsolete, changing priorities and, government rule changes. As such changes can render any acquisitions worthless, it must be covered for. The changes cannot be legislated for in many cases due to the nature of the phenomena as outside forces can also lead to such changes generally, but the usage and the solution for the issue being contemplated is the pivotal point of change that occurs later. Hence a fuller understanding of the potential change issues and concomitant solutions must be factored into the calculations.

<u>Latent systems/product:</u>

These risks related to the system issues again but for this stage. For example, hardware & software defects, integration issues, failure to integrate with existing systems, unavailability of the adequate test environment, failure to integrate components and security assets disrupting operations. Such risks can be mitigated through user experience and expertise due to acquisition, and also ensuring that significant acquisitions and the one over a pre-defined limit of expenditure are reviewed more than once prior to approval.

7.5 Summary

This chapter applied the factor analysis and data reduction process for the number of risk factors to handle the task more efficiently. Initially, there were 84 risk factors across all risk categories: initiation (Ri), implementation (Rm), acquisition (RA), operation and maintenance (Ro), and disposal (Rd) risks. However, SPSS had a principal component analysis used along with, to reduce the number of components in each category. Finally, a factor analysis score was implemented to reduce the risk factors to three components for each category, such as:

NRi1 =owner/ stakeholders (RIOS)

NRi2 = management (RIM)

NRi3 = contractor/project (RICP)

NRm1 = change and management (RMCM)

NRm2= staffing ND RESOURCES (RMSR)

NRm3= system/product issues (RMSPI)

NRA1 = financial issues (RAFI)

NRA2 = change issues (RACI)

NRA3 = systems/product (RASP)

NRo1 = staffing (ROST)

NRo2 = operation issues (ROO)

NRo3 = systems (ROSY)

CHAPTER 8. GOODNESS-OF-FIT TESTS

8.1 *Introduction*

This chapter examines whether the risk factor stated in the previous chapter and the data fit a specified probability distribution using the goodness-of-fit methodology. The method first creates a frequency table of the risk factors and then compares the observed frequencies with those that would be expected if the hypothesis was correct. To obtain the results regarding the risk factors, the following are used: a theoretical probability density function, a distribution function difference analysis, a probability-probability (P-P) plot, and goodness-of-fit tests. This statistical modeling analysis is performed using the software 'Easy-fit'.

The following sections present the results for the different risk factors.

8.1.1 Initiation Risk Factor (R1: Owner/Stakeholders RIOS)

The data sample was analyzedusing probabilistic modeling software (Easy fit).The Anderson-Darling goodness-of-fit tests showed that the Burr (4P) distribution was ranked first from a total number of 23 continuous distributions.

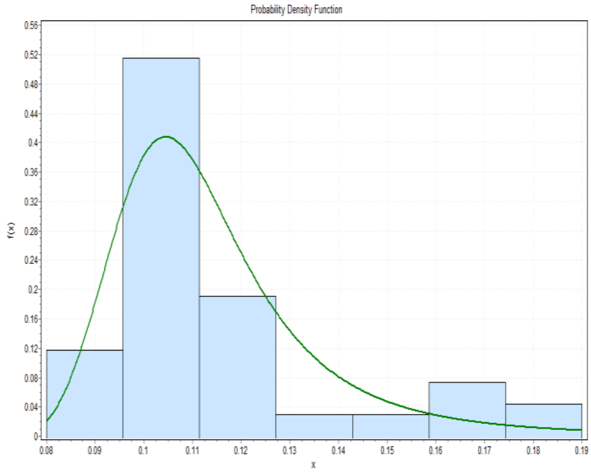


Figure 8-1: RIOS— theoretical probability density functions

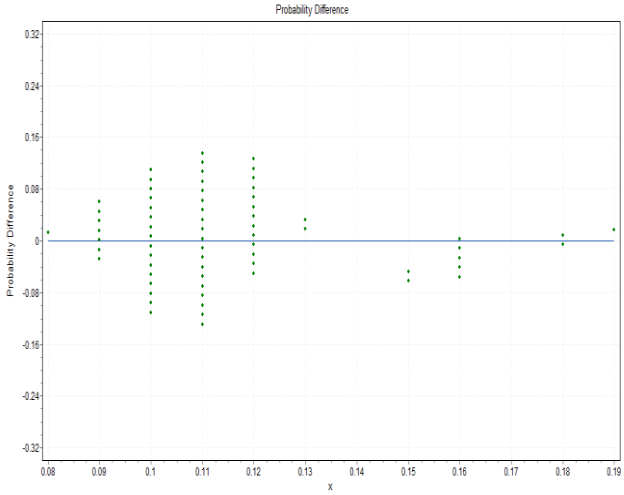


Figure 8-2: RIOS — Distribution-function-differences analysis

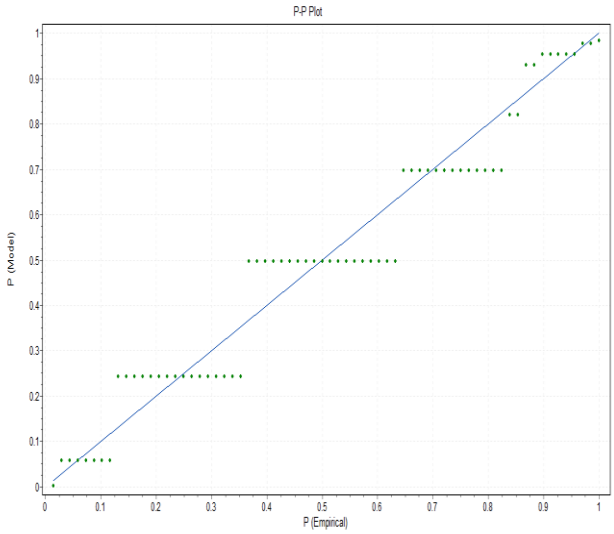


Figure 8-3: RIOS — Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Burr(4P)	0.1448	5	1.5239	1	9.5506	20

Anderson-Darling TEST WITH MODEL I					
Sample Size Statistic Rank	68 1.5239 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	Yes	No	No	No	No

Model	Mean	Variance	Skewness	Kurtosis
Burr(4P)	0.11612	6.8629E-4	3.7759	51.352

Table 8-1: Fit comparison for R1: owner/ stakeholders RIOS

This is verified using the statistic test value (1.52239), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.1, the Burr (4P) theoretical probability distribution is accepted at all alpha levels except for α=0.2. Hence, based on this evidence and these tests, there is no reason to believe that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.1.2 Initiation Risk Factor (R2: Management RIM)

The data sample was analysedusing probabilistic modelling software (Easy fit), and the Anderson-Darling goodness-of-fit tests showed that the Gen. Logistic distribution was ranked first from a total number of 23 continuous distributions.

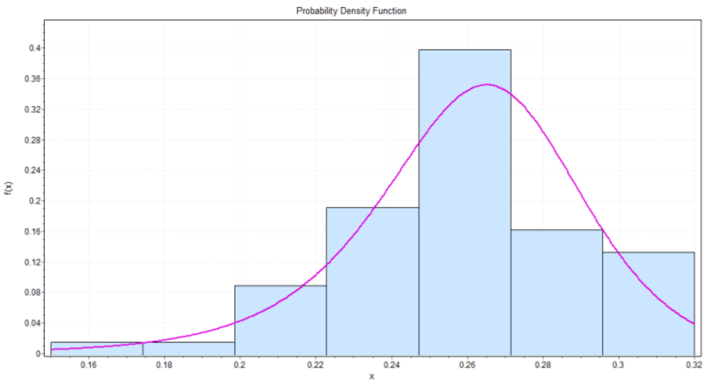


Figure 8-4: RIM— theoretical probability density functions

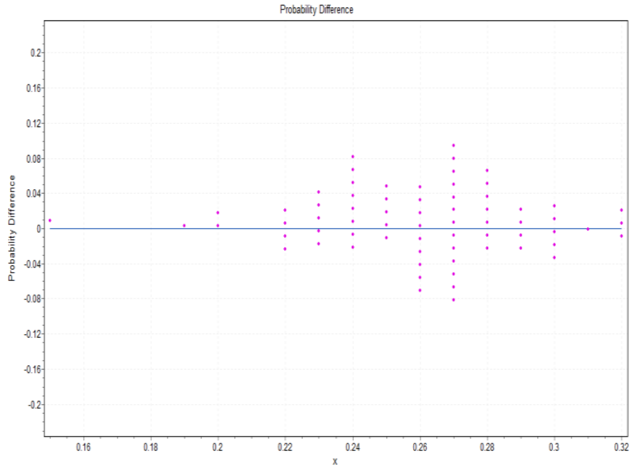


Figure 8-5: RIM — Distribution-function-differences analysis

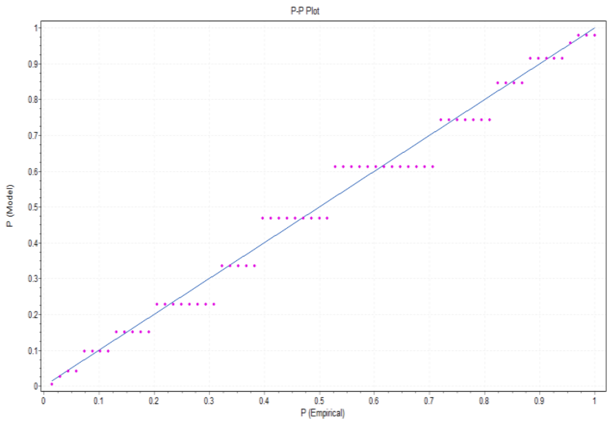


Figure 8-6: RIM — Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Gen. Logistic	0.09652	1	0.47718	1	6.1702	28

Anderson-Darling TEST WITH MODEL I				
Model	Mean	Variance	Skewness	Kurtosis
Gen. Logistic	N/A	N/A	N/A	N/A

ample Size Statistic Rank	68 0.47718 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Table 8-2: Fit comparison for R2: management RIM

The Gen. Logistic distribution is the first ranked distribution for this risk factor. This is verified using the statistic test value (0.47718), which is significantly lower than the critical values for level of significance. As demonstrated in table 7.2, the Gen. Logistic theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.1.3 Initiation Risk Factor (R3: Contractor/Project RICP)

The data sample was analyzed using probabilistic modeling software (Easy fit).The Anderson-Darling goodness-of-fit tests showed that the Johnson SB distribution was ranked first from a total number of 23 continuous distributions.

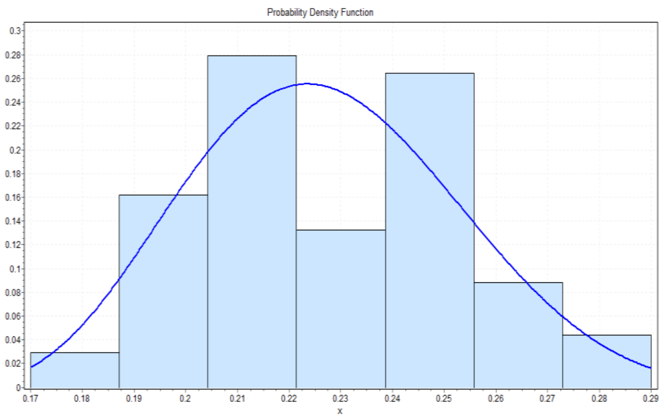


Figure 8-7: RICP— theoretical probability density functions

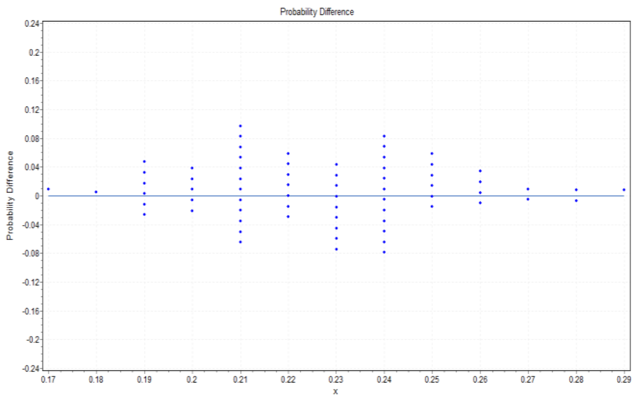


Figure 8-8: RICP — Distribution-function-differences analysis

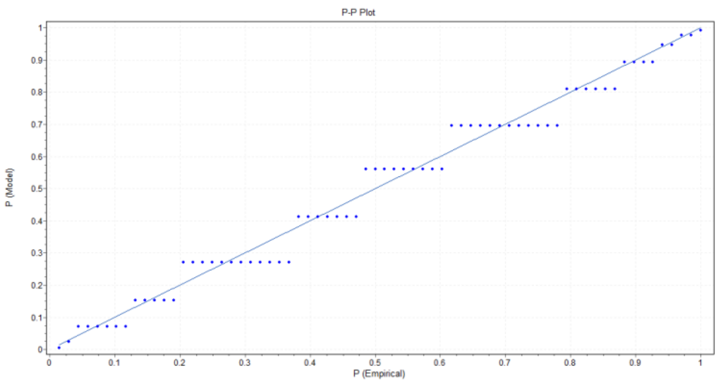


Figure 8-9: RICP— Probability-probability plot

	KolmogorovSmirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Johnson SB	0.09715	5	0.55396	1	8.9265	27
Anderson-Darling TEST WITH MODEL I						
Sample Size Statistic Rank	68 0.55396 1					
a	0.2	0.1	0.05	0.02	0.01	
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074	
Reject?	No	No	No	No	No	
Model	Mean	Variance	Skewness	Kurtosis		
Johnson SB	N/A	N/A	N/A	N/A		

Table 8-3: Fit comparison for R3: contractor/project RICP

The Johnson SB distribution is the first ranked distribution for this risk factor. This is verified using the statistic test value (0.55396), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.3, the Johnson SB theoretical probability distribution is accepted at all alpha levels. Hence, based on this evidence and these tests, there is no reason to believe that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.1.4 Operation and Maintenance Risk Factor (R1: Change and Management RMCM)

The data sample was analyzed using probabilistic modeling software (Easyfit).The Anderson-Darling goodness-of-fit tests showed that the value distribution was ranked first from a total number of 23 continuous distributions.

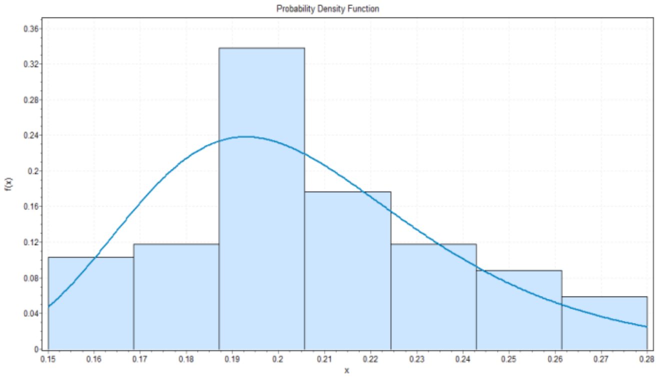


Figure 8-10: RMCN— theoretical probability density functions

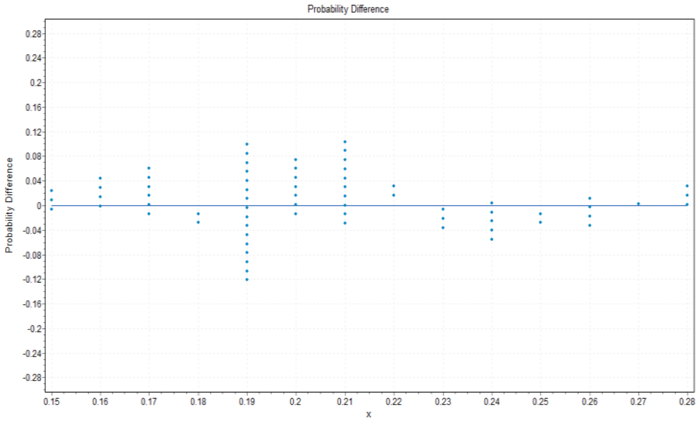


Figure 8-11: RMCM— Distribution-function-differences analysis

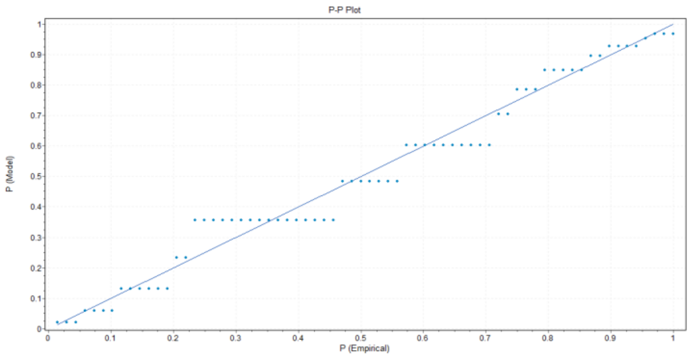


Figure 8-12: RMCM — Probability-probability plot

	KolmogorovSmirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Gen. Extreme Value	0.13609	17	0.78323	1	4.2758	19

Anderson-Darling TEST WITH MODEL I					
Sample Size Statistic Rank	68 0.78323 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	Mean	Variance	Skewness	Kurtosis
Gen. Extreme Value	0.20574	0.00117	0.79518	1.0222

Table 8-4: Fit comparison for R1: change and management RMCM

The Gen. Extreme Value distribution is the first ranked distribution for this risk factor. This is verified using the statistic test value (0.78323), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.4, the Gen. Extreme Value theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.1.5 Operation and Maintenance Risk Factor (R2: Staffing and Resources RMSR)

Using the probabilistic modeling software (Easyfit), the Anderson-Darling goodness-of-fit tests showed that the Burr distribution was ranked first from a total number of 23 continuous distributions.

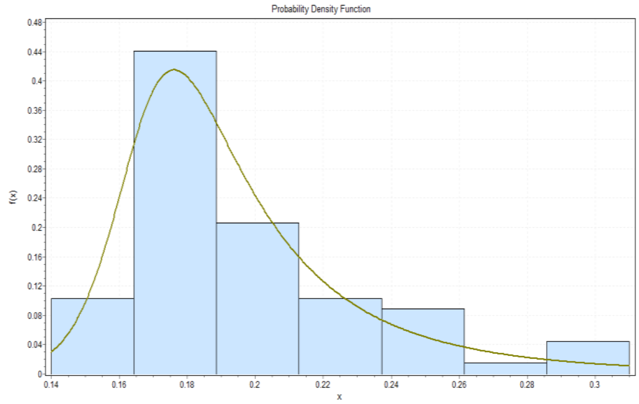


Figure 8-13: RMSR— Theoretical probability density functions

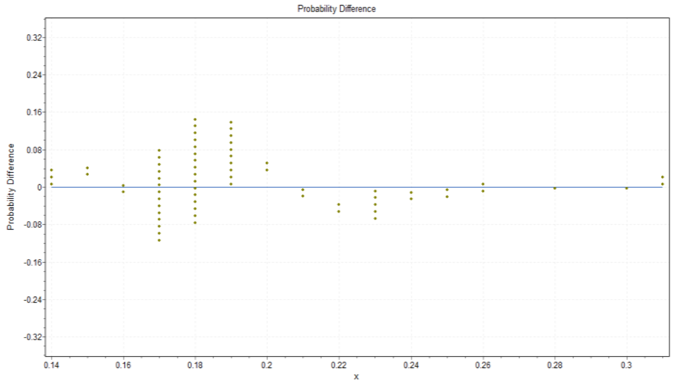


Figure 8-14: RMSR— Distribution-function-differences analysis

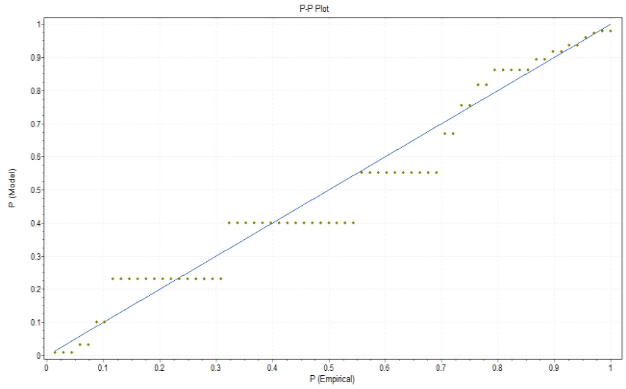


Figure 8-15: RMSR— Probability-probability plot

	KolmogorovSmirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Burr	0.14468	2	1.2785	1	18.083	22

Anderson-Darling TEST WITH MODEL I					
Sample Size Statistic Rank	68 1.2785 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	Mean	Variance	Skewness	Kurtosis
Burr	0.19609	0.00172	3.044	24.444

Table 8-5: Fit comparison for R1: change and management RMCM

The Burr distribution is the first ranked distribution for this risk factor. This is verified using the statistic test value (1.2785), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.5, the Burr theoretical probability distribution is accepted at all alpha levels. Hence, based on this evidence and these tests, there is no reason to believe that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.1.6 Operation and Maintenance Risk Factor (R3: System/Product Issues RMSPI)

The data sample was analyzed using probabilistic modeling software (Easyfit), and the Anderson-Darling goodness-of-fit tests showed that the **Burr** distribution was ranked first from a total number of 23 continuous distributions.

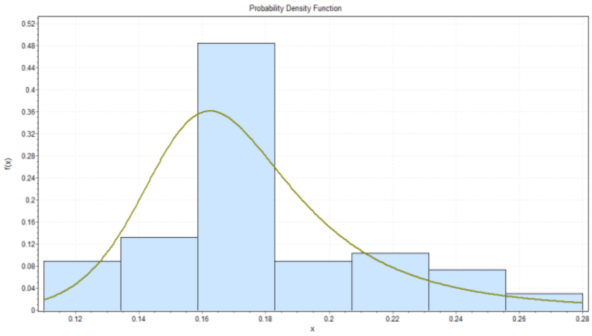


Figure 8-16: RMSPI— Theoretical probability density functions

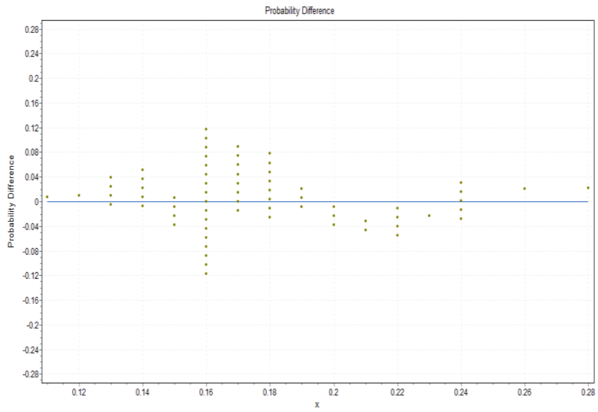


Figure 8-17: RMSPI— Distribution-function-differences analysis

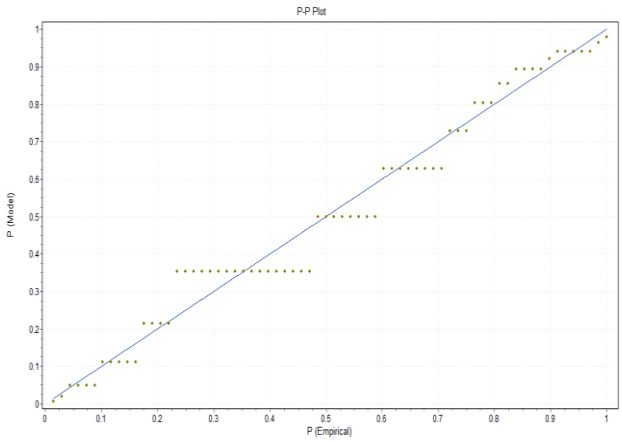


Figure 8-18: RMSPI— Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Burr	0.13235	6	0.80381	1	2.9279	5

Anderson-Darling TEST WITH MODEL I					
Sample Size Statistic Rank	68 0.80381 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	Mean	Variance	Skewness	Kurtosis
Burr	0.17702	0.00155	2.2715	15.031

Table 8-6: Fit comparison for R3: system/product issues RMSPI

The Burr distribution is the first ranked distribution for this risk factor. This is verified using the statistic test value (0.80381), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.6, the Burr theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.1.7 Acquisition Risk Factor (R1: Financial Issues RAFI)

Using probabilistic modeling software (Easyfit), the Anderson-Darling goodness-of-fit tests showed that the Burr (4P) distribution was ranked first from a total number of 23 continuous distributions.

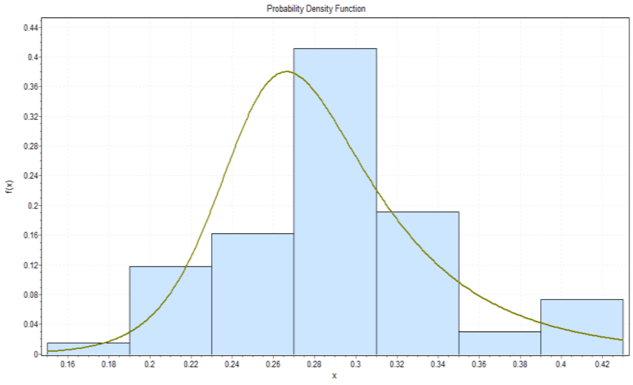


Figure 8-19: RAFI— Theoretical probability density function

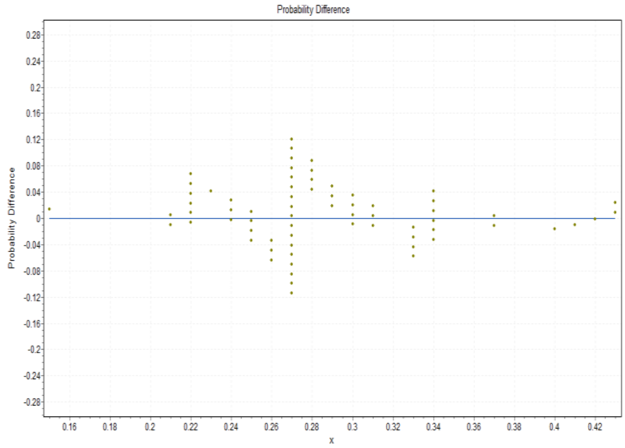


Figure 8-20: RAFI— Distribution-function-differences analysis

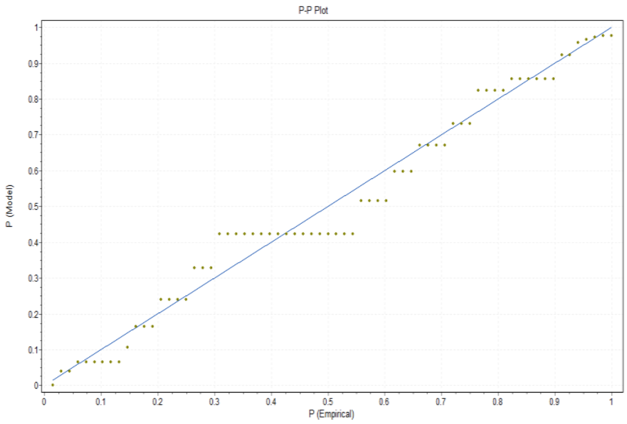


Figure 8-21: RAFI— Probability-probability plot

	Kolmogorov Smirnov Test		**Anderson-Darling**		**Equal-Probability Chi-Square Test**	
Model	**Statistic**	**Rank**	**Statistic**	**Rank**	**Statistic**	**Rank**
Burr (4P)	0.12909	6	0.78255	1	3.6454	2

Anderson-Darling TEST WITH MODEL I					
Sample Size Statistic Rank	68 0.78255 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No
Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**	
Burr (4P)	0.28751	0.00319	1.3654	4.4126	

Table 8-7: Fit comparison for R1: financial issues RAFI

The Burr distribution (4P) is the first ranked distribution for this risk factor. This is verified using the statistic test value (0.78255), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.7, the Burr (4P) theoretical probability distribution is accepted at all alpha levels. Hence, based on this evidence and these tests, there is no reason to believe that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.1.8 Acquisition Risk Factor (R2: Change Issues RACI)

Using probabilistic modeling software (Easyfit), the Anderson-Darling goodness-of-fit tests showed that the **Wakey** distribution was ranked first from a total number of 23 continuous distributions.

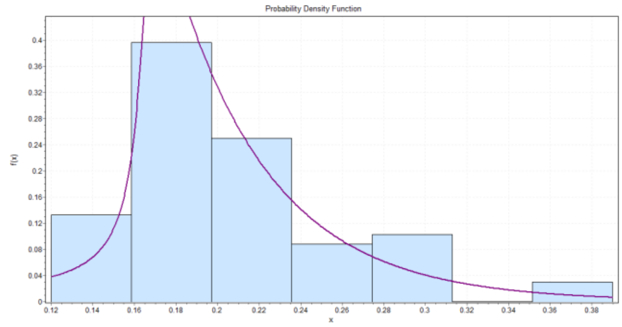


Figure 8-22: ARCI— Ttheoretical probability density function

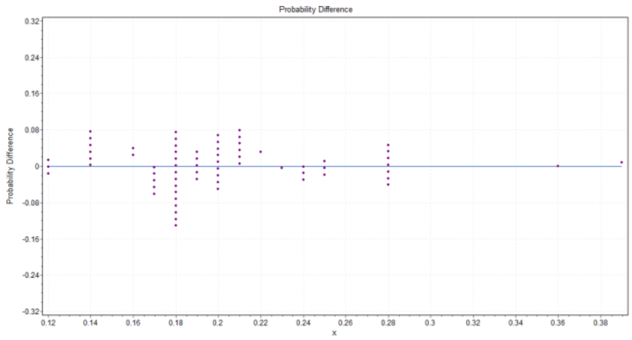


Figure 8-23: RAFI— Distribution-function-differences analysis

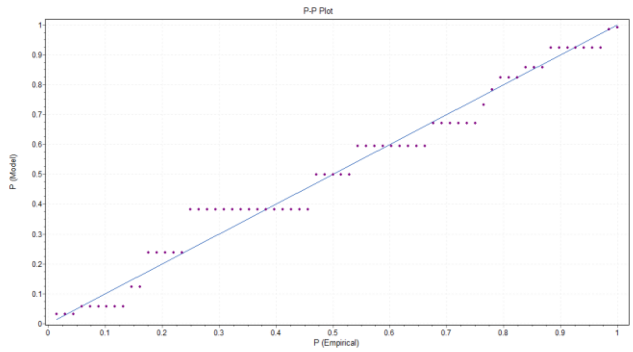


Figure 8-24: RAFI— Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Wakeby	0.14585	21	0.84148	1	13.384	29

Anderson-Darling TEST WITH MODEL I					
Sample Size Statistic Rank	68 0.84148 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	Mean	Variance	Skewness	Kurtosis
Wakeby	N/A	N/A	N/A	N/A

Table 8-8: Fit comparison for R2: change issues RACI

The Wakeby distribution is the first ranked distribution for this risk factor. This is verified using the statistic test value (0.84148), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.8, the Wakeby theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.1.9 Acquisition Risk Factor (R3 = Systems/Product RASP)

The data sample was analyzed using probabilistic modeling software (Easyfit), and the Anderson-Darling goodness-of-fit tests showed that the Burr distribution was ranked first from a total number of 23 continuous distributions.

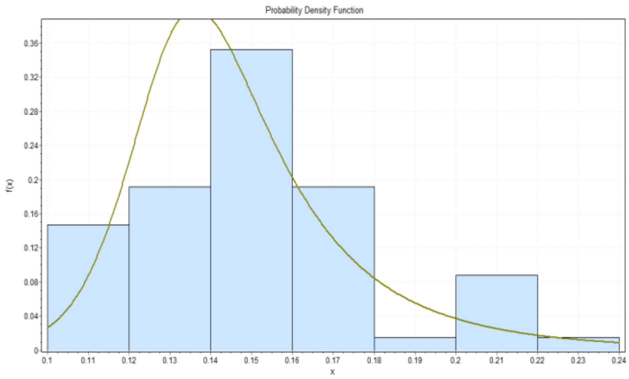


Figure 8-25: ARSP— Theoretical probability density function

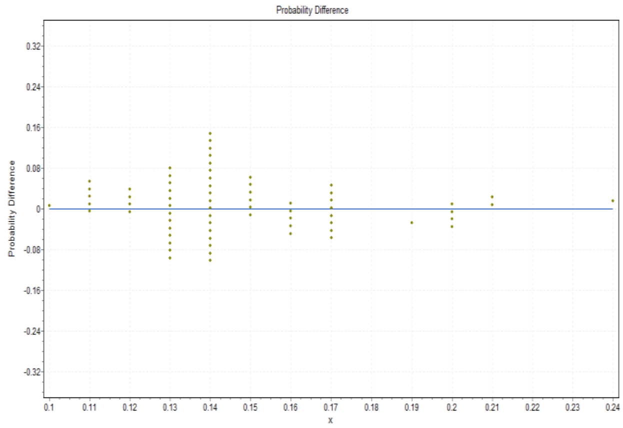


Figure 8-26: RASP— Distribution-function-differences analysis

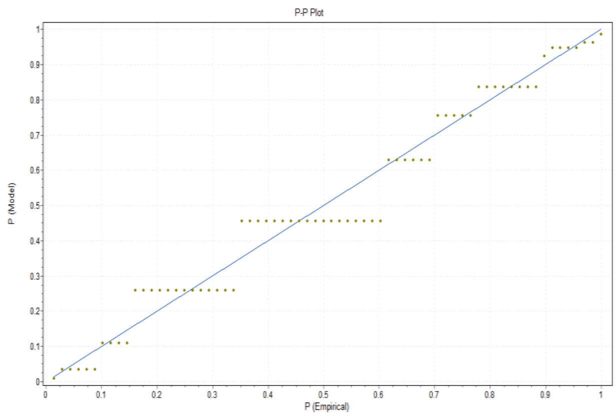


Figure 8-27: RASP— Probability-probability plot Probability-Probability Plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Burr	0.14813	3	0.98954	1	4.5336	18

Anderson-Darling TEST WITH MODEL I	
Sample Size Statistic Rank	68 0.98954 1

α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	Mean	Variance	Skewness	Kurtosis
Burr	0.14804	9.0247E-4	2.3283	14.878

Table 8-9: Fit comparison for R3 = systems/product RASP

The Burr distribution is the first ranked distribution for this risk factor. This is verified using the statistic test value (0.98954), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.9, the Burr theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this research.

8.1.10 Operation and Maintenance Risk Factor (R1: Staffing ROST)

The data sample was analyzed using probabilistic modeling software (Easyfit). The Anderson-Darling goodness-of-fit tests showed that the **Gen. Logistic** distribution was ranked first from a total number of 23 continuous distributions.

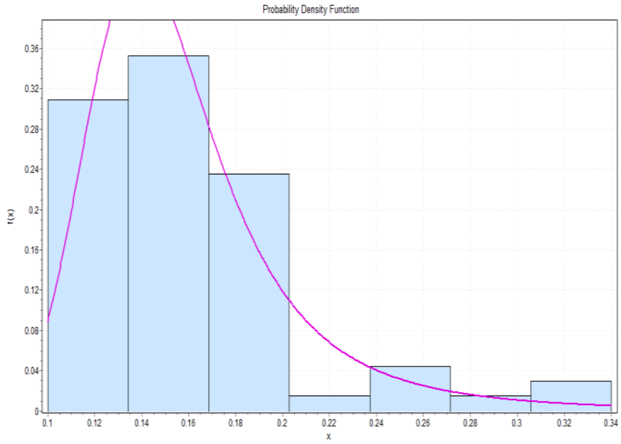


Figure 8-28: ROST— Theoretical probability density function

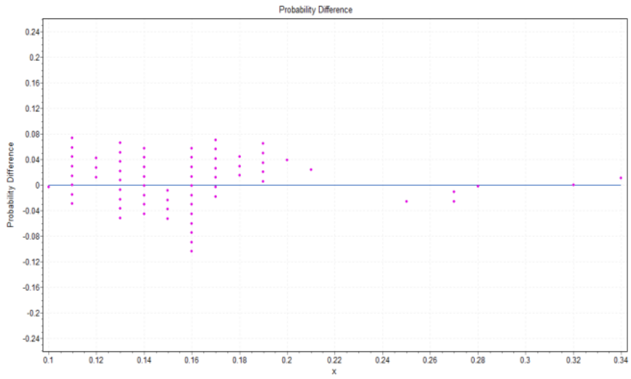


Figure 8-29: ROST— Distribution-function-differences analysis

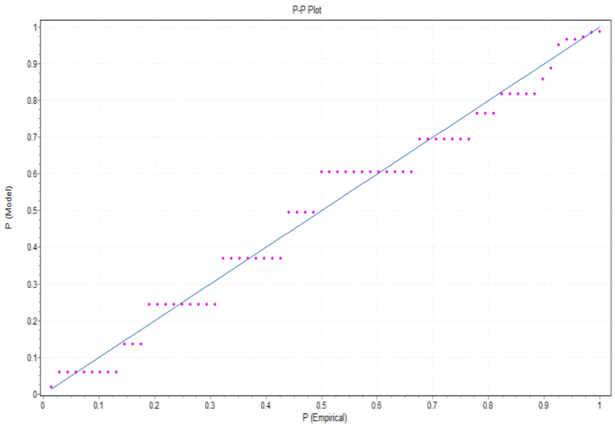


Figure 8-30: ROST— Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Gen. Logistic	0.11893	17	0.69163	1	2.0067	3

Anderson-Darling TEST WITH MODEL I					
Sample Size Statistic Rank	68 0.69163 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	Mean	Variance	Skewness	Kurtosis
Gen. Logistic	N/A	N/A	N/A	N/A

Table 8-10: Fit comparison for R1: staffing ROST

The Gen.Logistic distribution is the first ranked distribution for this risk factor. This is verified using the statistic test value (0.69163), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.10, the Gen.Logistic theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.1.11 Operation and Maintenance Risk Factor (R2: Operation Issues ROO)

The data sample was analyzed using probabilistic modeling software (Easyfit), and the Anderson-Darling goodness-of-fit tests showed that the secant distribution was ranked first from a total number of 23 continuous distributions.

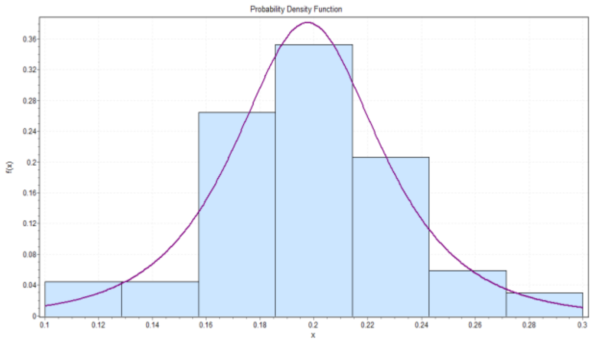


Figure 8-31: ROST— Theoretical probability density function

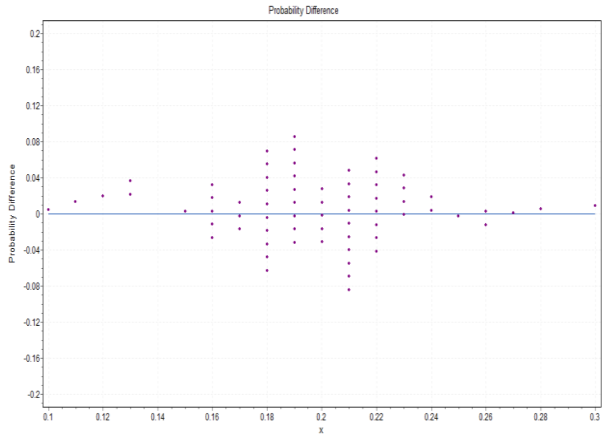


Figure 8-32: ROO— Distribution-function-differences analysis

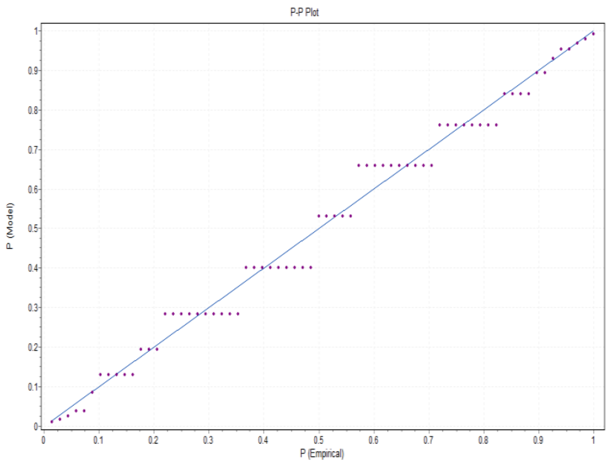


Figure 8-33: ROO— Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Hypersecant	0.09914	9	0.42606	1	4.6109	13

Anderson-Darling TEST WITH MODEL I					
Sample Size Statistic Rank	68 0.42606				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	Mean	Variance	Skewness	Kurtosis
Hypersecant	0.19765	0.0014	0	2

Table 8-11: Fit comparison for R2: operation issues ROO

The Hypersecant distribution is the first ranked distribution for this risk factor. This is verified using the statistic test value (0.42606), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.11, the hyper secant theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.1.12 Operation and Maintenance Risk Factor (R3: Systems ROSY)

The data sample was analyzed using probabilistic modeling software (Easyfit), and the Anderson-Darling goodness-of-fit tests showed that the **Wakeby** distribution was ranked first from a total number of 23 continuous distributions.

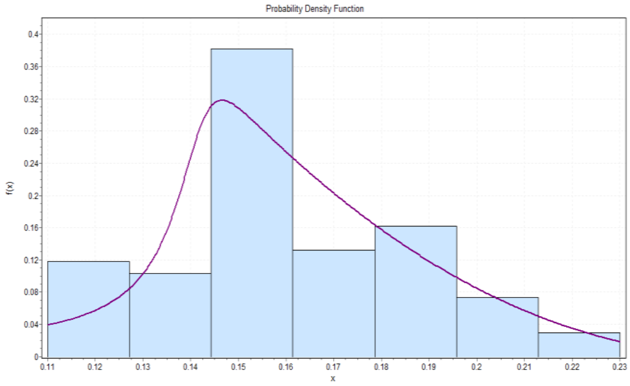


Figure 8-34: ROSY— Theoretical probability density function

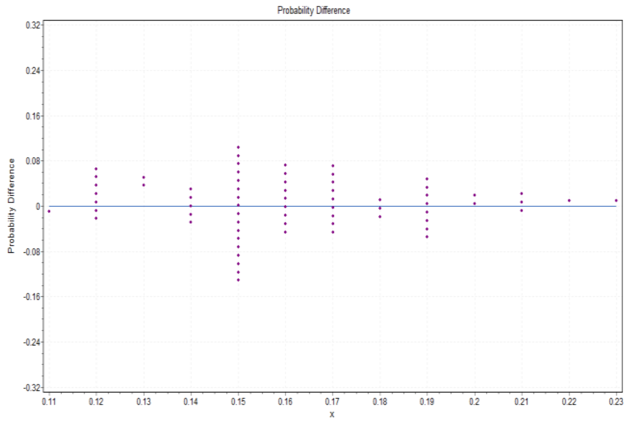


Figure 8-35: ROSY— Distribution-function-differences analysis

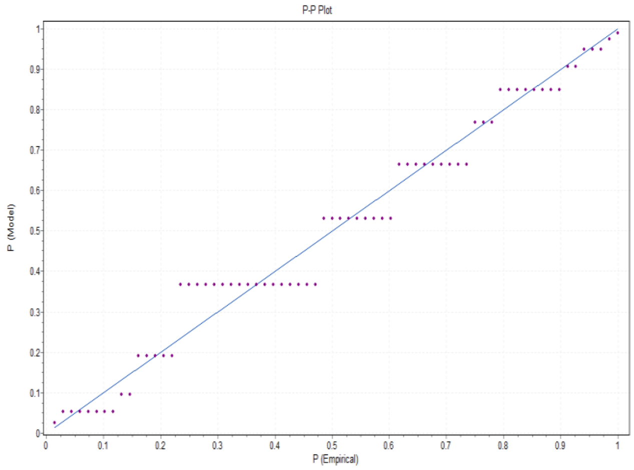


Figure 8-36: ROSY— Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Wakeby	0.14617	29	0.84081	1	9.547	41

Anderson-Darling TEST WITH MODEL I					
Sample Size Statistic Rank	68 0.55516 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No
Model	Mean	Variance		Skewness	Kurtosis
Wakeby	N/A	N/A		N/A	N/A

Table 8-12: Fit comparison for R3: systems ROSY

The Wake by distribution is the first ranked distribution for this risk factor. This is verified using the statistic test value (0.84081), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.12, the Wake by theoretical probability distribution is accepted at all alpha levels. Hence, based on this evidence and these tests, there is no reason to believe that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2 Goodness-of-fit Tests for Cost Factors

This section examines whether the cost factors data fits a specified probability distribution using the goodness-of-fit methodology. In this method, a frequency table of the cost factors is first created, and then the observed frequencies are compared with those that would be expected if the hypothesis was correct. To obtain the cost factor results, the following were used: a theoretical probability density function, a distribution function difference analysis, a probability-probability plot, and goodness-of-fit tests. This statistical modeling analysis is performed using the software 'Easy-fit'. The following sections present the results for the different capital cost factors.

8.2.1 Camera Cost Factor

The data sample was analyzed using probabilistic modeling software (Easy fit). The Anderson-Darling goodness-of-fit tests showed that the **Gen. Logistic** distribution was ranked first from a total number of 23 continuous distributions.

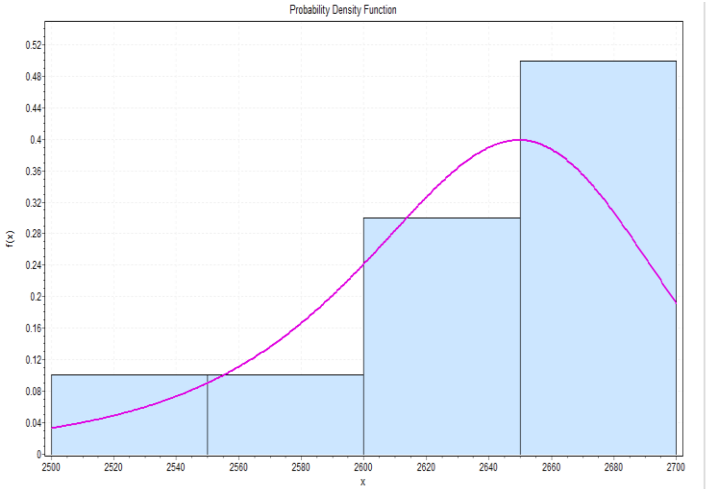


Figure 8-37: Camera Cost — Theoretical probability density function

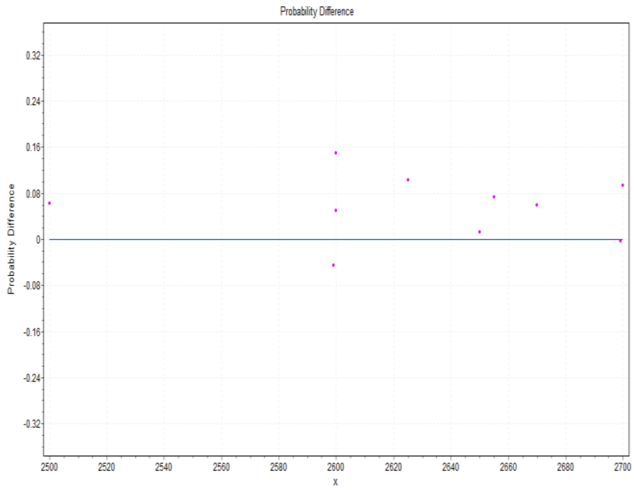


Figure 8-38: Camera Cost — Distribution-function-differences analysis

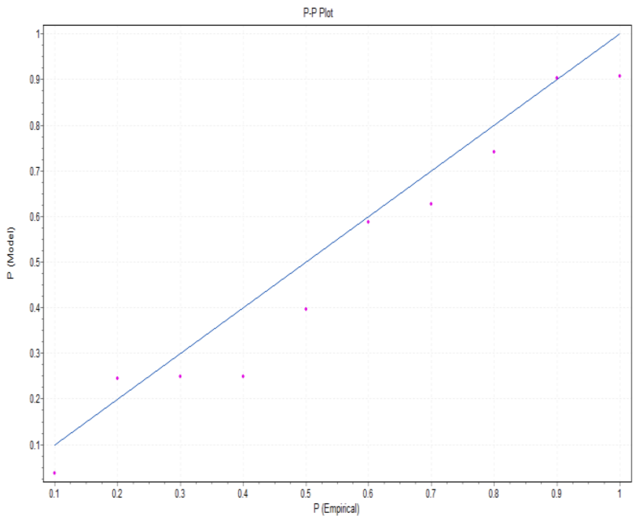


Figure 8-39: Camera Cost — Probability-probability plot

	Kolmogorov Smirnov Test		**Anderson-Darling**		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Gen. Logistic	0.15038	2	0.25856	1	0.03105	10

Anderson-Darling **TEST WITH MODEL I**					
Sample Size Statistic Rank	10 0.25856 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**
Gen. Logistic	N/A	N/A	N/A	N/A

Table 8-13: Fit comparison for camera cost

The Gen. Logistic distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.25856), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.13, the Gen. Logistic theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.2 Switches Cost Factor

Using probabilistic modeling software (Easy fit), the Anderson-Darling goodness-of-fit tests showed that the **Johnson SB** distribution was ranked first from a total number of 23 continuous distributions.

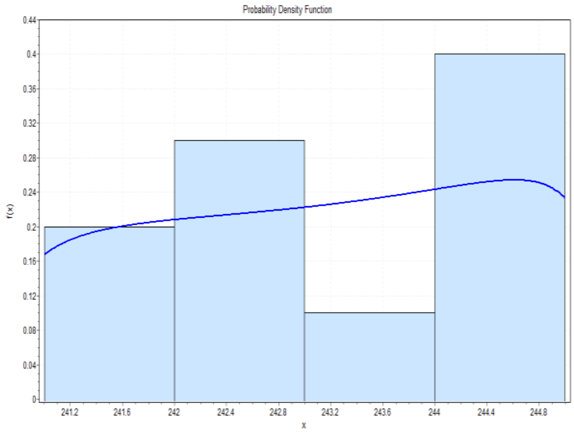


Figure 8-40: Switches cost — Theoretical probability density function

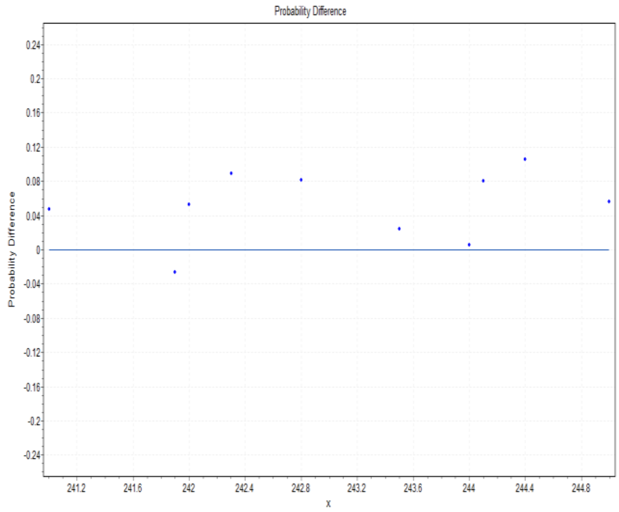


Figure 8-41: Switches cost — Distribution-function-differences analysis

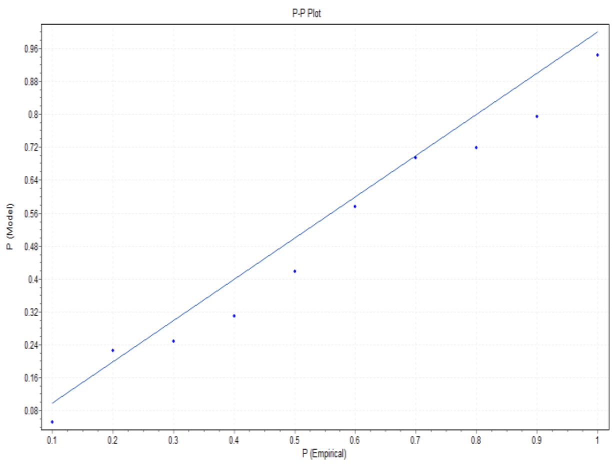


Figure 8-42: Switches cost — Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Johnson SB	0.12692	1	0.16306	1	9.16E-05	7

Anderson-Darling **TEST WITH MODEL I**					
Sample Size Statistic Rank	10 0.16306 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No
Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**	
Johnson SB	N/A	N/A	N/A	N/A	

Table 8-14: Fit comparison of switches cost

The Johnson SB distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.25856), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.13, the Gen. Logistic theoretical probability distribution is accepted at all alpha levels. Hence, based on this evidence and these tests, there is no reason to believe that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.3 Servers Cost Factor

The data sample was analyzed using probabilistic modeling software (Easy fit), and the Anderson-Darling goodness-of-fit tests showed that the **Johnson SB** distribution was ranked first from a total number of 23 continuous distributions.

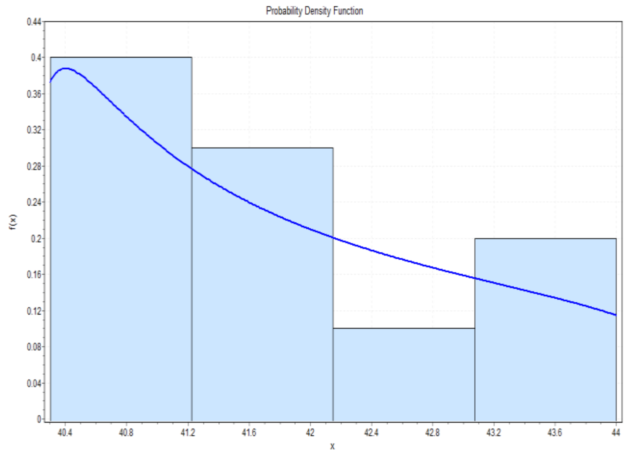


Figure 8-43: Servers cost — Theoretical probability density function

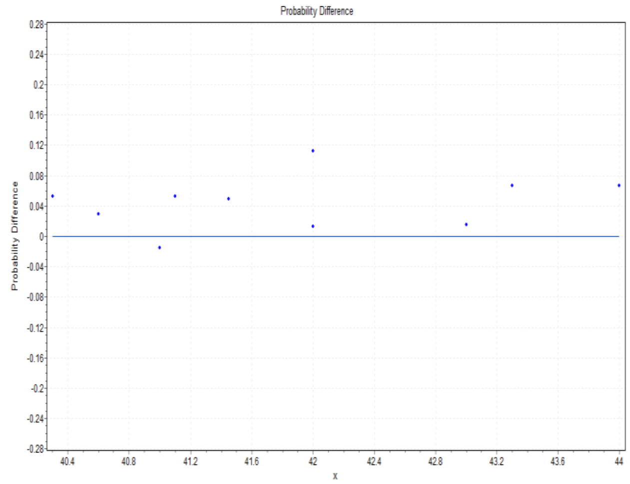


Figure 8-44: Servers cost — Distribution-function-differences analysis

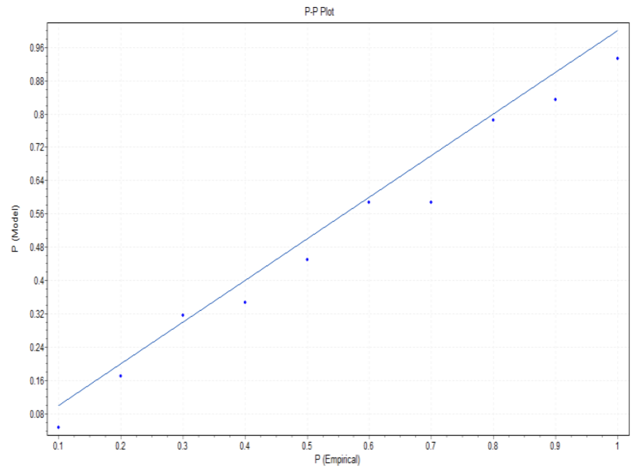


Figure 8-45: Servers cost — Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Johnson SB	0.11526	1	0.13638	1	0.00408	10

Anderson-Darling **TEST WITH MODEL I**					
Sample Size Statistic Rank	10 0.13638 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**
Johnson SB	N/A	N/A	N/A	N/A

Table 8-15: Fit comparison for servers cost

The Johnson SB distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.13636), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.15, the Johnson SB theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.4 Software Cost Factor

Using probabilistic modeling software (Easy fit), the Anderson-Darling goodness-of-fit tests showed that the **Johnson SB** distribution was ranked first from a total number of 23 continuous distributions.

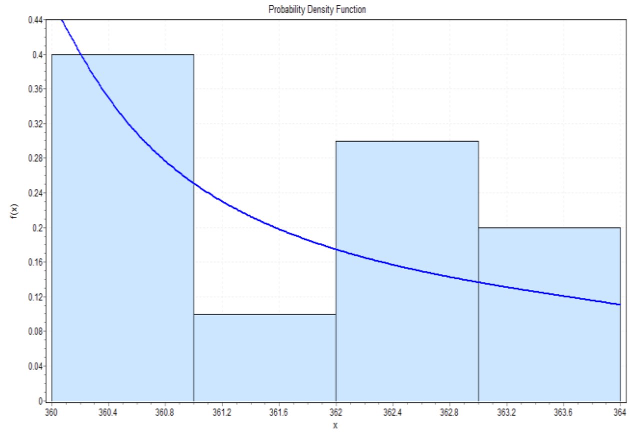


Figure 8-46: Software cost — Theoretical probability density function

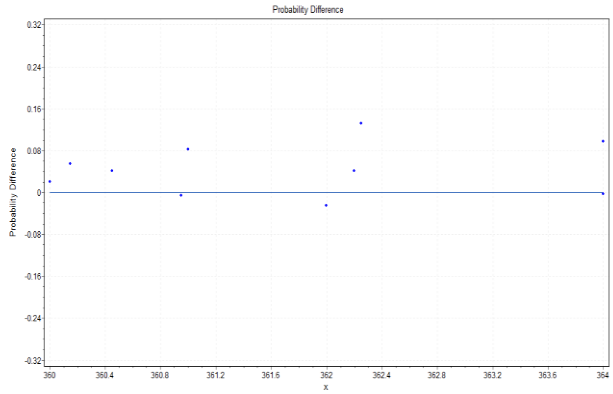


Figure 8-47: Software cost — Distribution-function-differences analysis

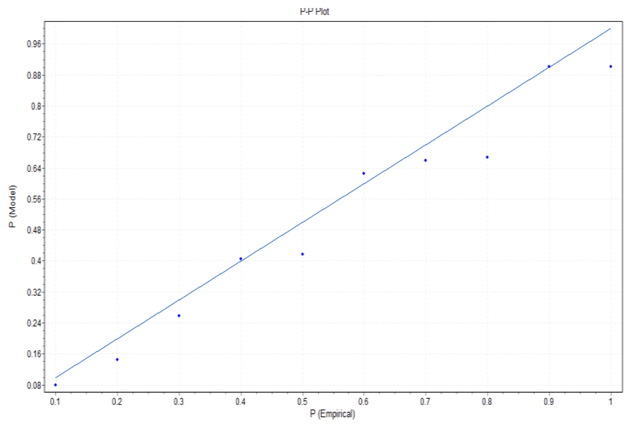


Figure 8-48: Software cost — Probability-probability plot

	Kolmogorov Smirnov Test		**Anderson-Darling**		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Johnson SB	0.13266	3	0.22226	1	0.00326	7

Anderson-Darling **TEST WITH MODEL I**					
Sample Size Statistic Rank	10 0.22226 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**
Johnson SB	N/A	N/A	N/A	N/A

Table 8-16: Fit comparison for software cost

The Johnson SB distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.22226), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.16, the Johnson SB theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.5 Monitors Cost Factor

The data sample was analyzed using probabilistic modeling software (Easy fit). The Anderson-Darling goodness-of-fit tests showed that the **Johnson SB** distribution was ranked first from a total number of 23 continuous distributions.

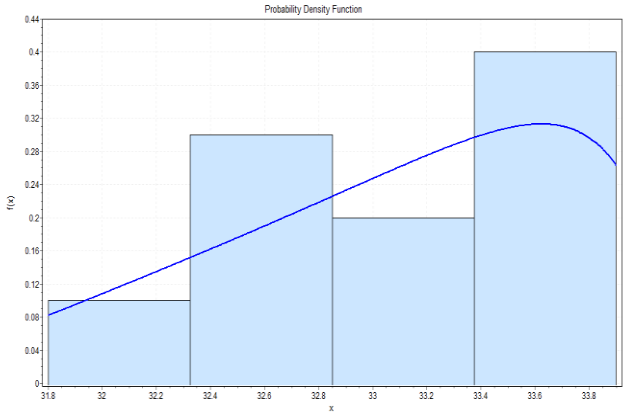


Figure 8-49: Monitors cost — Theoretical probability density function

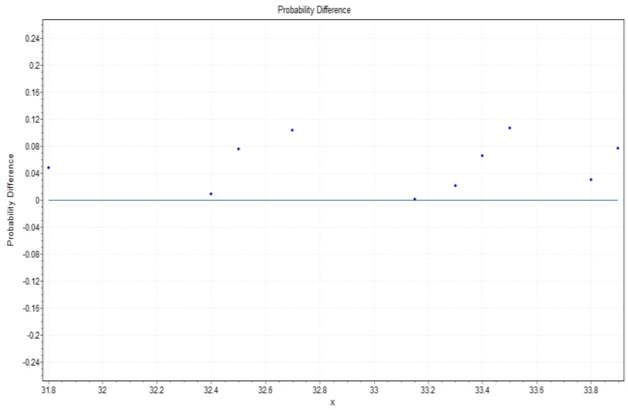


Figure 8-50: Monitors cost — Distribution-function-differences analysis

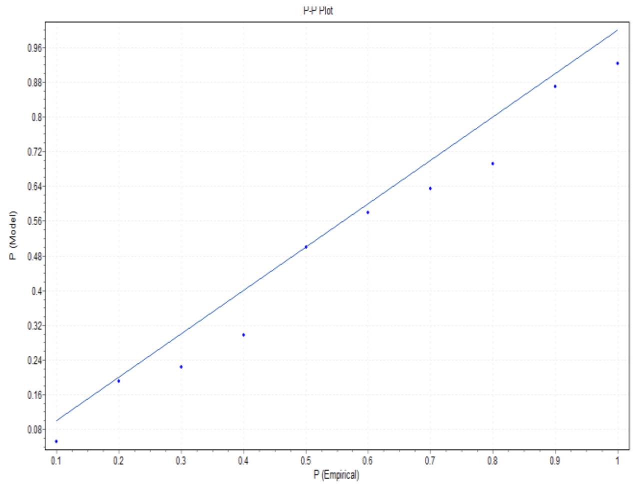


Figure 8-51: Monitors cost — Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Johnson SB	0.10733	1	0.15058	1	N/A	N/A

Anderson-Darling **TEST WITH MODEL I**					
Sample Size Statistic Rank	10 0.15058 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**
Johnson SB	N/A	N/A	N/A	N/A

Table 8-17: Fit comparison of monitors cost

The Johnson SB distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.15058), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.17, the Johnson SB theoretical probability distribution is accepted at all alpha levels. Hence, based on this evidence and these tests, there is no reason to believe that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.6 Storage Cost Factor

The data sample was analyzed using probabilistic modeling software (Easy fit), and the Anderson-Darling goodness-of-fit tests showed that the **Johnson SB** distribution was ranked first from a total number of 23 continuous distributions.

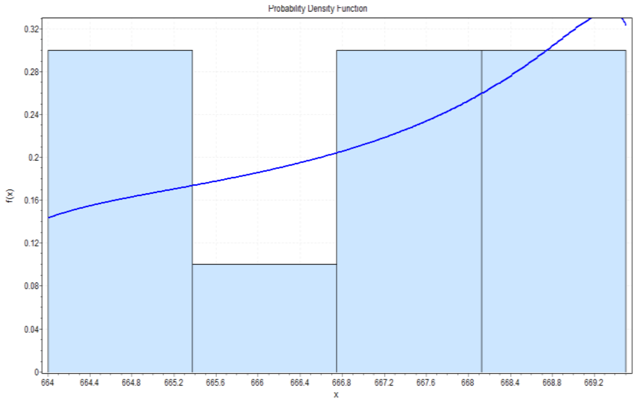


Figure 8-52: Storage cost — Theoretical probability density function

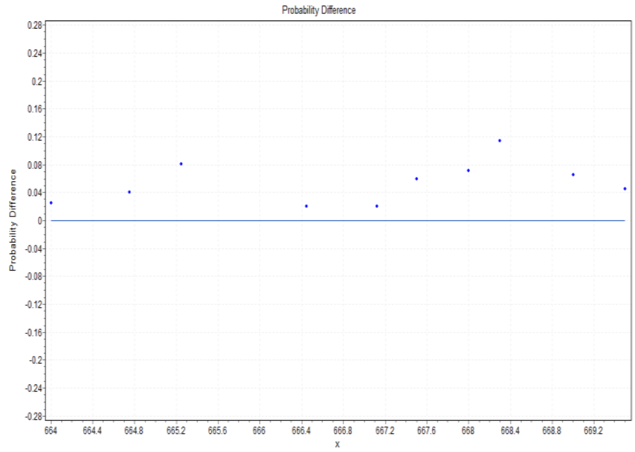


Figure 8-53: Storage cost — Distribution-function-differences analysis

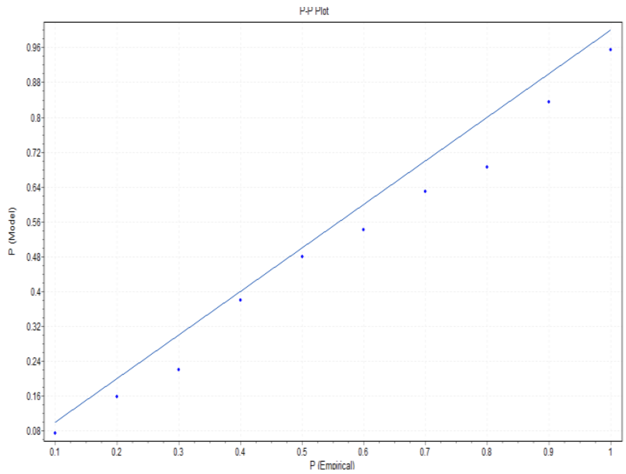


Figure 8-54: Storage cost — Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Johnson SB	0.11454	2	0.12467	1	0.0091	8

Anderson-Darling **TEST WITH MODEL I**					
Sample Size Statistic Rank	10 0.12467 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**
Johnson SB	664.51	143.57	-2.0254	6.1709

Table 8-18: Fit comparison for storage cost

The Johnson SB distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.12467), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.18, the Johnson SB theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.7 UPS Cost Factor

The data sample was analyzed using probabilistic modeling software (Easy fit), and the Anderson-Darling goodness-of-fit tests showed that the **Error** distribution was ranked first from a total number of 23 continuous distributions.

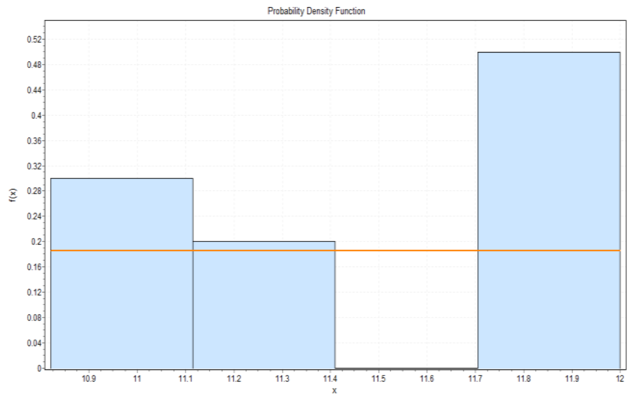


Figure 8-55: UPS cost — Theoretical probability density function

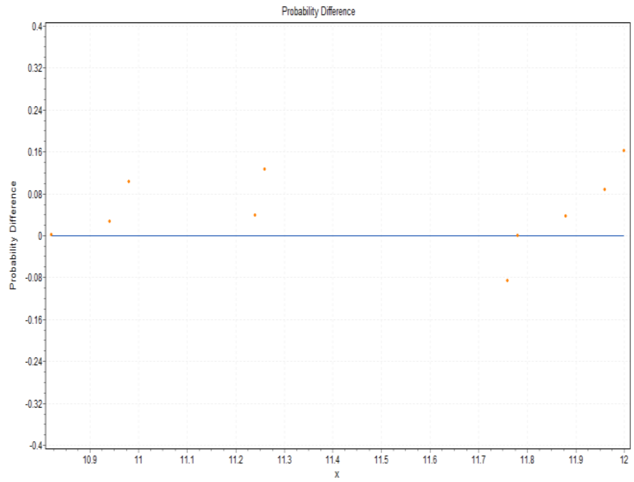


Figure 8-56: UPS Cost — Distribution-function-differences analysis

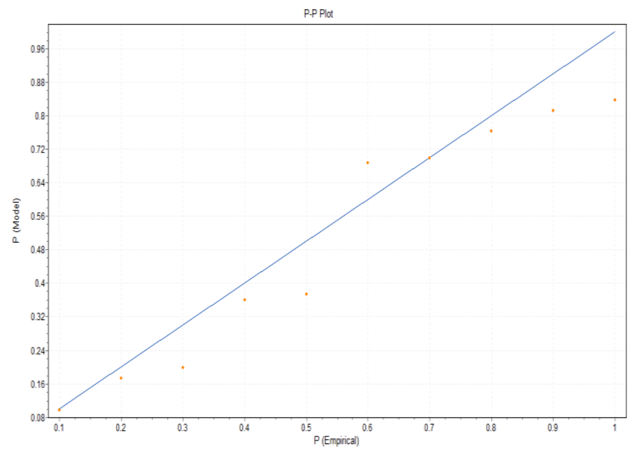


Figure 8-57: UPS Converter cost — Probability-probability plot

	Kolmogorov Smirnov Test		**Anderson-Darling**		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Error	0.18682	6	0.37802	1	0.04269	33

Anderson-Darling **TEST WITH MODEL I**					
Sample Size Statistic Rank	10 0.37802 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**
Error	11.462	0.21213	0	-1.1989

Table 8-19: Fit comparison for UPS converter cost

The Error distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.37802), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.19, the Error theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.8 Control Room Cost Factor

Using probabilistic modeling software (Easy fit), the Anderson-Darling goodness-of-fit tests showed that the **Gen. Logistic** distribution was ranked first from a total number of 23 continuous distributions.

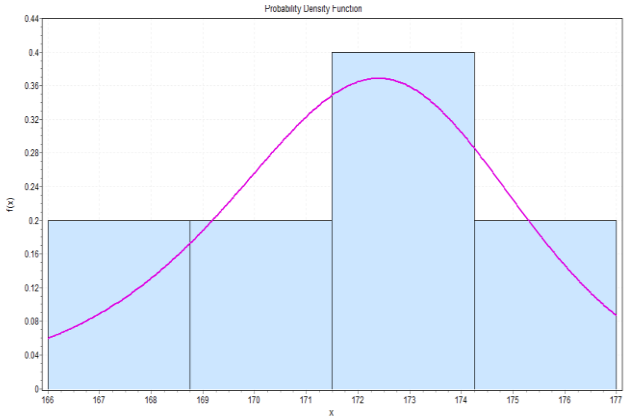


Figure 8-58: Control room cost — Theoretical probability density function

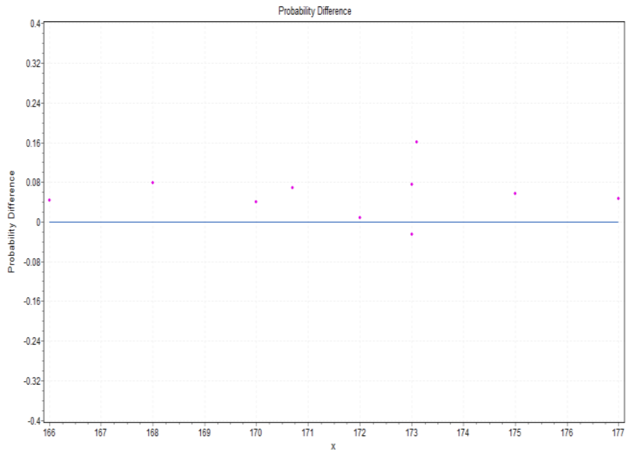


Figure 8-59: Control room cost— Distribution-function-differences analysis

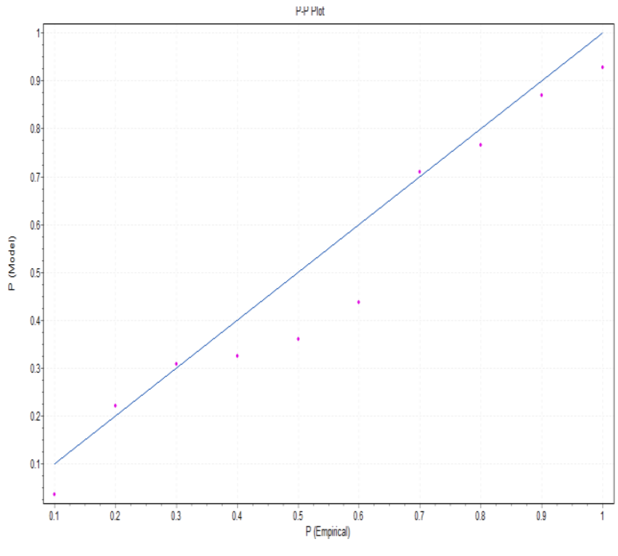


Figure 8-60: Control Room Cost — Probability-probability plot

	Kolmogorov Smirnov Test		**Anderson-Darling**		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Gen. Logistic	0.16164	20	0.17724	1	6.36E-04	2
Anderson-Darling **TEST WITH MODEL I**						
Sample Size Statistic Rank	10 0.17724 1					
α	0.2	0.1	0.05	0.02	0.01	
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074	
Reject?	No	No	No	No	No	
Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**		
Gen. Logistic	N/A	N/A	N/A	N/A		

Table 8-20: Fit comparison of control room cost

The Gen. Logistic distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.17724), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.20, the Gen.Logistic theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.9 Transmission Cost Factor

The data sample was analyzed using probabilistic modeling software (Easy fit). The Anderson-Darling goodness-of-fit tests showed that the **Gen. Logistic** distribution was ranked first from a total number of 23 continuous distributions.

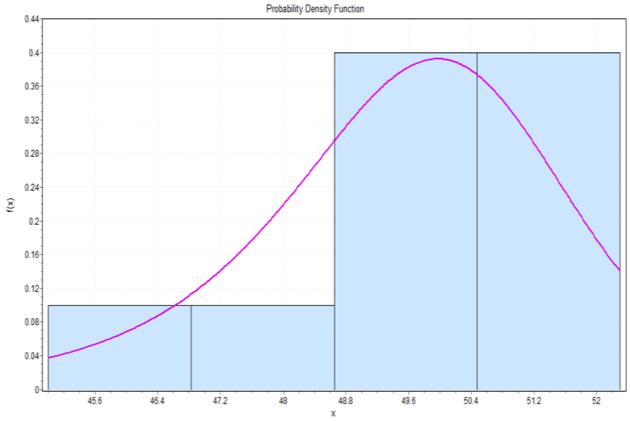


Figure 8-61: Transmission cost — Theoretical probability density function

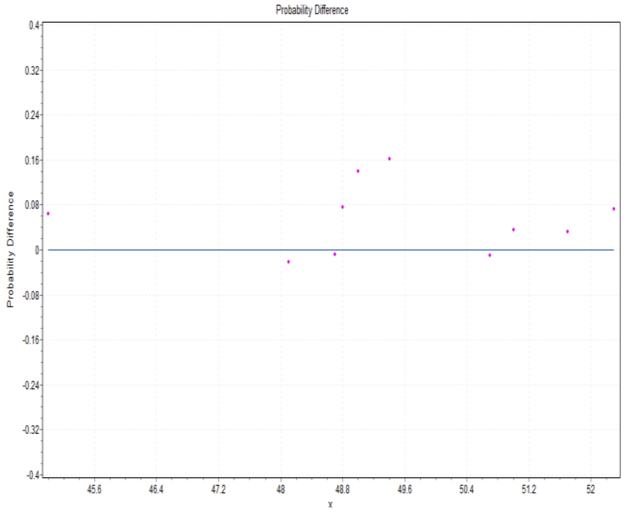


Figure 8-62: Transmission cost — Distribution-function-differences analysis

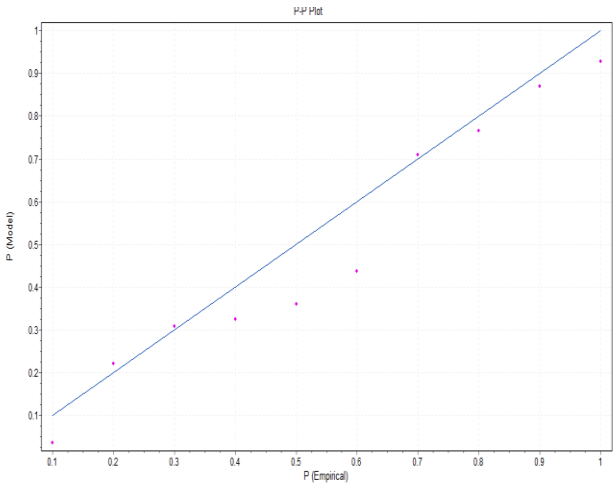


Figure 8-63: Transmission cost — Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Gen. Logistic	0.16211	20	0.24638	1	N/A	N/A

Anderson-Darling **TEST WITH MODEL I**					
Sample Size Statistic Rank	10 0.24638 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**
Gen. Logistic	N/A	N/A	N/A	N/A

Table 8-21: Fit comparison of control room cost

The Gen. Logistic distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.24638), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.21, the Gen.Logistic theoretical probability distribution is accepted at all alpha levels. Hence, based on this evidence and these tests, there is no reason to believe that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.10 Layout Cost Factor

The data sample was analyzed using probabilistic modeling software (Easy fit), and the Anderson-Darling goodness-of-fit tests showed that the **Gen. Extreme Value** distribution was ranked first from a total number of 23 continuous distributions.

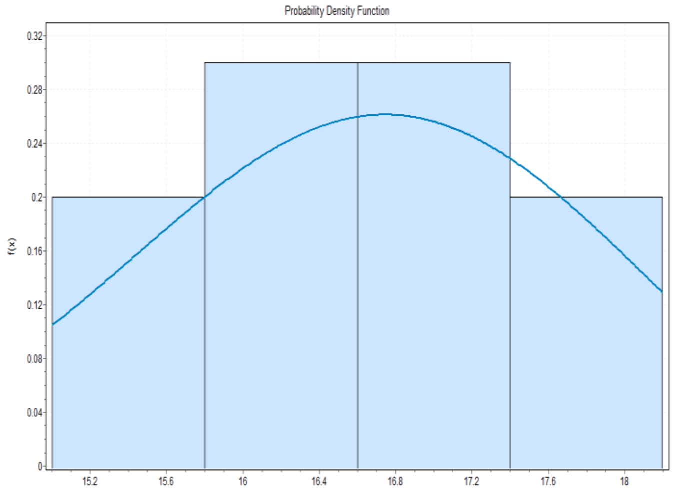


Figure 8-64: Layout cost — Theoretical probability density function

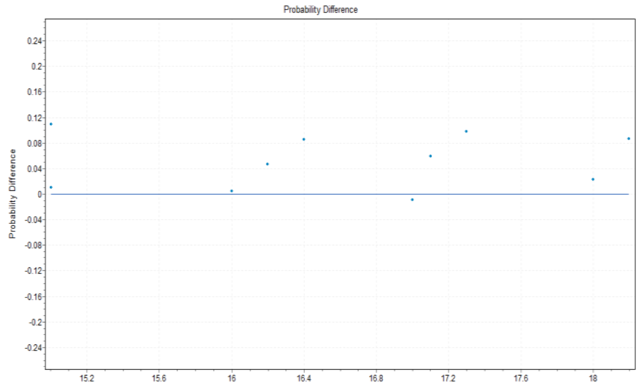


Figure 8-65: Layout cost — Distribution-function-differences analysis

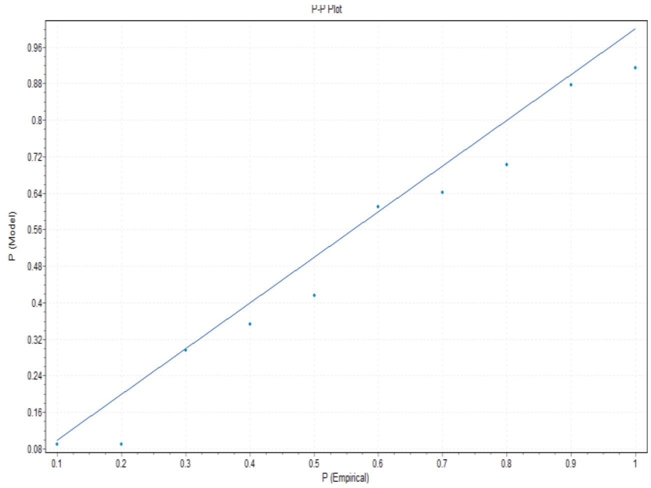


Figure 8-66: Layout cost — Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Gen. Extreme Value	0.10973	1	0.20475	1	1.20E-04	7

Anderson-Darling **TEST WITH MODEL I**					
Sample Size Statistic Rank	10 0.20475 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	**Mean**	**Variance**	**Skewness**	**Kurtosis**
Gen. Extreme Value	16.62	1.3632	-0.23819	-0.23756

Table 8-22: Fit comparison for layout cost

The Gen. Extreme Value distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.20475), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.21, the Gen. Extreme Value theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.11 Man Power Cost Factor

The data sample was analyzed using probabilistic modeling software (Easy fit), and the Anderson-Darling goodness-of-fit tests showed that the **Gen.Logistic** distribution was ranked first from a total number of 23 continuous distributions.

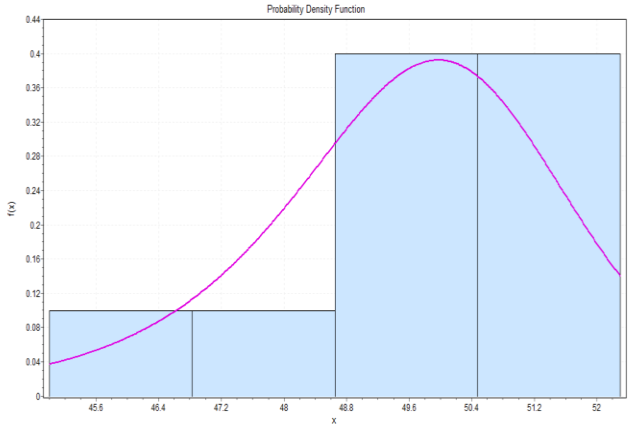


Figure 8-67: Manpower cost — Theoretical probability density function

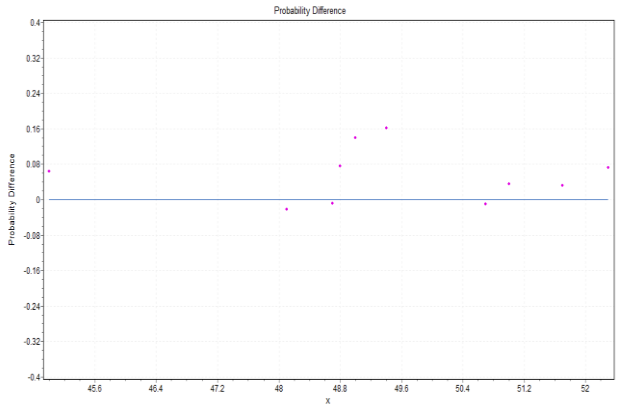


Figure 8-68: Manpower cost — Distribution-function-differences analysis

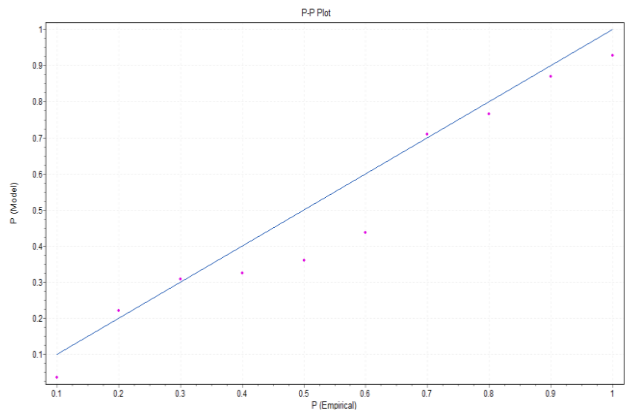


Figure 8-69: Manpower cost — Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Gen. Logistic	0.16211	20	0.24638	1	N/A	N/A

Anderson-Darling TEST WITH MODEL I					
Sample Size Statistic Rank	10 0.24638 1				
α	0.2	0.1	0.05	.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No

Model	Mean	Variance	Skewness	Kurtosis
Gen. Logistic	N/A	N/A	N/A	N/A

Table 8-23: Fit comparison for manpower cost

The Gen. Logistic distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.20475), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.23, the Gen.Logistic theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

8.2.12 Power Supply Cost Factor

The data sample was analyzed using probabilistic modeling software (Easyfit). The Anderson-Darling goodness-of-fit tests showed that the **Johnson SB** distribution was ranked first from a total number of 23 continuous distributions.

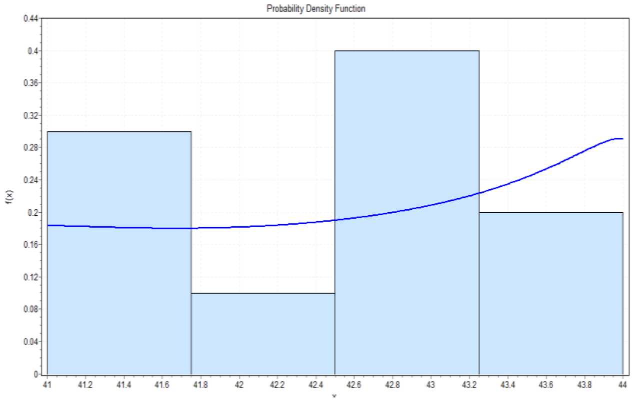


Figure 8-70: Power supply cost — Theoretical probability density function

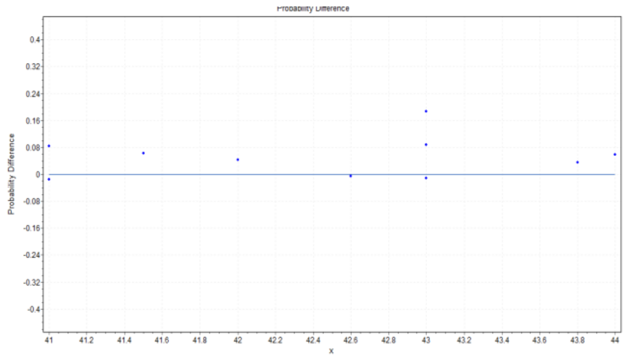


Figure 8-71: Power supply cost — Distribution-function-differences analysis

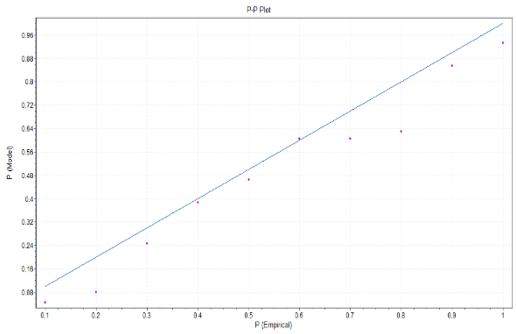


Figure 8-72: Power supply cost — Probability-probability plot

	Kolmogorov Smirnov Test		Anderson-Darling		Equal-Probability Chi-Square Test	
Model	Statistic	Rank	Statistic	Rank	Statistic	Rank
Johnson SB	0.18743	17	0.26349	1	0.03378	7

Anderson-Darling **TEST WITH MODEL I**					
Sample Size Statistic Rank	10 0.26349 1				
α	0.2	0.1	0.05	0.02	0.01
Critical Value	1.3749	1.9286	2.5018	3.2892	3.9074
Reject?	No	No	No	No	No
Model	**Mean**	**Variance**		**Skewness**	**Kurtosis**
Johnson SB	N/A	N/A		N/A	N/A

Table 8-24: Fit comparison of power supply cost

The Johnson SB distribution is the first ranked distribution for this cost factor. This is verified using the statistic test value (0.26349), which is significantly lower than the critical values for the level of significance. As demonstrated in table 7.24, the Johnson SB theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and these tests, that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study.

Summary:

1. Risk Factors	**Model**	**A-D Test (Statistic)**	**Accepted at all Alpha Levels?**
Initiation Risk Factor (R1: Owner / Stakeholders RIOS)	Johnson SB	0.03378	Yes, except one α=0.2
Initiation Risk Factor (R2: Management RIM)	Gen. Logistic	0.47718	Yes
Initiation Risk Factor (R3: Contractor/Project RICP)	Johnson SB	0.55396	Yes
Operation and Maintenance Risk Factor (R1: Change and Management RMCM)	Gen. Extreme V alue	0.78323	Yes
Operation and Maintenance Risk Factor (R2: Staffing and Resources RMSR)	Burr	1.2785	Yes
Operation and Maintenance Risk Factor (R3: System/Product Issues RMSPI)	Burr	0.80381	Yes
Acquisition Risk Factor (R1: Financial Issues RAFI)	Burr (4P)	0.78255	Yes
Acquisition Risk Factor (R2: Change Issues RACI)	Wakeby	0.84148	Yes
Acquisition Risk Factor (R3 = Systems/Product RASP)	Burr	0.98954	Yes
Operation and Maintenance Risk Factor (R1: Staffing ROST)	Gen. Logistic	0.69163	Yes
Operation and Maintenance Risk Factor (R2: Operation Issues ROO)	Hypersecant	0.42606	Yes
Operation and Maintenance Risk Factor (R3: Systems ROSY)	Wakeby	0.84081	Yes

Table 8-25: Risk goodness of fit results

In this chapter, the results of the simulation and the goodness-of-fit outcomes for the selected output distributions used for risk and cost factors. The results of the simulation showed that the risk and cost factors are best fitted to different theoretical probability distributions. The best-fit probabilistic distribution was used to present the most influential causes of variation. First, a frequency table of the risk factors was created, and then the observed frequencies were compared to those that would be expected if the hypothesis was correct. This required that the best-fit probabilistic distribution is found to represent the most influential causes of variation. The results of this exercise revealed that a significant number of best-fitting theoretical distributions for causes of variation belonged to different distributions. In general, all the causes of variation assumption distributions were found to be positively skewed theoretical distributions. The selected distribution was validated using the goodness-of-fit tests and the inspection of respective plots. The probability-probability plot revealed a relatively good fit for other regions of criticality for most of the causes of variation distributions. A systematic procedure was adopted here to transform these input probabilities into useable assumptions in the simulation model. For the goodness-of-fit tests, the Anderson-Darling was selected for the different risk and cost factors. The Burr (4P) distribution was the most frequently selected for the risk costs calculation and the Johnson SB distribution for the cost factors.

The above results were verified using the used software 'Easy-fit' and the Anderson-Darling goodness-of-fittest for each risk and cost factor. As demonstrated in the results analysis (see Chapter 7), different theoretical probability distributions for each factor were accepted at all alpha levels, except one risk factor (RIOS) for one alpha level ($\alpha=0.2$). Hence, there is no reason to believe, based on this evidence and these tests, which the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this study. The robustness of the results was also demonstrated by comparing the simulated distributions for duration overrun and based on both original and simulated data.

The comparison results presented in the following table showed that both original and simulated data fit into the theoretical probability distribution. This is further evidence to suggest that the developed model produces results that are similar to real cases.

2. Cost Factors	**Model**	**A-D Test (Statistic)**	**Accepted at All Alpha Levels?**
Camera Cost Factor	Gen. Logistic	0.25856	Yes
Switches Cost Factor	Johnson SB	0.16306	Yes
Servers Cost Factor	Johnson SB	0.13638	Yes
Software Cost Factor	Johnson SB	0.22226	Yes
Monitors Cost Factor	Johnson SB	0.15058	Yes
Storage Cost Factor	Johnson SB	0.12467	Yes
UPS Cost Factor	Error	0.37802	Yes

Control Room Cost Factor	Gen. Logistic	0.17724	Yes
Transmission Cost Factor	Gen. Logistic	0.24638	Yes
Layout Cost Factor	Gen. Extreme Value	0.20475	Yes
Man Power Cost Factor	Gen. Logistic	0.24638	Yes
Power Supply Cost Factor	Johnson SB	0.26349	Yes

Table 8-25: Cost goodness of fit results

Following the statistical analysis of the different risk factors, the LCC models were developed with different categories considering the cost of each phase of the project. The collected data were formed with the adjustment of the present value of each category including the risk and cost factors.

CHAPTER 9. THE WHOLE LIFE CYCLE COST MODEL

9.1 Introduction

In my thesis, the data used to drive the modelling was extracted from 10 companies, thus for each input variables, there were 10 sets of data from which a theoretical probability distribution can be fitted to much the data frequencies. There are many forms and types of pre-defined probability distribution functions that may be used to fit the case study data. In my research @Risk software was used to find the best theoretical distribution that fit each input variable. The software used to model the theoretical distribution employs in excess of 40 continuous distributions to identify the highest ranked theoretical representation of each input variable.

As shown in previous chapters 7 and 8 we have applied the factor analysis for the reduction of the numbers for risk factors and then the Goodness of Fit (GOF) methodology for the risk factors are analyzed for the validation of the data fitting in the probability distributions. For each input variable, the data sample from the case studies sample was analyzed in the simulation software to find determine the best theoretical probability distribution to the actual data set. The "@Risk" software used to conduct the fitting process. This was necessary so that to choose the distribution that has parameters closest to the original dataset. Various distribution fits were investigated for their suitability to represent the input variables. Each distribution is tested and ranked using statistical g goodness-of-fit tests. The following tests were used.

- Chi-squared statistic
- Anderson-Darling statistic
- Kolmogorov-Smirnov statistic

The distribution that was ranked first by **Anderson-Darling** was selected. In addition to the above tests, several graphs P-P and Q-Q are used to visually assess the fitness of the selected theoretical distributions. In the following section, the goodness-of-fit tests for each cost and annual present values (PV) are presented.

9.2 Simulation Model

This section presents the Goodness of fit (GOF) methodology adopted for the different costs as described in the previous chapters. The aim of this simulation is to obtain information how the costs fitting into the probability distributions for all possible outputs results from the simulation process. The simulation process was conducted by repeatedly calculating output values for the dependent variable based on defined randomly selected input values for the independent uncertain variables. As the previous chapter, the software "@Risk" issued for the GOF testing.

In the previous chapter,a LLC model with different categories is created taking into consideration the cost of each phase of the project. An adjustment of the present value for each category including risks and cost factors are presented.

For the appraisal of the physical security projects, present values over a period of 10 years are calculated. In order to capture the variability and uncertainty of the present values variables a methodology based on Monte Carlo simulation is developed.

Then, a present value calculation for each year presented and for the evaluation of risks and uncertainty a sensitivity analysis is applied. The most two parameters can have influenced the data were the maintenance costs and the discount rate. The proposed LCC model follows correctly the variation of the discount rate and for the maintenance costs is arequired improvement using personnel with high technical skills.

Furthermore, the sensitivity analysis is a study that aims to study the effect of variability of the main input parameters, which assist in realizing data evaluation. Sensitivity analysis measures the impact on life-cycle cost project outcomes of changing key input values about which there is uncertainty, typically:

- discount rate
- future inflation assumptions
- period of analysis
- Maintenance, replacement, and operational cost data.

Following to present value (PV) method, a sensitivity analysis was applied to predict what the most sensitive variable is if it changes. In my thesis, sensitivity analysis aimed to examine the following uncertainty variables:

- Sensitivity analysis for the effect of maintenance costs in CCTV solution
- Sensitivity analysis for the variation of the discount rate.

The process adopted for conducting Monte Carlo simulation is depicted in Figure 8-1and summarized in the following steps:

- The different cost and PV values were entered into an Excel spreadsheet format using the risk analysis software @Risk;

- Each independent variable of the developed WLLC model was represented in @Risk by the best probability distribution generated for each cost and annually present values.
- Monte Carlo simulation was used to repeatedly sample random values from each of the independent variables or causes of variation. The simulation was conducted to include the number of optimum iterations that were reported in the literature and in my thesis 1000 iterations is selected.
- The output value was tracked as probability distributions. The results were presented as graphs, histograms,and descriptive statistics;
- The model is also tested for sensitivity and robustness in order to determine the most influential input variables on the dependent construct.

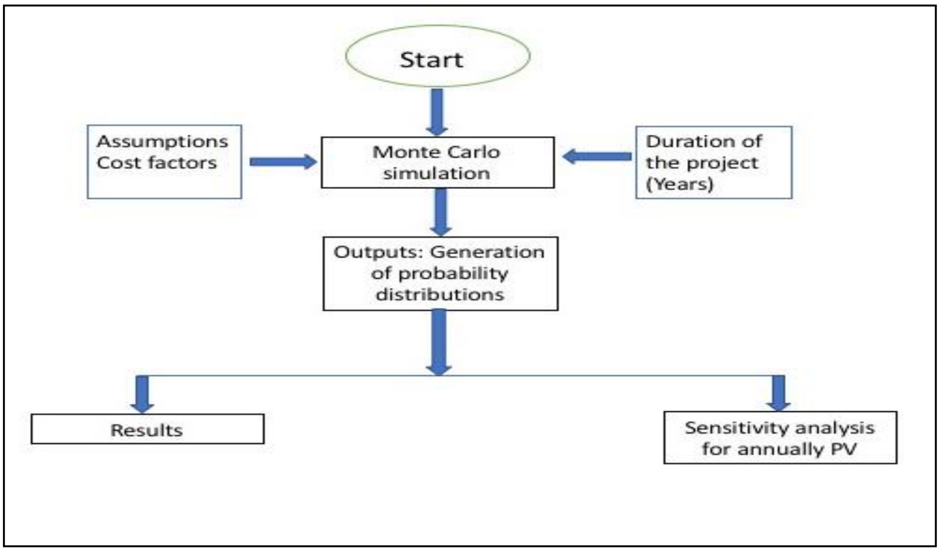


Figure 9-1: The simulation development process

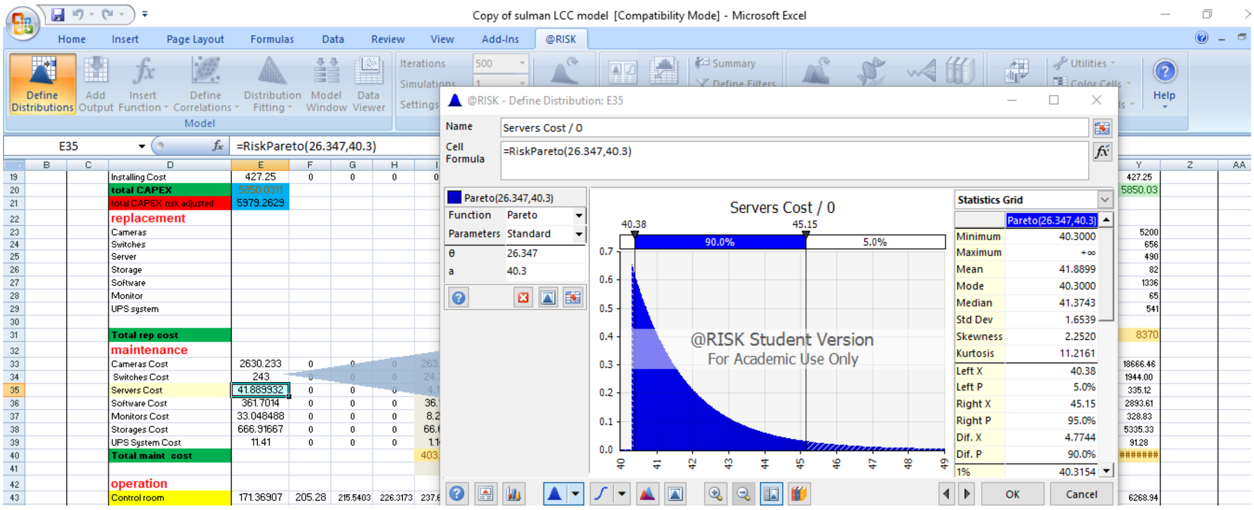


Figure 9-2: @Risk software representation of the simulation model

9.3 Cost Factors Goodness-of-fit Test -Results

The results derived from the simulation software for each cost items. In the following presented each cost separately:

9.3.1 Model Input parameters:

9.3.1.1 Camera Cost

The data sample was analyzed in the probabilistic modelling software for Camera Cost, and it was found that using Anderson-Darling the goodness-of-fit tests, the **ExtValueMin** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.0060

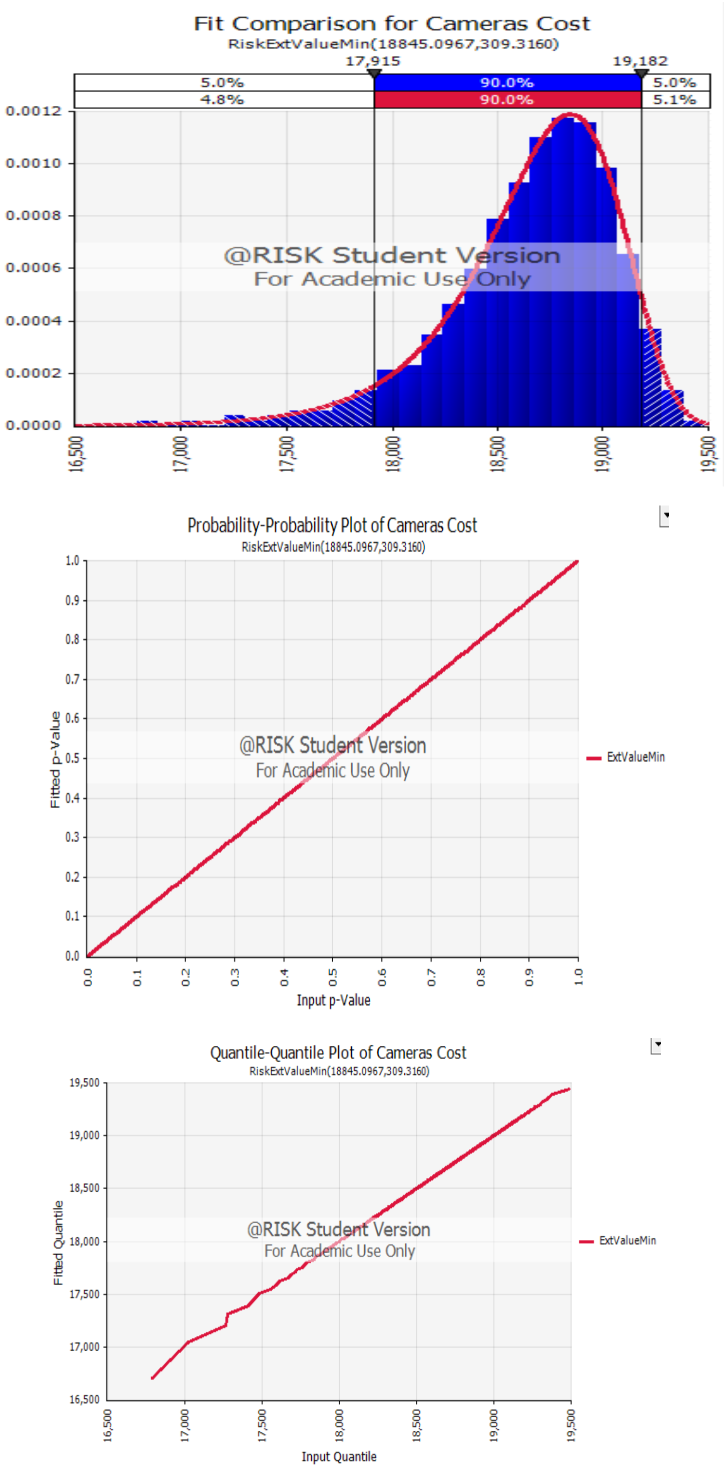


Figure 9-3: Fit comparison for Camera Cost

9.3.1.2 Switches Cost

The data sample was analyzed in the probabilistic modelling software for "Switches costs" and potentials and it was found that using Anderson-Darling the goodness-of-fit tests, the **BetaGeneral** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.0139

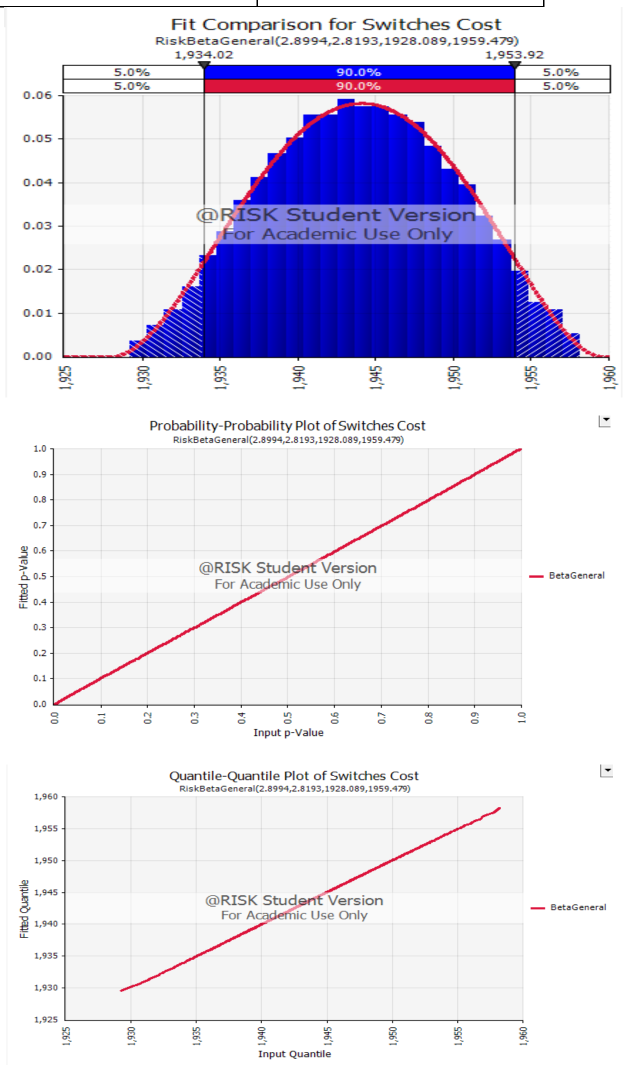


Figure 9-4: Fit comparison for Switches cost

9.3.1.3 Servers Cost

The data sample on Servers cost was analyzed in the probabilistic modelling software for "Servers Cost" and it was found that using Anderson-Darling the goodness-of-fit tests, the **Expon** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.0756

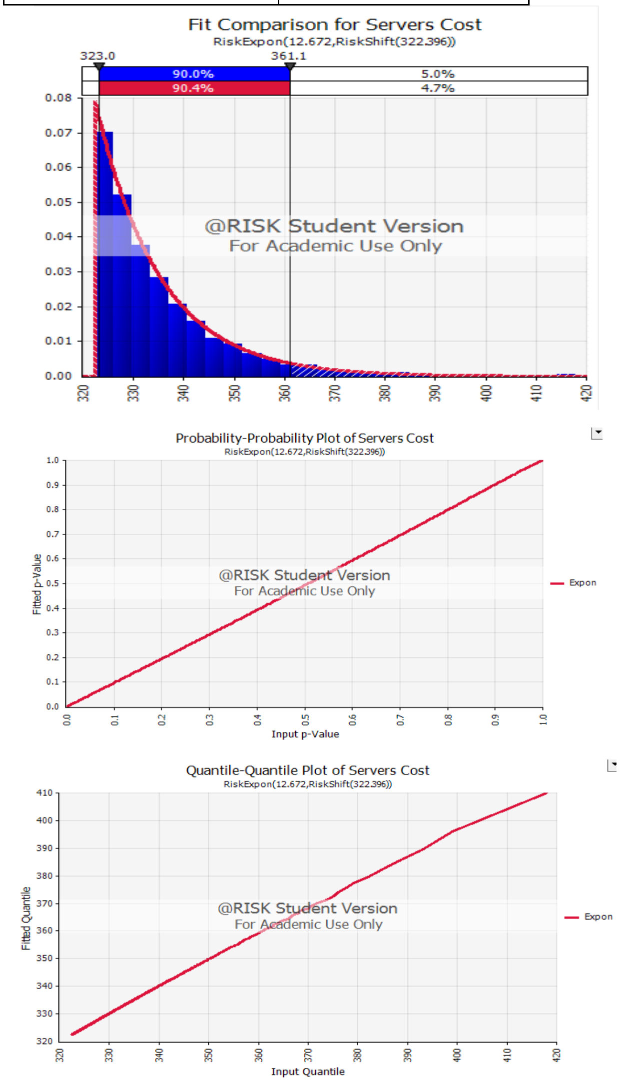


Figure 9-5: Fit comparison for Server Cost

9.3.1.4 Software cost

The data sample on Software cost was analyzed in the probabilistic modelling software for “Software Cost” and it was found that using Anderson-Darling the goodness-of-fit tests, the **Expon** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.0068

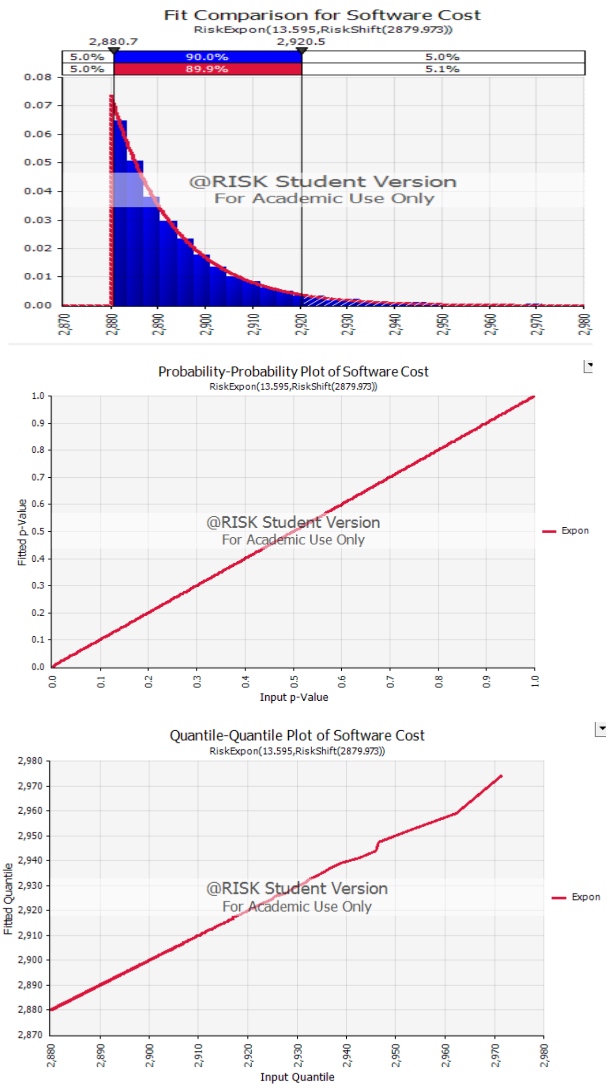


Figure 9-6: Fit comparison for Software cost

9.3.1.5 Monitors cost

The data sample was analyzed for Monitors costs in the probabilistic modelling software for “Monitors Cost” and it was found that using Anderson-Darling the goodness-of-fit tests, the **ExtValueMin** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.0073

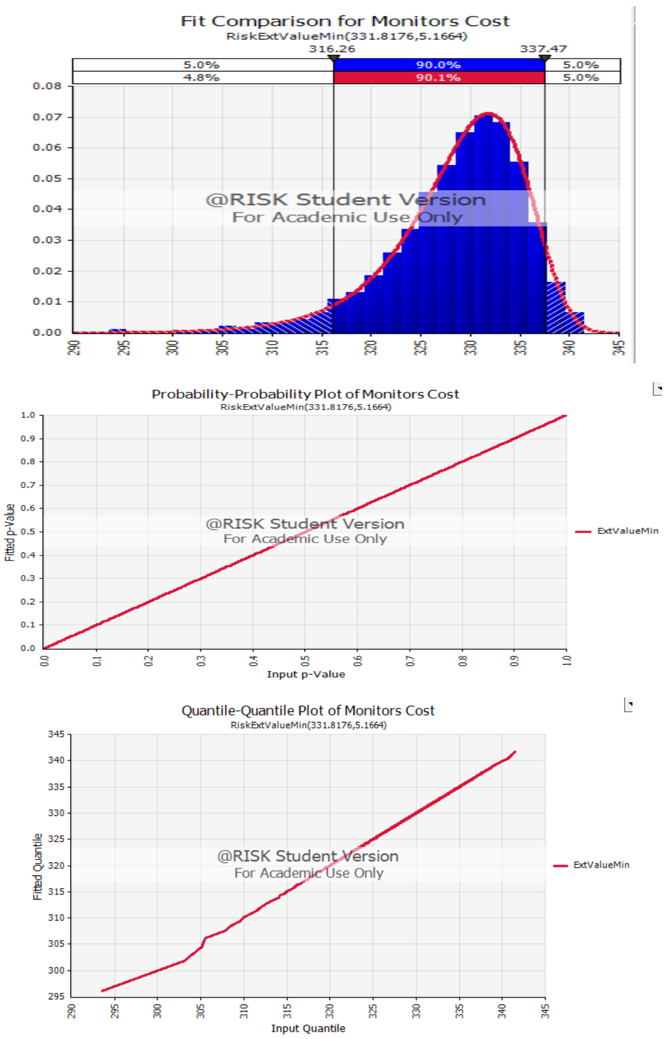


Figure 9-7: Fit comparison for Monitors Cost

9.3.1.6 Storage Cost

The data sample was analyzed on Storage Cost, using the probabilistic modelling software for “Storage Cost” and it was found that using Anderson-Darling the goodness-of-fit tests, the **BetaGeneral** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.0110

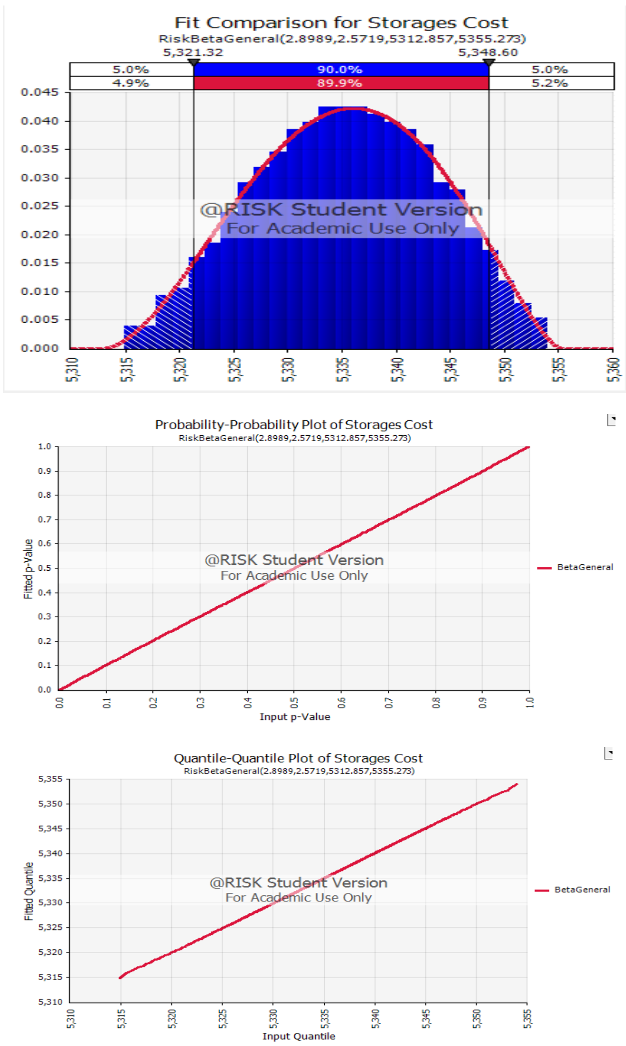


Figure 9-8: Fit comparison for Storage cost

9.3.1.7 UPS system cost

As asimilartest was undertaken for “UPS system” cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **Uniform** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.0953

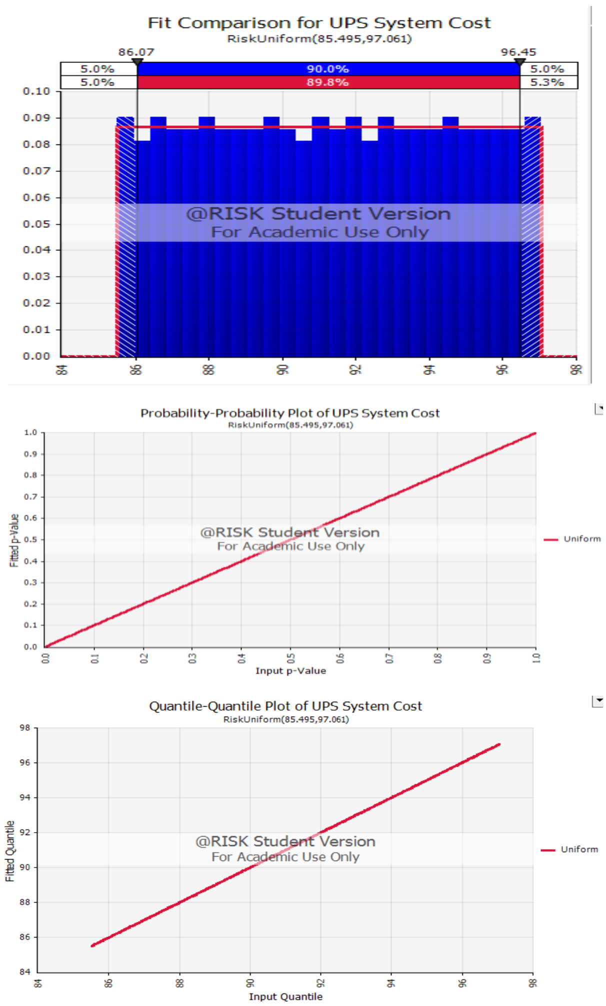


Figure 9-9Fit comparison for UPS System Cost

9.3.1.8 Control room cost

Asimilartest was undertaken for Control Room cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **Logistic** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.0953

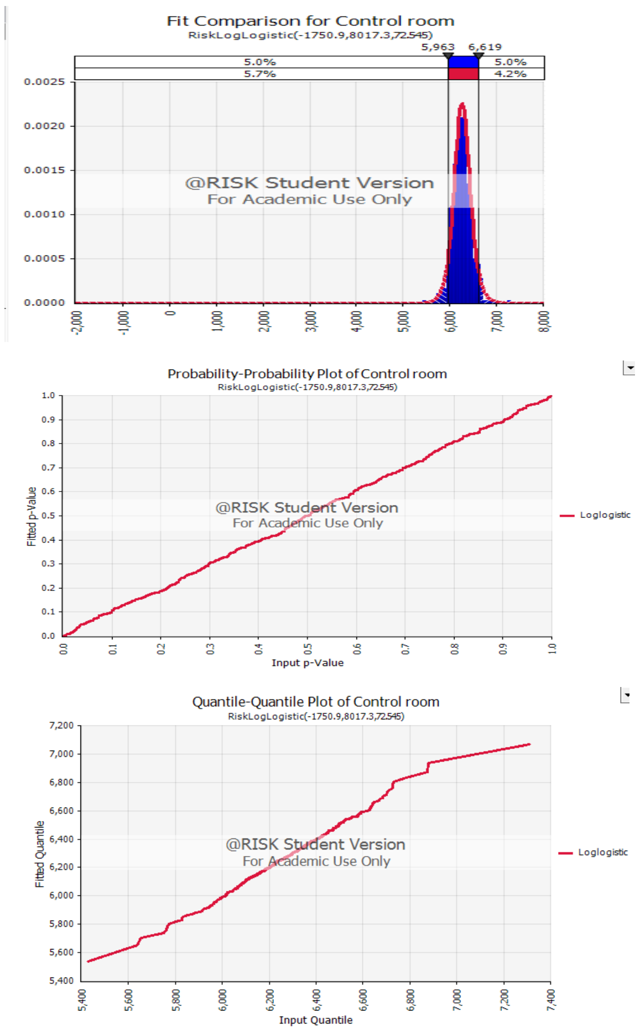


Figure 9-10: Fit comparison for Control Room cost

9.3.1.9 Transmission Cost

As asimilartest was undertaken for Transmission cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **log-logistic** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.2977

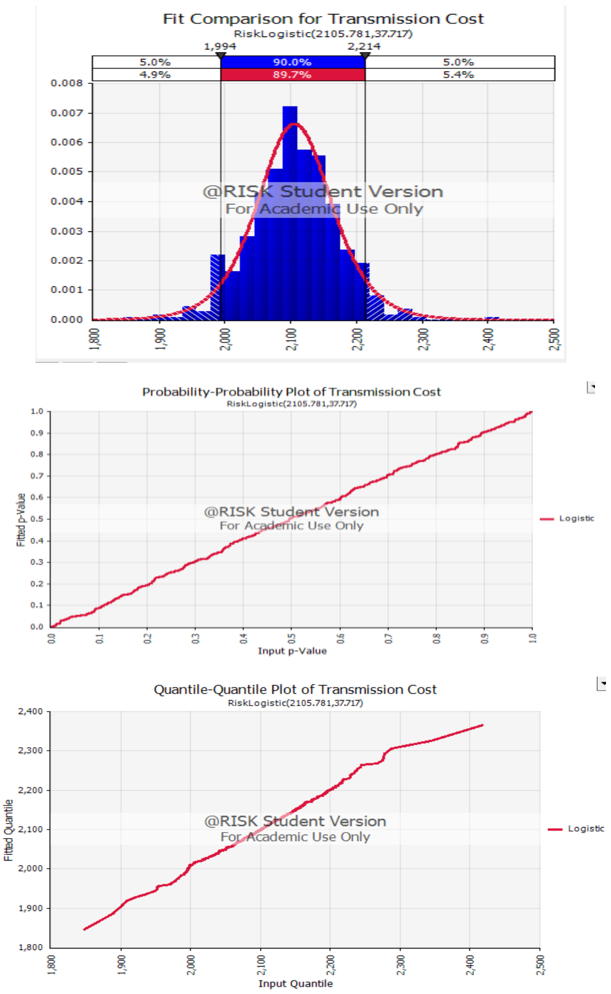


Figure 9-11: Fit comparison for Transmission cost

9.3.1.10 Layout Cost

As thesimilar test was undertaken for Layout cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **BetaGeneral** distribution was the first ranked distribution from available continuous distributions (figure8-11). The goodness-of-fit test parameters were:

test	fit value
A-D	0.1603

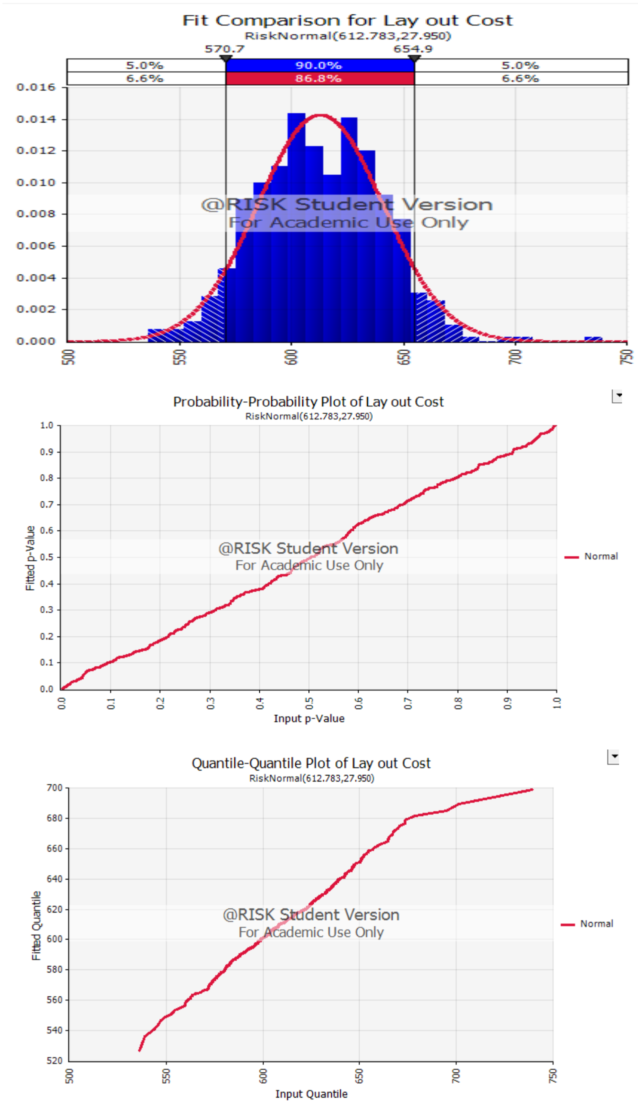


Figure 9-12: Fit comparison for Layout cost

9.3.1.11 Manpower Cost

Assimilartest, was undertaken for Manpower cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **Expon** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.0123

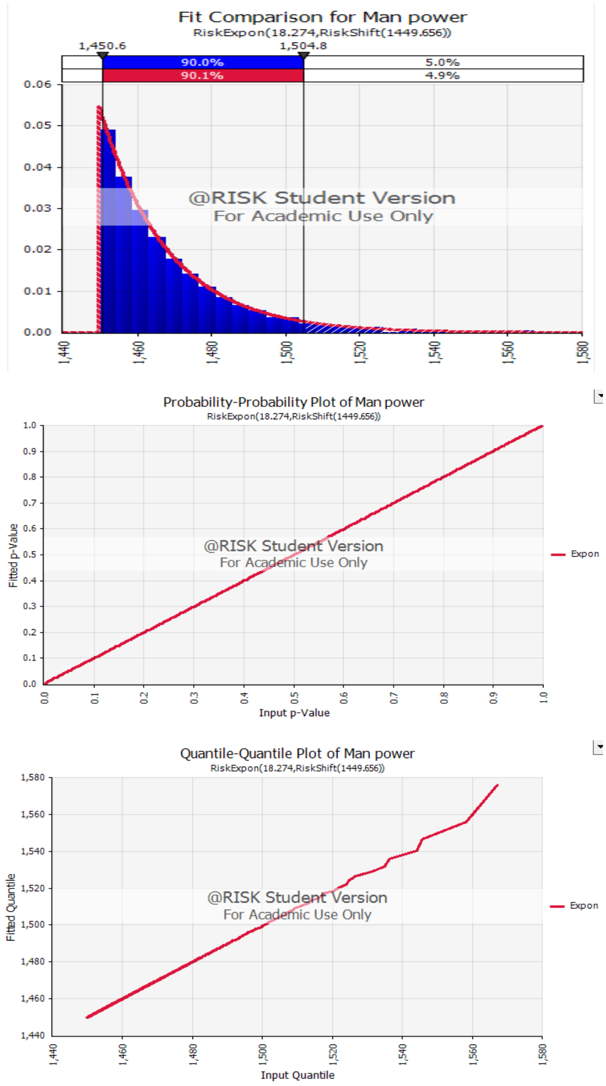


Figure 9-13: Fit comparison for Manpower cost

9.3.1.12 Electricity Power Cost

As asimilartest was undertaken for Electricity Power cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **BetaGeneral** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.2206

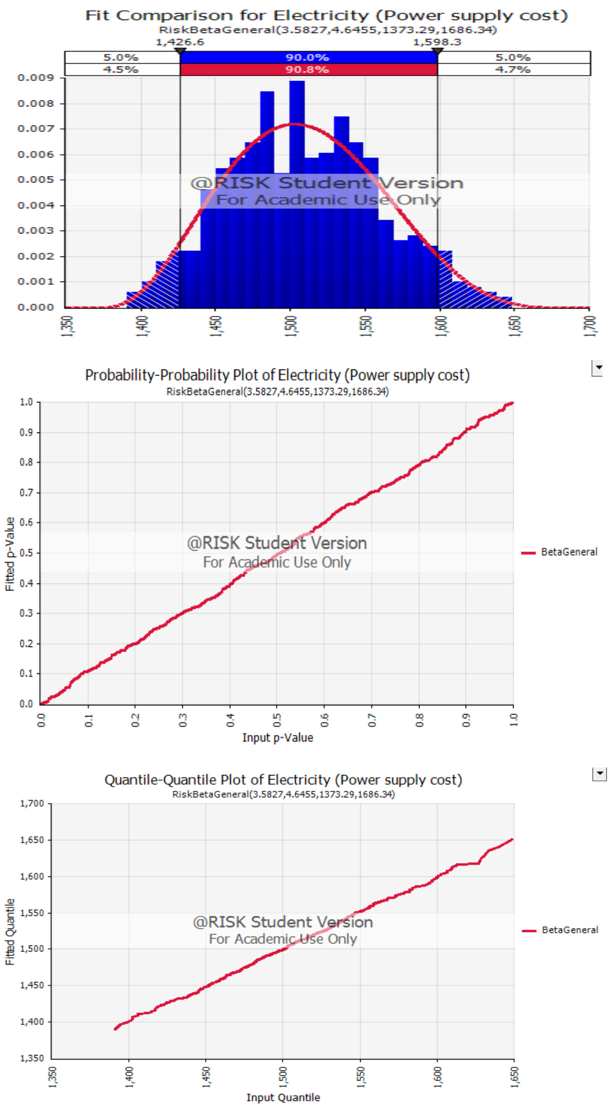


Figure 9-14: Fit comparison for Electricity Power cost

9.3.2 Simulation Results

9.3.2.1 CAPEX Cost

Asimilartest was undertaken for total maintenance cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **ExtValueMin** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.1108

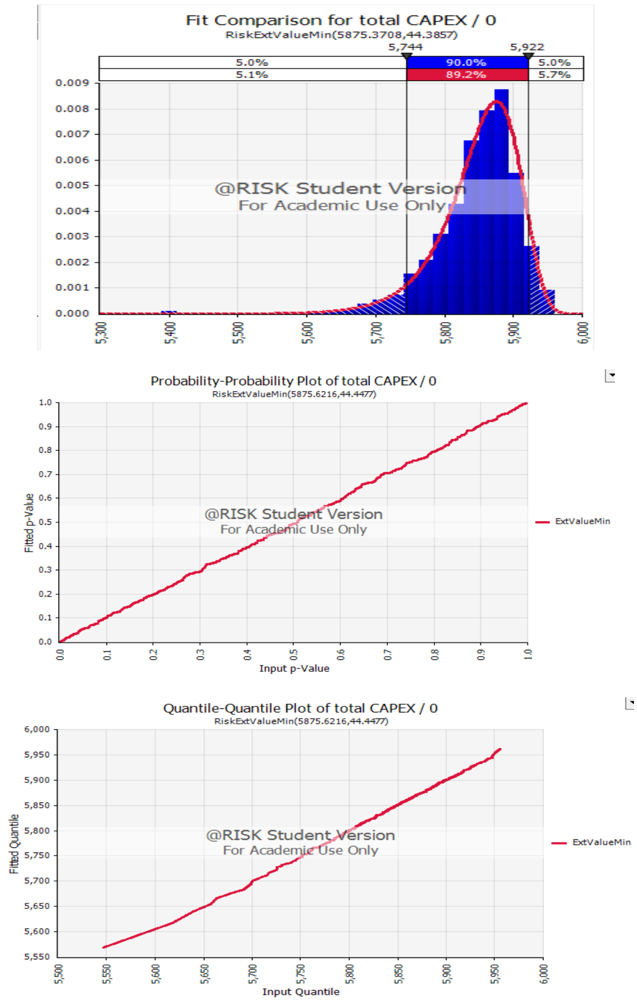


Figure 9-15: Fit comparison for Total CAPEX cost

9.3.2.2 Total CAPEX with Adjusted risk Cost

Asimilartest was undertaken for total maintenance cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **ExtValueMin** distribution were the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	1.6391

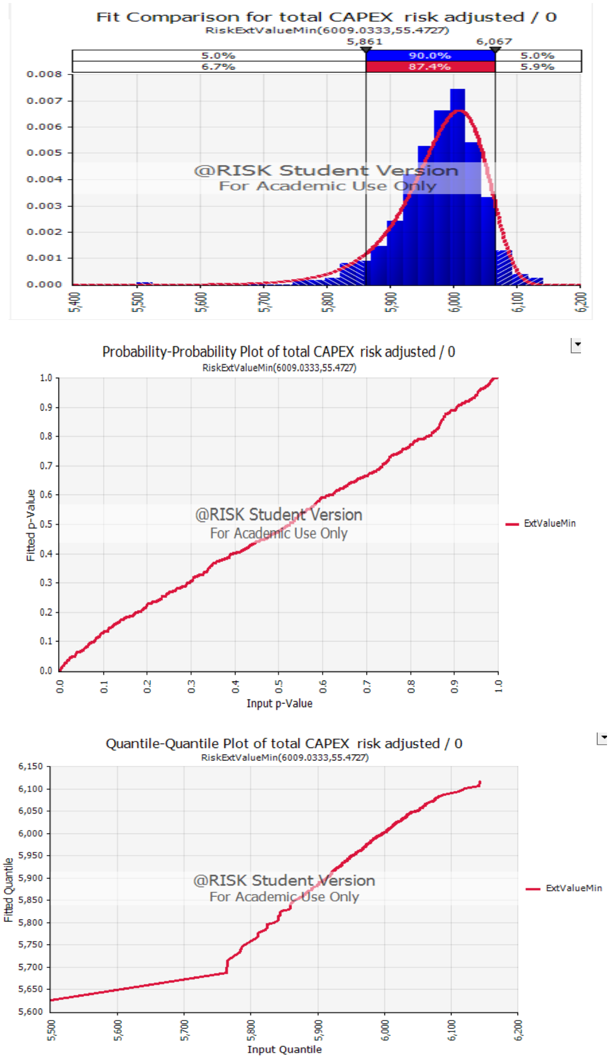


Figure 9-16: Fit comparison for Total CAREX with Adjusted cost

9.3.2.3 Total maintenance Cost

Asimilartest was undertaken for total maintenance cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **ExtValueMin** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.0525

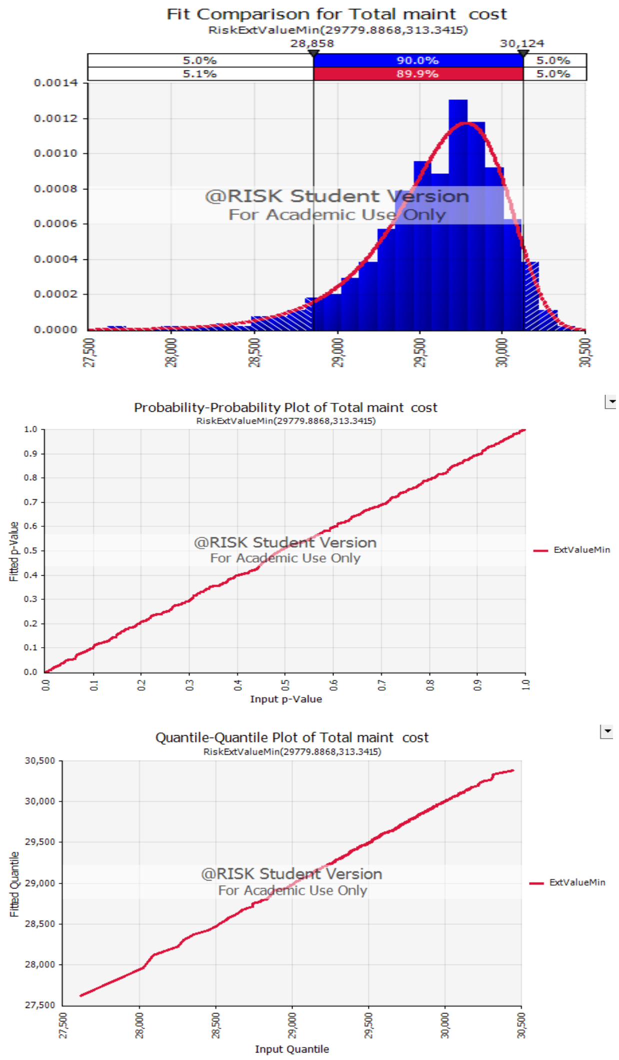


Figure 9-17: Fit comparison for Total maintenance cost

9.3.2.4 Total Operation Cost

Asimilartest was undertaken for total operation cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **Logistic** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.1325

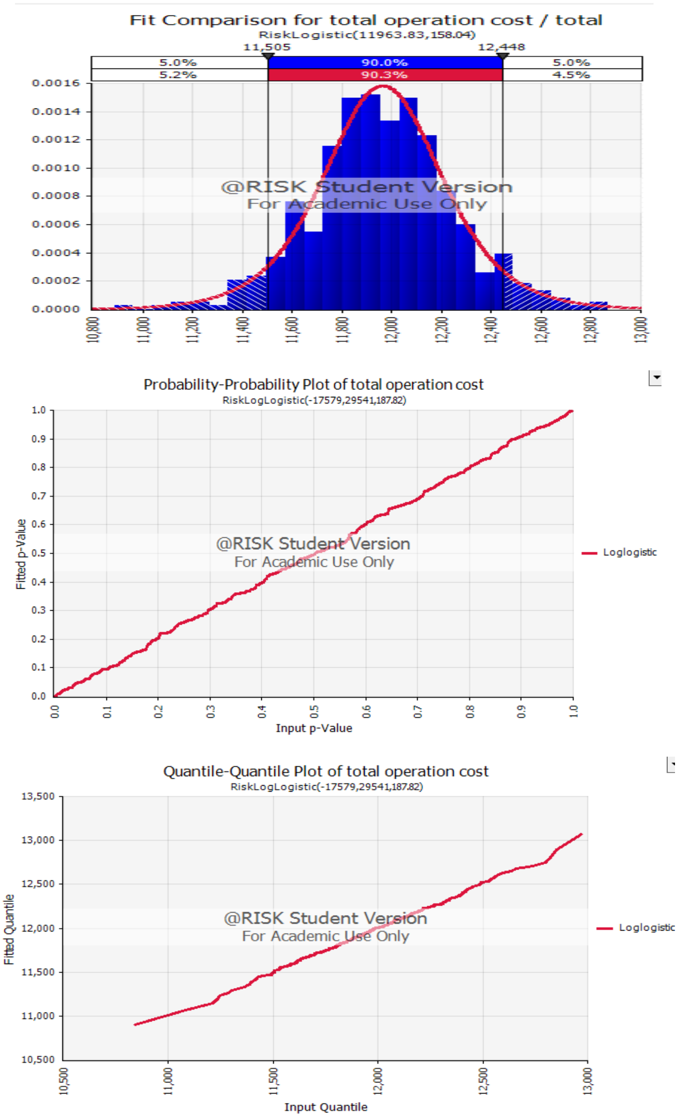


Figure 9-18: Fit comparison for Total operation cost

9.3.2.5 Total Operation with Adjusted risk Cost

Asimilartest was undertaken for total operation cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **Logistic** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.2276

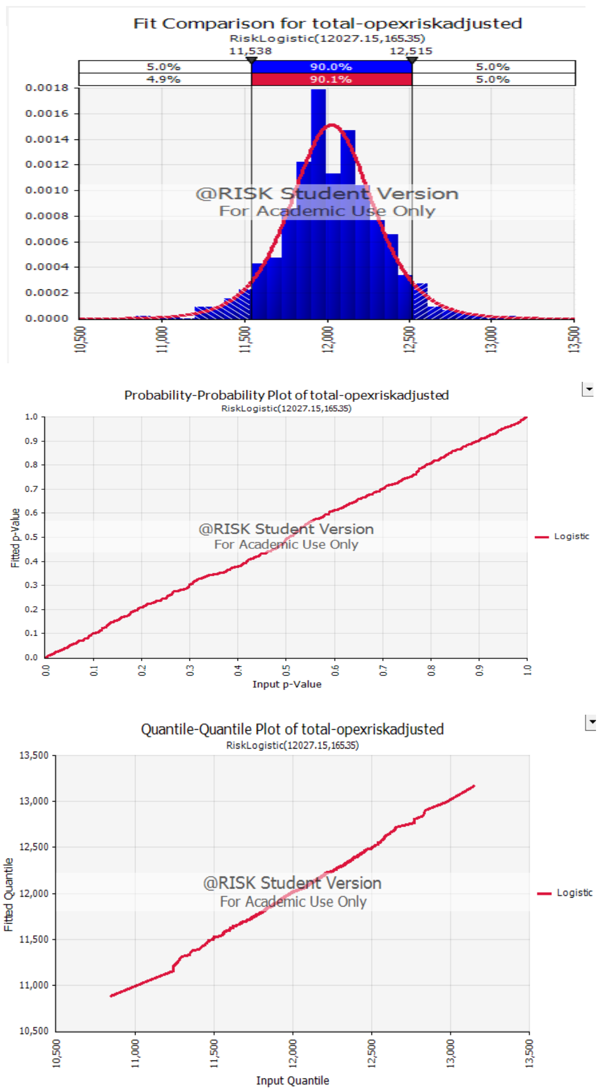


Figure 9-19: Fit comparison for Total operation with Adjusted risk cost

9.3.2.6 Total LCC Cost

Asimilartest was undertaken for total LLC cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **Weibull** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.3138

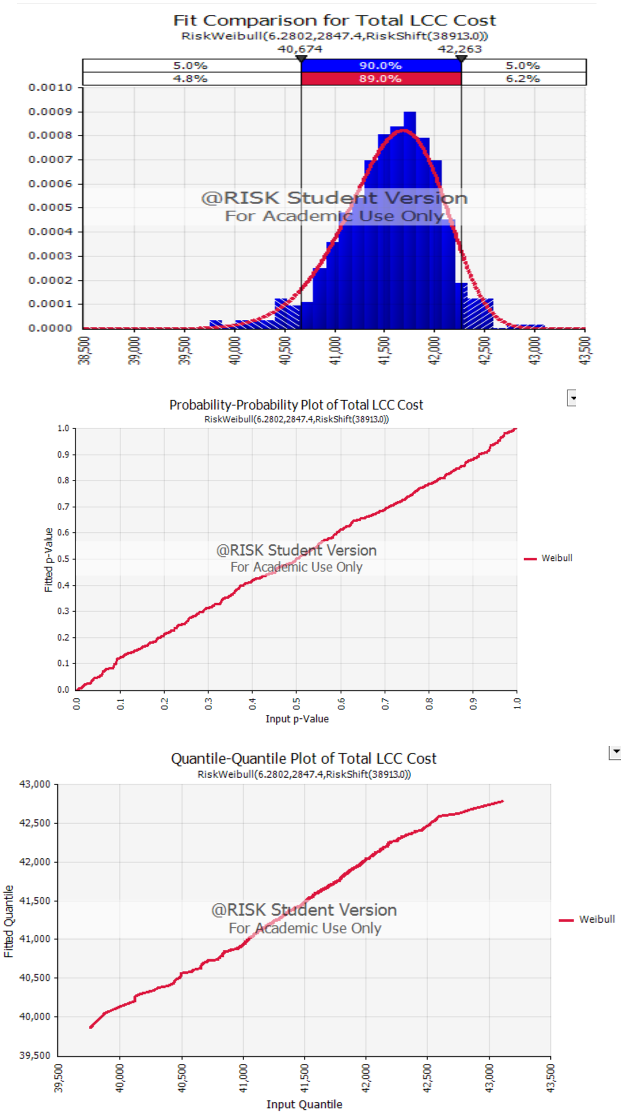


Figure 9-20: Fit comparison for Total LCC cost

9.3.2.7 Total PV Cost

Asimilartest was undertaken for total PV cost. The data sample was analyzed in the probabilistic modelling software and it was found that using Anderson-Darling the goodness-of-fit tests, the **Weibull** distribution was the first ranked distribution from available continuous distributions. The goodness-of-fit test parameters were:

test	fit value
A-D	0.3110

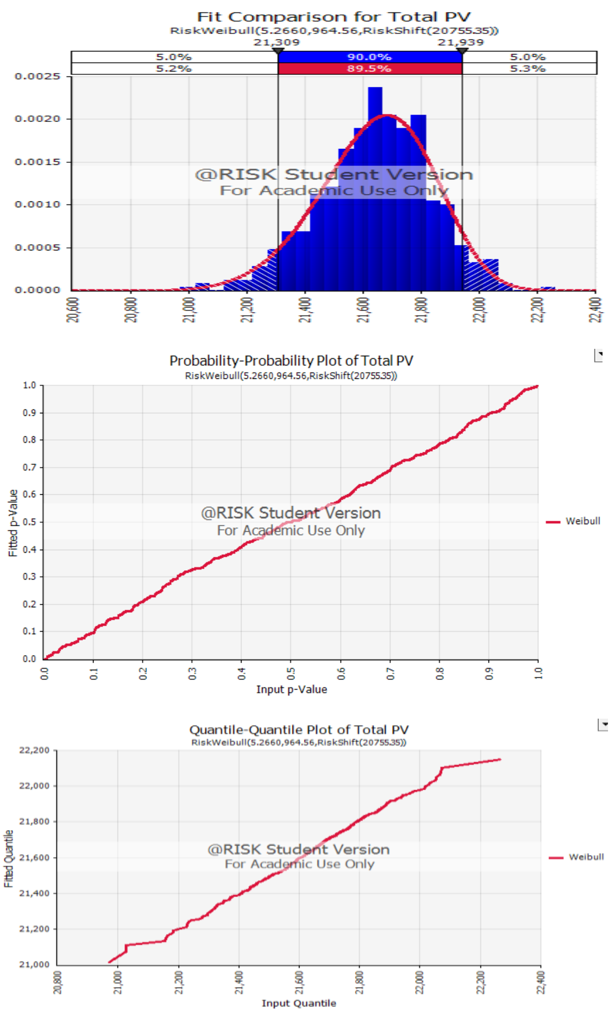


Figure 9-21: Fit comparison for Total PV cost

9.4 Summary of Test Results –Distribution

In this section, the goodness-of-fit tests for each separated cost presented using the simulation software to determine the best probability distribution to the actual dataset using Anderson-Darling test. In the Table, (9-1) shows the results of the fitting procedure tests.

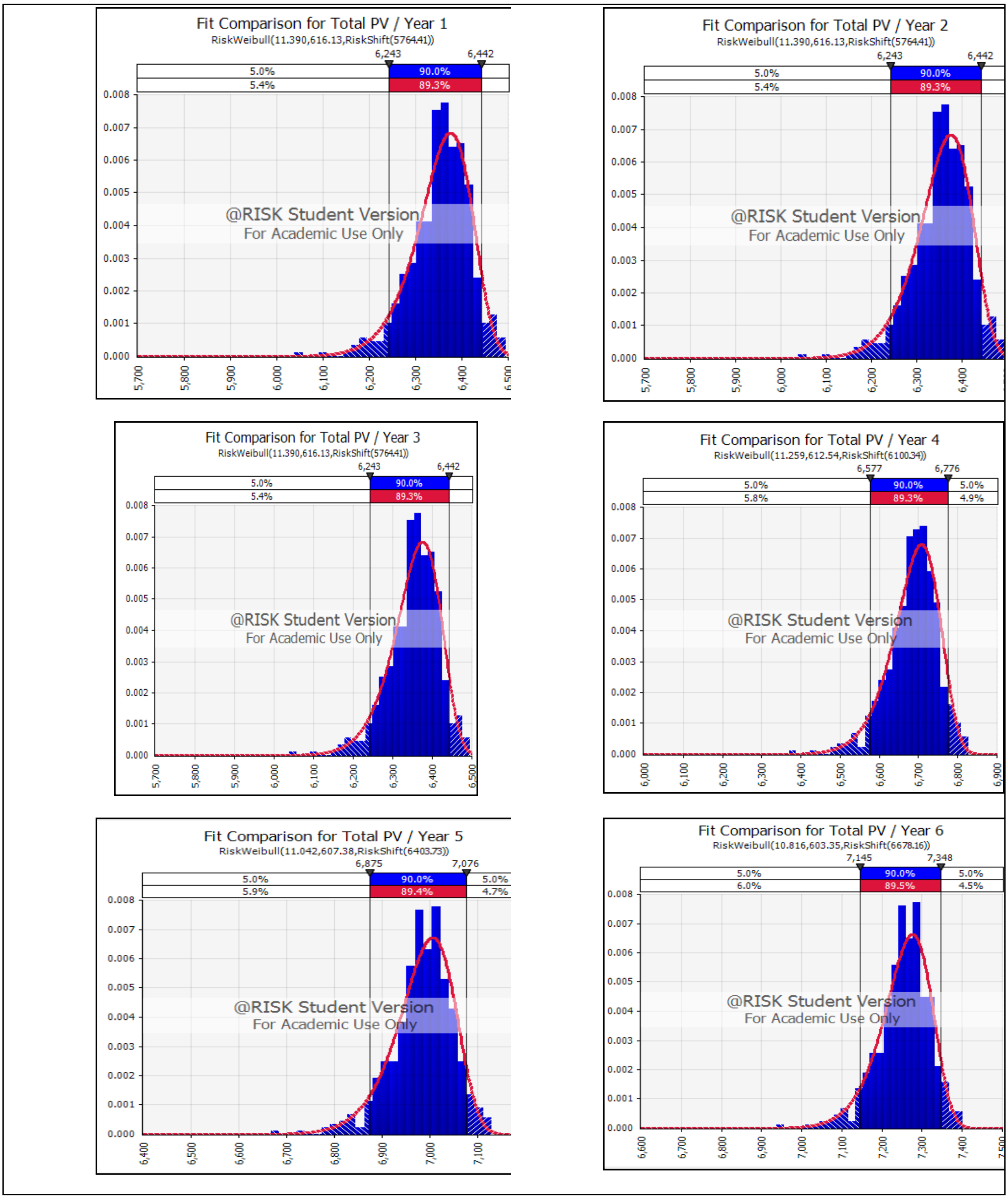
Table 9-1: Summary of the Anderson-Darling goodness of fit results

	Cost Items	**First ranked distribution Using the Anderson-Darling The goodness of fit test**	**Categories Costs**
1	Cameras cost	ExtValueMin	Capital, Replacement, Maintenance costs
2	Switches cost	BetaGeneral	Capital, Replacement, Maintenance Costs
3	Servers cost	Expon	Capital, Replacement, Maintenance costs
4	Software cost	Expon	Capital, Replacement, Maintenance costs
5	Monitor cost	ExtValueMin	Capital, Replacement, Maintenance costs
6	Storage cost	BetaGeneral	Capital, Replacement, Maintenance costs
7	UPS cost	Uniform	Capital, Replacement, Maintenance costs
8	Control room cost	Logistic	Operational costs
9	Transmission cost	LogLogistic	Operational costs
10	Layout cost	BetaGeneral	Operational costs
11	Manpower cost	Expon	Operational costs
12	Electricity cost	BetaGeneral	Operational costs
13	Total CAPEX	ExtValueMin	
14	Total CAPEX Adj	ExtValueMin	
15	Total maintenance	ExtValueMin	
16	Total operation	Logistic	
17	Total operation Adj	Logistic	
18	Total LCC	Weibull	
19	Total PV	Weibull	

It can be observed from the above table that different distributions were founded for each cost. However, it’s very difficult to assign only one distribution for our fit-tests distributions.

9.5 Simulation of annual cost present values

In this section, the annual present value (PV) was calculated in the spreadsheet for 10 years. A discount rate of 5% was used. The simulation results derived from the Monte Carlo simulation for each year in order to derive the annual PV cost.



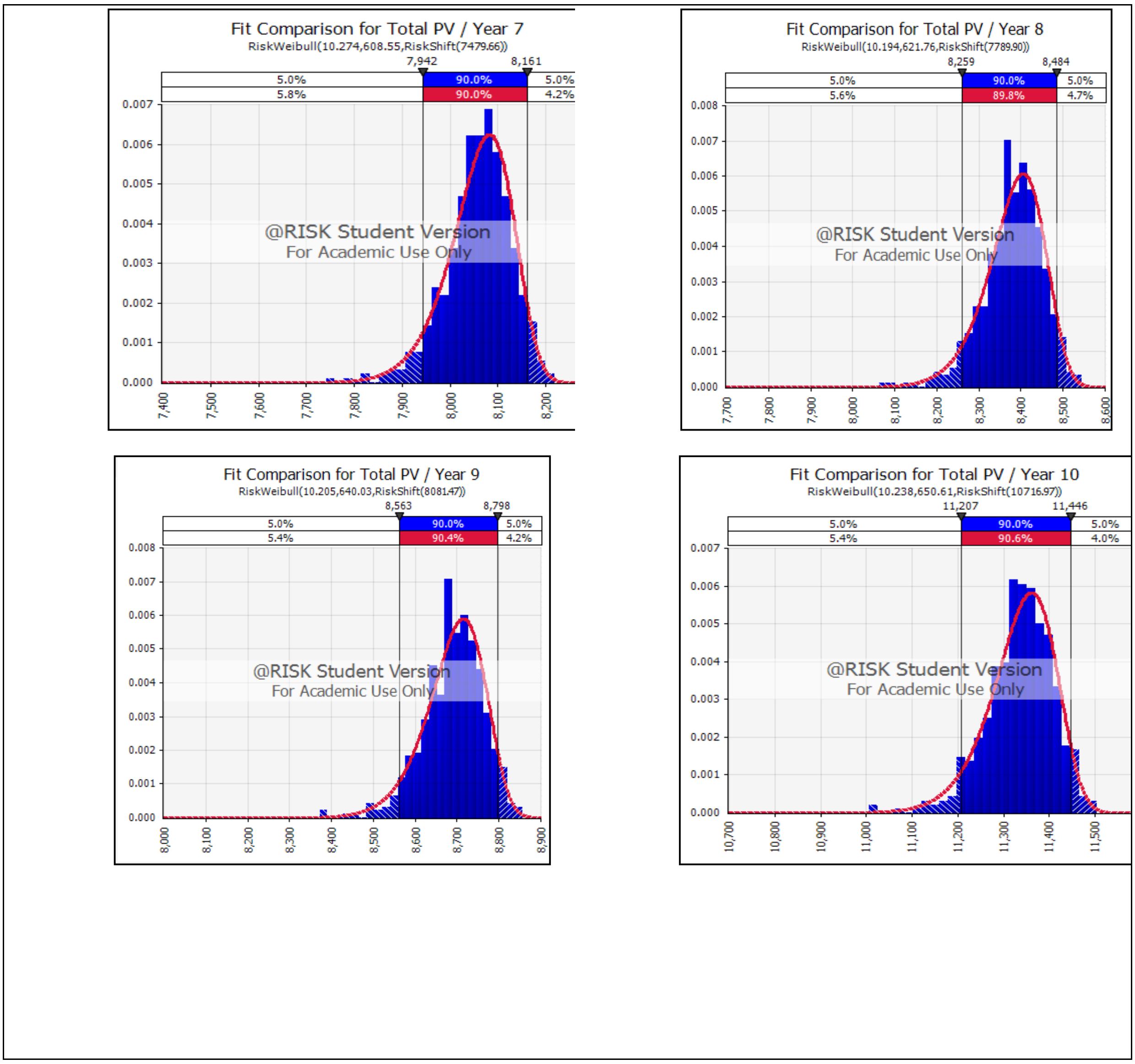


Figure 9-22: Comparison PV cost Distribution for 10 years

The present value distribution was best represented by the Weibull distribution and the results are presented in Fig. 9-22.

9.6 *Trends*

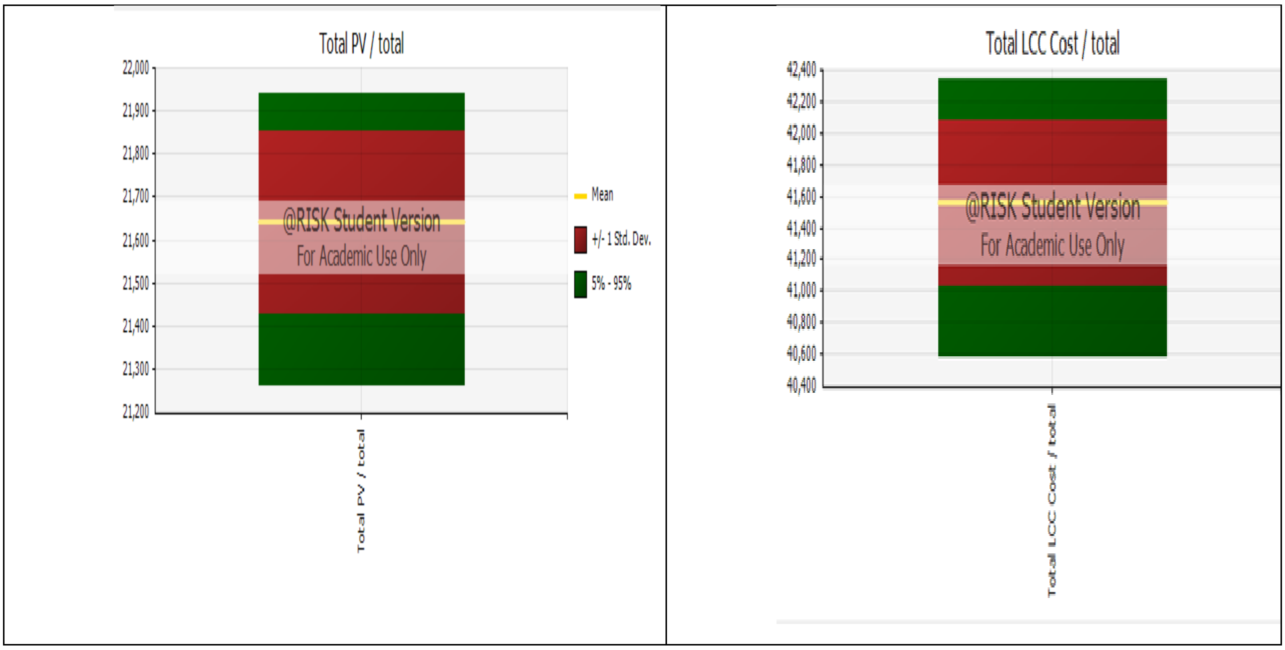


Figure 9-23: Comparison of Trends of LCC & PV

In the Fig. 8.23 shows the simulated present values for the selected year within the band levels between 5% and 95%. The level band percentage provides that the present values for the selected year lie within the limit levels. Also, shows the Total LCC with the same level of bands but different presents.

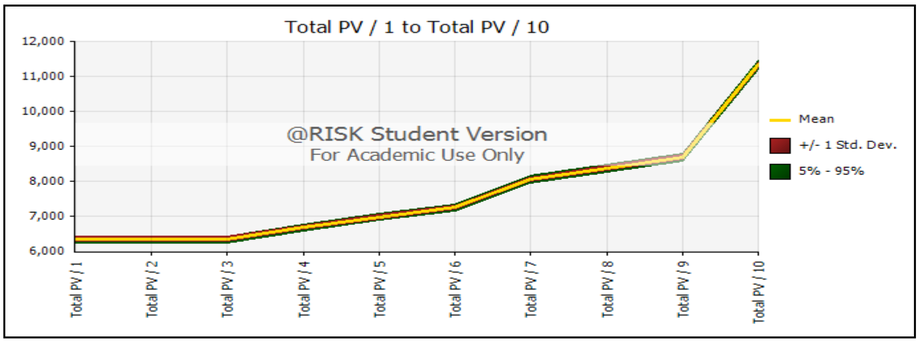


Figure 9-24: Trends for present value distribution

The +/- 1 Std Dev certainty band, for example, reveals that more than 50% of the simulated present values (PVs) lies within the band. The minimum and maximum end-points of the certainty ranges can be obtained by looking at the value axis to the left of the chart area. The trend graph of the input data shows that the bulk of data revolves around the +/- 1 Std Dev certainty band.

9.7 Sensitivity Analysis

Sensitivity analysis is a study that aims to study the effect of variability of the main input parameters, which assist in realizing data evaluation. Tesfamariam& Sanchez-Silva (2011) have used a sensitivity analysis to measure the effect of various building performance on LCC. Results of the sensitive analysis show that construction quality has the most impact on LCC; however, plan irregularity was the lowest impact. Sensitivity analysis measures the impact on life-cycle cost project outcomes of changing key input values about which there is uncertainty, typically:

- Discount rate
- Future inflation assumptions
- Period of analysis
- Maintenance, replacement, and operational cost data.

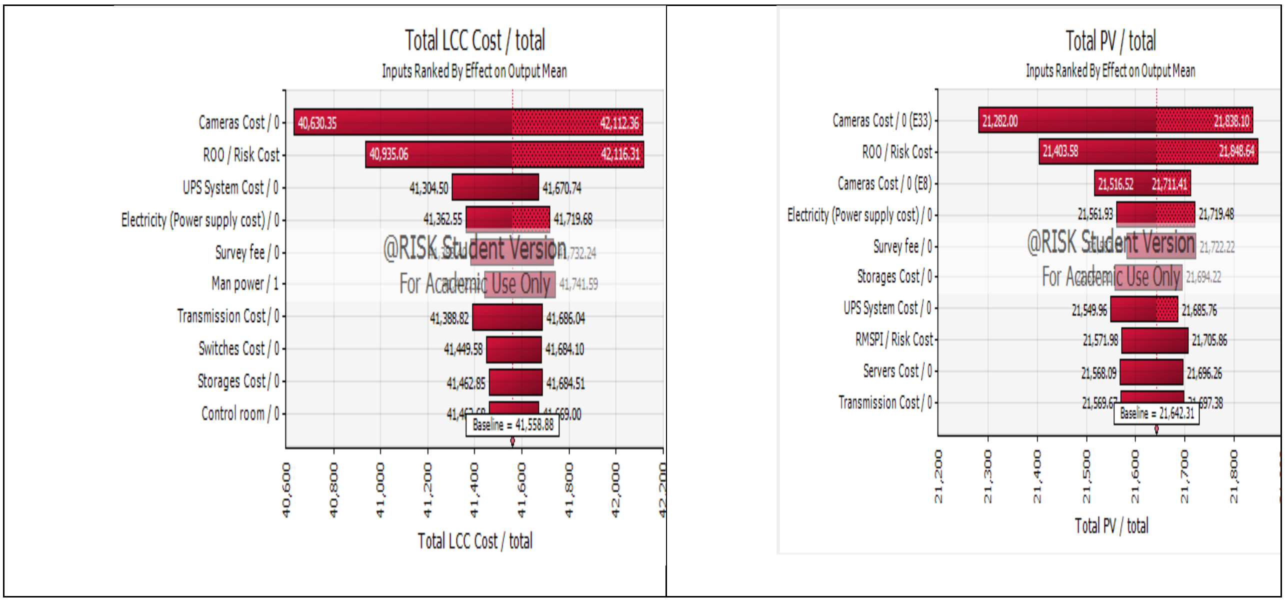


Figure 9-25: Comparison of different Output means

The sensitivity results in Figure 9-25 above shows and compares between the LCC and PV for in the magnitude of the effect of causes of variation on duration for each. The figure presents the magnitude of the effect causes of variation on duration overrun is mainly positive. The chart above reviewed the effect that each input variable has on the output variable as a result of the performed simulation analysis. This kind of results is also affected by the weight connected with each input variable. The level of the effect that each input variable has on the output variable was evaluated from the size of the relevant bar that each input variable represents, so if the impact is positive to the right or negative to the left of the center line defines.

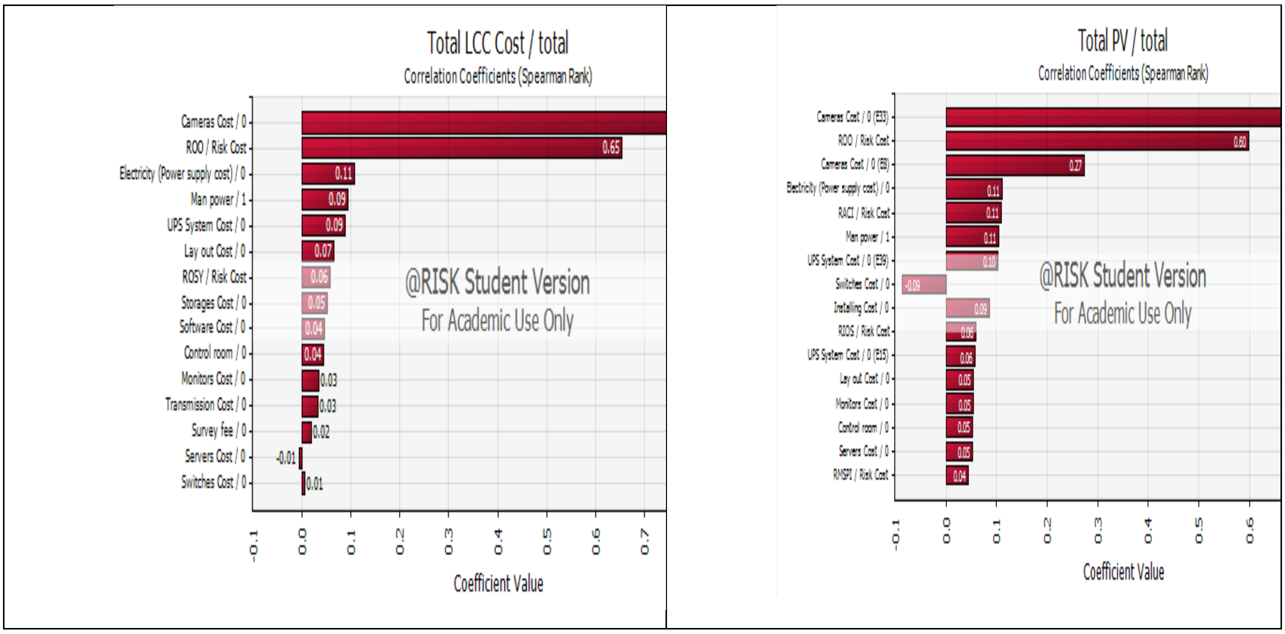


Figure 9-26: Comparison of different Coefficients (Spearman)

The sensitivity results in Figure 9-26 above shows and compares between the LCC, and PV for in causes of variation input used to measure the sensitivity of the output for total PV cost.

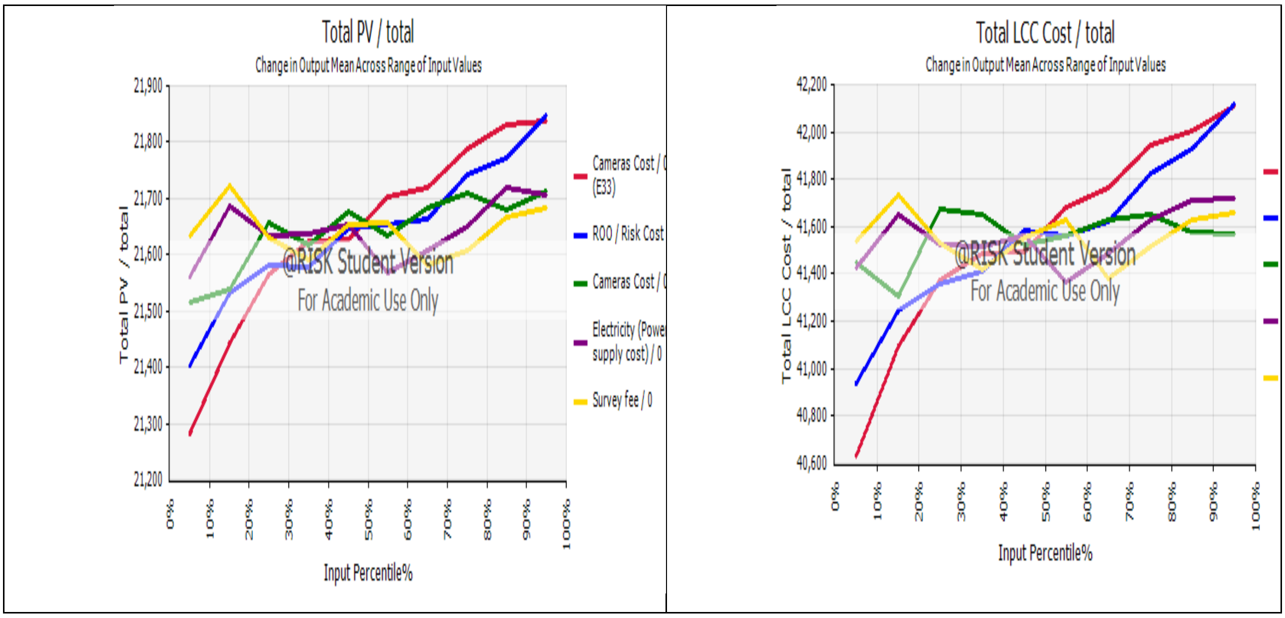


Figure 9-27: Comparison of Different spider charts for different outcomes

The sensitivity results Figure 9-27 above shows and compare between the LCC and PV for in Spearman rank correlation coefficient for analysis of the sensitivity of the variables. So each shows the relative sensitivities of the causes of variation input probability distributions on the simulated forecasted duration overrun percentage. The sensitivity analysis outcome was also verified graphically via "tornado" charts. In the x-axis of the chart, it characterizes the % of variation in the expected values of the output duration variation. The input disturbing the output variable is shown on the y-axis.

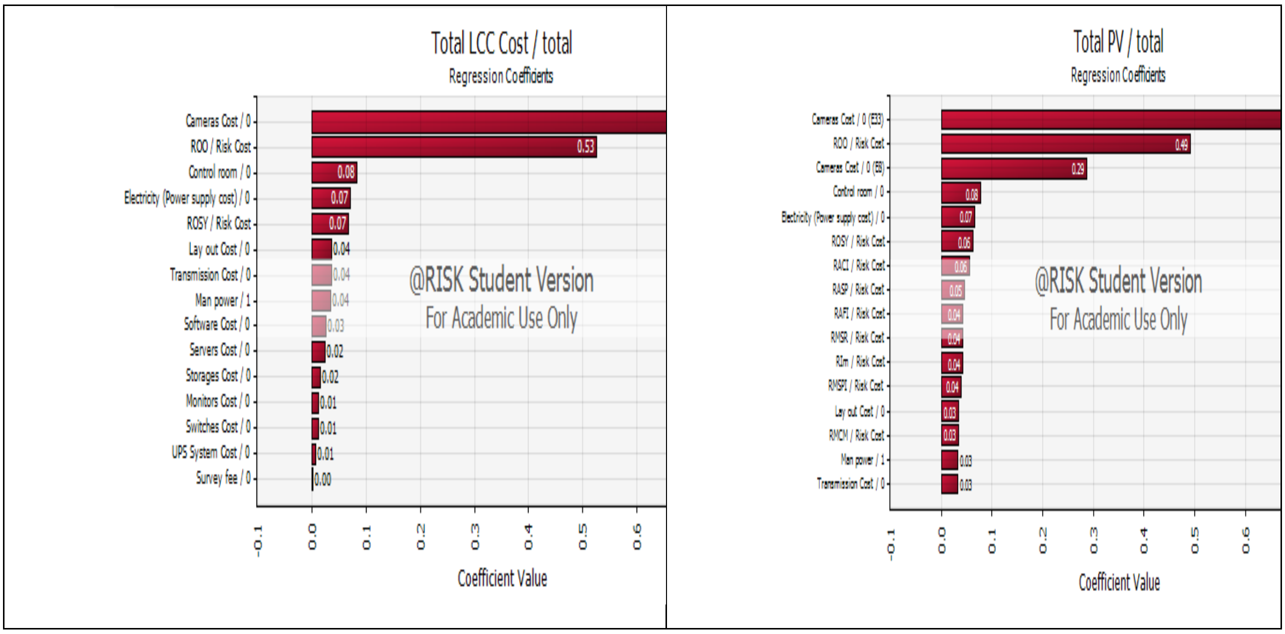


Figure 9-28: Comparison for different Regression Coefficients for PV & LCC

The sensitivity results in Figure 9-28 above shows and compares between the LCC, and PV for in results for sensitivity analysis of change from base values for input variables. As it's another techniques were also experimented in performing sensitivity analyses on the duration overrun. The figure shows there 15 causes of variations that have a positive effect on duration overrun for the total LCC and 16 causes of variations that have a positive effect on duration overrun for PV. Focusing at "Camera Cost" has a very high positive correlation with duration overrun for both sides. It is also obvious that most causes of variations have negative coefficients. So, as the rate of any of these causes of variation increases, the value of the duration overruns decreases. This gives an idea these causes of variation have a lower effect on duration overrun if their value estimated high. Although ,it can be visible if their estimate impact is lower than the affect band.

Sensitivity analysis can be carried out for different combinations of input values and several parameters can be altered at the same time. Sensitivity analysis identifies how significant specific input parameters or combinations of parameters are in determining the LCC outcomes and indicates the range of variability in the output, allowing decision makers to concentrate onthe analysis of the most critical parameters. Carrying out sensitivity analysis can also indicate a potentially inefficient outcome not otherwise apparent. Sensitivity analysis is useful for identifying critical LCC estimating assumptions, but it has limited effectiveness in providing a comprehensive sense of overall uncertainty.

Following to present value (PV) method a sensitivity analysis was applied to predict what the most sensitive variable is if it changes. In my thesis, sensitivity analysis aimed to examine the following uncertainty variables:

- Sensitivity analysis for the effect of maintenance costs in LCC CCTV solution
- Sensitivity analysis for the variation of the discount rate.

Moreover, Sensitivity analysis results can be verified graphically using tornado diagrams. The change in the approximated values of the output duration variation is demonstrated on the x-axis. The input affecting the output variable is demonstrated on the y-axis. The research has also introduced some other analysis i.e. the Spearman rank correlation coefficient, Mapped Vales correlation coefficient, Contribution to Variance correlation and Contribution to Variance correlation coefficient. It added such analysis to investigate the sensitivity of the output from the model to the causes of variation inputs. The higher the correlation between outputs and inputs; the greater of the input in the formation of the output value.

9.7.1 Sensitivity analysis for the effect of maintenance costs.

The maintenance costs in LCC model plays an important contribution to the total cost. With the sensitivity analysis compared the LCC total cost with the LCC cost without including the maintenance cost. The results are reflected in Table 9-3.

LCC model CCTV systems	Initial Costs (AED)	Replacement Costs (AED)	Maintenance costs (AE)	Operations costs (AED)	Total LLC costs (AED)	Total PV (AED)
	[A]	[B]	[C]	[D]	[C+D]	
LCC model with maintenance	5,978	8,370	29,595	11,906	41,501	21,620
LCCmodel without maintenance	5,978	8,370	0,00	11,906	11,906	10,465

Table 9-3 – Lifecycle costs of CCTV systems with and without maintenance

Not performing any maintenance activity induces a decrease of 52% in the NPV of the LLC model solution, which proves that maintenance activities during the life cycle bare high costs, they are necessary to improve the correct usage from the personnel. The personnel required to have technical skills and experience for the CCTV security components such as cameras, and IT systems.

9.7.2 Variation of the discount rate

In order to verify the effect of the discount rate in this study, calculations are made for a discount rate of 2%. With the sensitivity analysis compared the LCC cost and PV total cost between two discount rates 5% and 2%. The results are presented in Table 9-4.

LCC model CCTV systems	Initial Costs (AED)[A]	Replacement Costs (AED) [B]	Maintenance costs (AED) [C]	Operations costs (AED) [D]	Total LLC costs (AED) [C+D]	Total PV (AED)
	[A]	[B]	[C]	[D]	[C+D]	
LCC model with 5% discount rate	5,978	8,370	29,595	11,906	41,501	21,650

Table 9-4: Lifecycle costs of CCTV systems for a discount rate of 2%

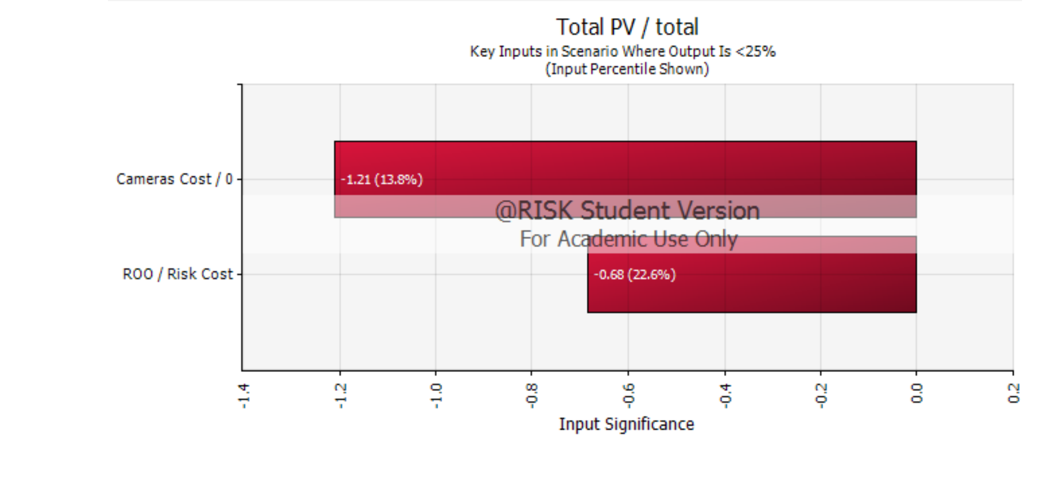
For a discount rate of 2%, the LCC model presents the life cycle costs higher than for the discount rate of 5%. The model LCC follows correctly that increased the discount rate the present value (PV) was decreased.

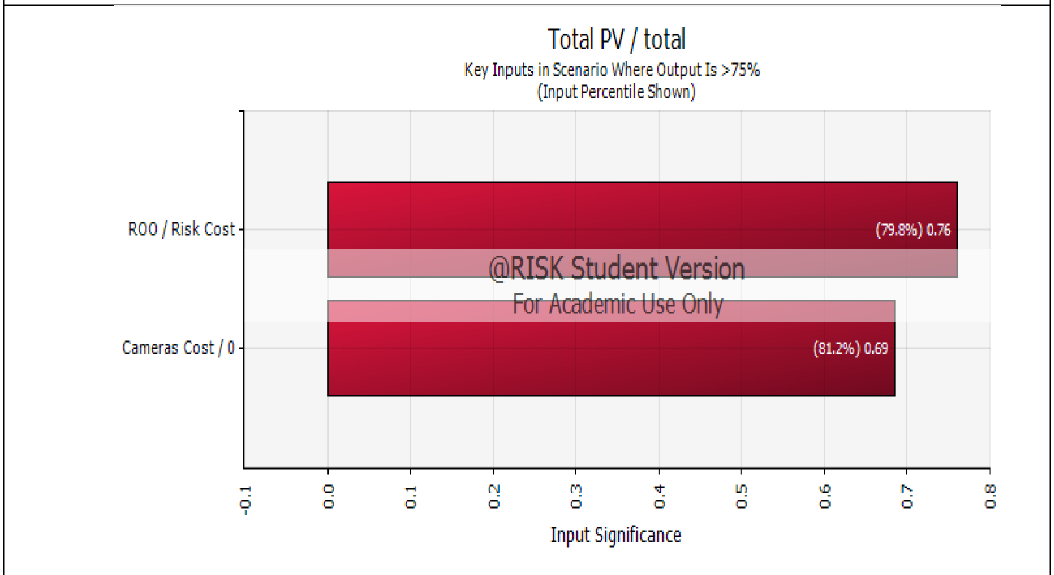
9.8 *Scenario Analysis*

Scenario analysis is also used to examine the influence that given input changeable has on the output founded on the restricted median analysis. In this research, the scenario mark values that were applied in the examination were:

- duration overrun > 75th%
- duration overrun < 25th%
- duration overrun > 90th%

The results of this exercise are shown in Figure 9-65 and Figure 9-66 below.





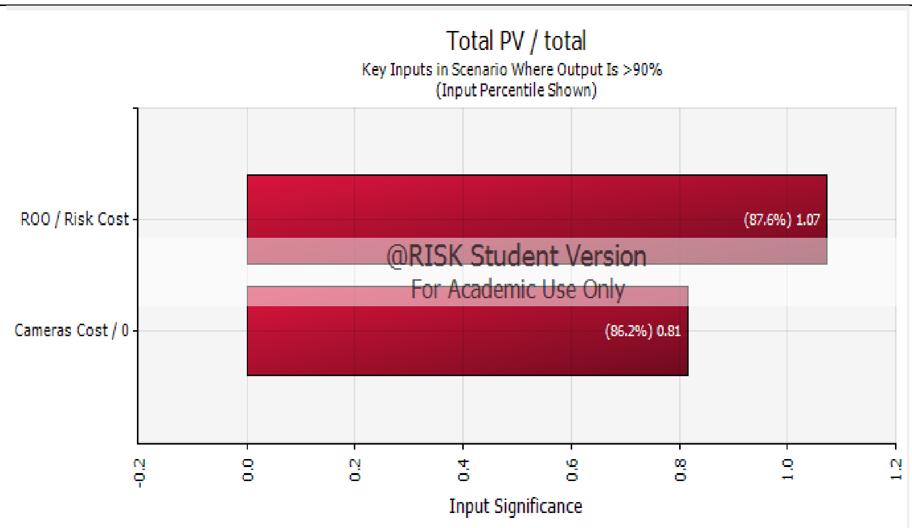


Figure 9-29: Comparison for variation in total PV > 75th % &< 25th % &> 90th %

9.9 *Summary*

In this chapter presented the goodness-of-fit tests for each separated cost presented using the simulation software to determine the best probability distribution to the actual dataset using Anderson-Darling test. Then, a present value calculation for each year presented and for the evaluation of risks and uncertainty a sensitivity analysis is applied. The most two parameters can have influenced the data were the maintenance costs and the discount rate. The proposed LCC model follows correctly the variation of the discount rate and for the maintenance costs is required improvement using personnel with high technical skills.

CHAPTER 10. DISCUSSION

10.1 Introduction

The essence of utilizing modelling risks in assessing the integrity of human assets eliminates the going concern for a corporate organization conducting business in the United Arab Emirates (UAE). Since the quality of products relates to competitive advantage, incorporating the use of life-cycle costing (LCC) helps to reduce fixed overheads. Similarly, the provision of physical security for high-value retailers due to the presence of high-value demand necessitates quality human capital that creates value. As such, a business manager must use knowledge of modelling risks, political skills on the UAE and cost-effective measures including Public Private Partnership mechanisms (3P) used for efficient development of capital. High-value retailer markets include the construction industries, real estate segment, and the rising demand for consumer electronics. As such, an organization whole life cycle approach (WLCC) in the operational and production process effects on minimizing costs while improving the individual productivity of employees. Regarding management and distribution of resources, inferences from Public-Private Partnership mechanisms (3P) assists in decision making since incorporating the civil and formal statutes of the UAE may present challenges and inherent opportunities.

This chapter discusses the results of this study. Prior studies that have noted the importance of the investigation of the cost variables included in the physical security systems and to establish a model that can be used to estimate the whole life cycle cost considering the risk integrated analysis. In this study, the UAE market was used as a reference for the data collection and analysis.

10.2 Discussion of Findings from the Literature Review

This study is set to answer the two literature review questions and problems. The first question is:

- *What are the risk issues that associated with PSA WLCC?*

The associated risks have been extracted and documented from literature are illustrated in the following figure, and discussed in the subsequent sections:

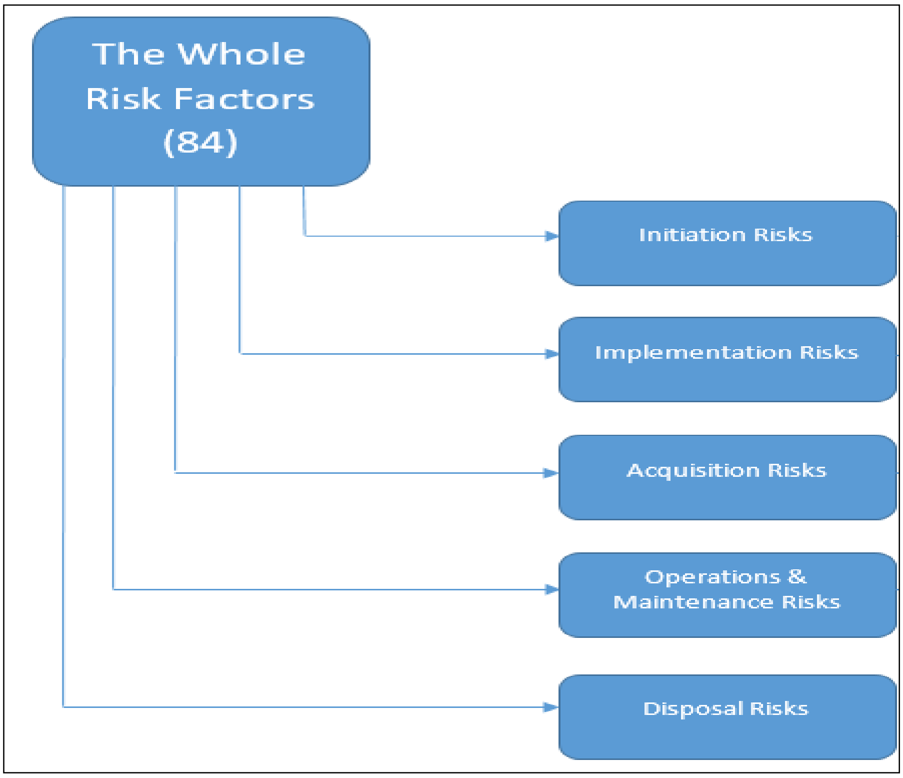


Figure 10-1: New Risk clusters

➢ Initiation Risks

An initial objective of the project was to extracted 34 initial risks from different sources and included them in the questionnaire. According to the literature review, this is composed initially of incorrect spending estimation that stems from inaccurate judgments and ideas about the prices of gadgets and other apparatus. The project scope extension may also cause additional costs to be borne. A critical part of the initiation risks is the incapacity or inability of the entity to understand the dynamics of the matters at stake.

As identified and mentioned in the literature review by Fennelly (2012), this is the most critical stage regarding costs. The Questionnaire validated the earlier findings in the field that lack of proper communication between the stakeholders regarding the requirements was the main risk drivers and concern for the respondents, regarding initiation risks. Respondents also indentified wrong estimation of costs as one of the main risk factor at this stage. Bad planning may cause cost overruns. Moreover, change in technology may render equipment obsolete. In cases where the specifications are not defined and articulated well, issues are very likely to arise later on. Unrealistic expectations from the system, and over-reliance would also cause harm. Schedule imperfections would also causedelays and cost overruns for the whole process. Unanticipated increases in prices of the apparatus and other equipment would also lead to cost over-runs. The classification of risks in this category is one of the contributions of this study.

- Implementation Risks

The literature review helped identify eighteen different risks that were included in the questionnaire for implementation risks. The respondents to the questionnaire pinpointed changing priorities amongst the various stakeholders as the main risk at the implementation stage. These findings align with those of Hastings (2010). Moreover, inaccurate time estimation regarding phases of the process may delay completion. In cases where the operators are not fully conversant with the technicalities and functionalities of the apparatus, implementation risks will increase. This will be very relevant in cases where specialists have not been commissioned to work on the phases. As in the case with initiation risk, unexpected scope developments would further increase the risks of implementation. Staff turnover represents an additional risk, as the replacement may be costly in terms of the training and development needs, as they may not be trained to operate, or experienced for the same. Ranging from planning, operationalization, staff issues, and others regarding resources, a whole ambit of implementation was covered in the questionnaire.

- Acquisition Risks

Fourteen types of acquisition risks were included in the questionnaire, upon detailed review of literature. When acquiring the physical resources, the organization may neglect certain dimensions initially considered and agreed upon, in cases the details are not tracked diligently. McDougall and Woodruff (2016) asserted damage to equipment upon conveyance and other harms being the chief risk elements, However, the findings were a bit different from this. According to the respondents to the questionnaire, the main risk at this stage is the mismatch and the lack of proper integration between the new equipment and software with the existing one at the sites. Necessities may evolve, providing additional requirements to be provided for. In cases where the organization runs out of storage space, or when the government makes some regulatory changes necessitating required amendments in the physical resources to be obtained, the additional costs may be very significant. As organizations change with time, the evolving needs may render the existing needs and possession redundant. Market improvement, leading to a different environment within which an entity operates may present it with additional dimensions of risk. Moreover, the new equipment may not integrate seamlessly with the existing.

- Operational and Maintenance Risks

Risks arising from technical hazards are present due to continual innovations and need for upgrading. The Questionnaire catered for fourteen types of operations and maintenance risks. The findings show evidence that the most critical risk at this stage is of the inability to get timely and efficient replacement of spare parts for the CCTV apparatus. This relates to the evidence as gathered in earlier research by Kincaid (2013). In cases where the differences in the needs between relevant parties is not resolved adequately, issues ware more than likely to crop up later. Similarly, these risks also extend to task duties where there is alwaysscope for misunderstanding and miscommunication. The assets being deployed may simply turn out to be inadequate in meeting the objectives. A lack of preparation of staff for operating and maintaining the systems will render the company liable to extra risks.

- Disposition Risks

The literature review identified thirteen types of disposition risks that were then included in the questionnaire. Health and safety risks would emanate due to sub-par or obsolete physical resources, and even inadequate staff training. The findings from the questionnaire corroborate that health and safety risks rank first at the disposition stage, as the respondents identified lack of technical knowledge regarding precautions and the sequence of disposition routines to be followed. This thus aligns with the research of Straub and Welke (1998), which found that the necessary technical support and direction from managers regarding disposition presented the main risk. The assets might depreciate at a much faster pace than anticipated and therefore their salvage prices may be significantly below that expected. This is most likely to be the case when technological change in the industry is rapid. Moreover, outdated and compromised apparatus would defeat the purpose of its installation.

Also, this study is set to answer the second question which is:

- *What are the mathematical techniques used by scholars and practitioners in performing PSA WLCC?*

In the performance of PSA WLCC, the author reviewed all the existing techniques as demonstrated in Chapter 3. The Monte Carlo used as pre define the parameters. This study included a detailed review of the existing WLCC techniques currently implemented in the UK and other European countries. The author found that deterministic models are inadequate in taking into consideration the variability of CAPEX and OPEX due to risks. To address this problem, the author proposed to use stochastic models to integrate WLCC computation with risk estimation as demonstrated in Chapter 7. @RISK' platform was used to address this, being is a complex scientific displaying programs that utilizations Monte Carlo reproduction to exhibit conceivable results, and in this way the related probabilities of various results (Palisade, 2016).

Moreover, the concept of physical security in the organization was also examined. There are many security assets in physical security projects in the UAE industry; however, the categorization of the assets into different components there was no clear which was a critical indication of the need for the research. CCTV cameras we re-examined in this study in physical security projects in the UAE. Furthermore, interviews and an online survey were conducted with experts working in the physical security projects industry in the UAE. Based on the data collected from different projects,evidence was found that there is a commonly agreedunderstanding regarding the categorization of physical security components in the UAE.

10.3 *Discussion of Findings from the Questionnaire*

- What are the most important risks in PSA WLCC?

To identify the most important risks in the PSA WLCC, the research used a questionnaire to estimate the likelihood and impact of PSA risks. The results were analyzed both in terms of the number of responses on the itemized scale, and the content of the answers on the questionnaire. A total of 100 questionnaires were distributed to 100 different organizations, and 68 employees responded.

The current study found that:

- The majority of respondents (62%) were employed in the private sector.
- The questionnaire was distributed to different levels in the organizations, such as the tactical and operational levels, to ensure the integrity and consistency of the results.
- The majority of respondents (77%) have more than 9 years of experience and their contribution thus enhanced the quality of the responses.
- The majority of respondents (86%) have worked on projects with revenues of more than 5 million AED.

In this study, there are distinct phases of the calculation of the risk factors in the life cycle of PSAs such as CCTV cameras. Furthermore, there are an initiation, implementation, acquisition, operation and maintenance, and disposal risk factors. Initially, there were 84 risk factors across the different risk categories. Component Factor Analysis (CFA) was used to reduce the number of variables. This yielded a total of 23 variables. The study used a probability/ impact risk-rating matrix. Each risk result was rated on its probability of occurring, and impact on an objective if it did occur.

The results of this study show that required use of descriptive statistical analysis techniques to create a regression model that is able can estimate the impact of the causes of variations. The findings revealed mean and standard deviation tests exhibited significant differences, and the calculation of the kurtosis and skewness of each risk factor required the use of a probability/impact risk rating matrix. In high uncertainty, kurtosis is a high, positive number with a high level of significance, and the tail is much broader than the normal distribution. In contrast, the low uncertainty kurtosis is also significant but negative, meaning that the tail is thinner than the normal distribution.

Another important finding was that, skewness, if it is a strong negative number and highly significant in high uncertainty, shows that in this regime there is a much higher likelihood of a large negative return than a positive one. Conversely, in low uncertainty, skewness is close to zero and insignificant, reflecting a more symmetric distribution. Together, the graphical evidence and the conditional statistics show that tail risk for the so-called ‘risk-on’ assets is largely concentrated in periods of high uncertainty.

The most interesting finding was thatall the risk factors have positive skewness except for a few factors with negative results. In the initiation risk category alone, there are four negative risk factors (Ri1=wrong budget estimation, Ri2=cost overruns due to change of scope, Ri7= gold plating, Ri11= unknown stakeholders). Evidence was also found that the implementation risk category contains one negative risk factor (Rm2=wrong timeframe estimation).Finally, the operations and maintenance risk category also include one negative risk factor (Ro1= poor policy performance for monitoring the system).

Next, a correlation matrix was calculated to check the pattern of relationships. To validate the results, the KMO test was used and the data value was calculated as 0.631, which falls into the range of being mediocre. Therefore, there was adequate evidence to lead the author to be confident that the factor analysis is appropriate for these data. A factor rotating analysis was performed and the number of 23 variables was reduced to three component groups.

10.4 *Discussion of findings from Simulation Modelling*

This research has set to answer the following PSA WLCC modelling question.

- What are the best theoretical probability distributions that can represent PSA risks, OPEX and CAPEX?

To answer this question the research developed an analysis framework as shown in figures (chapter 9 & 10). Also, the author used best fit metrics (Anderson test) for selecting the best probabilities.

To find the best theoretical distribution that fit the risk factor that influences PSA development and operation was the first step. To achieve the best fit, software was used. The following were the findings regarding the identified theoretical probability distribution from using the best fit software, according to Table 10-1:

Risk Factors	Identified theoretical Probability Distribution	Contribution and Possible usage
RIOS	Burr (4P)	To deal with modeling income.
RIM	Gen. Logistic	Modelling the risk of decompression sickness (DeS) space (Kannan et al., 1998)
RICP	Johnson SB	To deal with variables constrained by extremes.
RMCM	Gen. Extreme	To model the minimum or maximum value among a large set of independent.
RMSR	Burr	To deal with modeling income
RMSPI	Burr	To deal with modeling income
RAFI	Burr	To deal with modeling income
RACI	Wakey	
RASP	Burr	To deal with modeling income
ROST	Gen. Logistic	Modelling the risk of decompression sickness (DeS) space (Kannan et al., 1998)
ROO	Hypersecant	
ROSY	Wakeby	

Table 10-1 Summary of probability distribution for risk factors

The second step is to find the best theoretical distribution that fit the CAPEX and OPEX cost items. To achieve this too, the best fit software was used

Table 10-2 shows the theoretical probability distribution for the cost factors.

Cost Factors	Theoretical Probability Distribution	Contribution and Possible usage
Camera Cost	Gen. Logistic	Modelling the risk of decompression sickness (DeS) space (Kannan et al., 1998)
Switches	Johnson SB	To deal with variables

Cost		constrained by extremes.
Servers Cost	Johnson SB	To deal with variables constrained by extremes.
Software Cost	Johnson SB	To deal with variables constrained by extremes.
Monitors Cost	Johnson SB	To deal with variables constrained by extremes.
Storage Cost	Johnson SB	To deal with variables constrained by extremes.
Control room	Gen. Logistic	Modelling the risk of decompression sickness (DeS) space (Kannan et al., 1998)
Transmission cost	Gen. Logistic	Modelling the risk of decompression sickness (DeS) space (Kannan et al., 1998)
Layout cost	Gen Extreme Value	To model the minimum or maximum value among a large set of independent.
Manpower cost	Gen. Logistic	Modelling the risk of decompression sickness (DeS) space (Kannan et al., 1998)
Power supply cost	Johnson SB	To deal with variables constrained by extremes.

Table 10-2 shows the theoretical probability distribution for the cost factors.

Following the statistical analysis of the different risk factors, the LCC models were developed with different categories considering the cost of each phase of the project. The collected data were formed with the adjustment of the present value of each category including the risk and cost factors.

Chapter 9 developed a methodology based on MC simulation techniques to capture the variability and uncertainty that may exist in the variation of the annual present values over a period. In this study, the period was 10 years. Subjectivity and uncertainty were present throughout the analysis, and management of causes of variations in physical security projects. MC simulation was shown to be a typical methodology to capture and construct the probability distribution of annual present values. This simulationallows the use of probability distributions in the management of causes of various mitigation strategies.

Subsequently, a present value calculation for each year was presented, and a sensitivity analysis was conducted for the evaluation of risks and uncertainty.

The findings showed that the two parameters that influenced the data the most were the maintenance costs and the discount rate. Thus, a critical finding is that the proposed LCC model correctly follows the variation of the discount rate and for the maintenance costs, and is an improvement using personnel with high technical skills. Furthermore, the sensitivity analysis was deployed, aimed to examine the effect of the variability of the main input parameters, which assisted in evaluating the data. Tesfamariam and Sanchez-Silva (2011) used a sensitivity analysis to measure the effect of various building performance on LCC.

The findings revealed that construction quality had the most impact on LCC. Another interesting finding was that plan irregularity had the lowest impact. Sensitivity analysis measures the impact on life-cycle cost project outcomes of changing key input values, which causes uncertainty. These key input values are typical:

- Discount rate
- Future inflation assumptions
- Period of analysis
- Maintenance, replacement, and operational cost data

Following to present value (PV) method, a sensitivity analysis was used to predict what the most sensitive variable is if it changes. The following uncertainty variables were examined:

- The effect of maintenance costs in the LCC CCTV solution
- The variation of the discount rate

The sensitivity analysis compared the total LCC to the LCC without the maintenance cost (see Chapter 9). An interesting finding was that not performing any maintenance activity induces a decrease of 52% in the NPV of the LLC model solution, which proves that maintenance activities during the life cycle are high, but are necessary to ensure the personnel's correct usage. This finding validates the necessity of maintenance activities during the life of a PSA. The personnel require technical skills and experience to use CCTV security components such as cameras and IT systems.

To verify the effect of the discount rate in this study, calculations were made for a discount rate of 2%. The sensitivity analysis compared the LCC and PV total cost between two discount rates: 5% and 2%. The results are presented in Chapter 9. For a discount rate of 2%, the LCC model showed higher LCC than for a discount rate of 5%. Thus, a main finding is that the model LCC follows correctly that indeed through increasing the discount rate, it decreases the present value (PV).

In Chapter 10, the author developed a methodology based on Monte Carlo simulation and @risk program based on MC to capture variability and uncertainty that may exist in variation constructs, techniques to capture the variability and uncertainty which may exist in the variation constructs. Subjectivity and uncertainty are present throughout the analysis and management of causes of variations in construction projects. These characteristics are present in the identification, prioritisation, costing, and mitigation of causes. The literature review has shown that there has been a lack of research to map causes of gaps between the cost and the risk, and MC simulation was suggested to capture the variations to their potential cost impact. Monte Carlo simulation was suggested to be a typical methodology to capture and construct the probability distribution of both causes of variation constructs and their associated cost impact. This will allow the use of probability distributions in the management of causes of variation mitigation strategies.

The findings obtained from the conducted Monte Carlo simulation were discussed in detail in Chapter 10, and the selected best-fitted probability distributions for the input variables (causes of variation) and output (cost overrun due to variation) were tested and validated using several statistical techniques. Chapter 10 illustrated the results of the simulation and the goodness-of-fit outcomes for the selected output distributions.

The findings of the simulation showed that the duration overrun percentage is best fitted to a Weibull distribution. As demonstrated in the results analysis, all theoretical probability distribution is accepted at all alpha levels. Hence, there is no reason to believe, based on this evidence and tests that the selected distribution does not provide a good fit for duration overrun within the limits of the data and context of this research. This is further evidence to validate and corroborate the claim that the developed regression model produces results that are similar to real cases. The simulation results have also demonstrated that the mean forecasted overrun duration revolves around the +/- 1 Std Dev certainty band. None of the input variables were found to be significant when the duration overrun is at or below their 25th percentile values in their probability distributions.

10.5 Discussion of research implications

This research has set out to answer the following implication question:

- Does the established WLCC framework lead to effective and efficient risk management for UAE PSA investments?

10.5.1 Analysis and Risk Modelling

Risk management of large retailer projects in the United Arab Emirates involves two necessary procedures, risk analysis and monitoring of risks of assets such as human capital, building, and logistical resources. First, human capital in the giant retailer projects possess quality skills, and the magnitude and nature cost of providing health care insurance to employees has gone up by more than 59% within a period of less than a decade. Due to this increase, organizations engaging with giant retailer projects are cautious in implementing health insurance covers since they come with added costs. Moreover, the use of Whole Life-Cycle Costing (WLCC) to reduce the increase in the prices does not reflect improvement of services offered by the service providers. In the results, a noteworthy population of the staff is not insured and must depend on individual and private assurance protection generating a risk on human capital in the operation and production procedures. A different research study by McCall, Rice, & Sangl (1986) explains that insurance policymakers overestimate the nature of services they receive, resulting in a financial risk, thereby threatening the going concern. Employees take individual health insurance cover believing that it includes physician and hospitalization costs, while the policies only include consultation fees (Berry et al., 2010, pp. 68).

Secondly, risk modelling the adoption of strategic information systems factors nature of costs since the price of products relates to consumer loyalty and ability to make a second purchase. In organizational and at corporate level within the United Arab Emirates, the use of strategic information systems leads to obtaining a competitive advantage. At the operational level, vital information systems improve on service delivery systems while strengthening labour productivity. On the financial side, strategic information systems facilitate the reduction of cost overheads and maximization of the utility of raw materials that is the fundamental principle of Whole Life-Cycle Costing (WLCC). In terms of organizational culture, strategic information systems foster productive interactions, and civilization, ethics assist in ensuring individuals and groups respect each other. The social structure is both sophisticated and dynamic in that conflicts arise and disappear based on how we approach them. In organized social structures such as companies and organizations, use of strategic information systems is mandatory as it ensures professionally conducting business and operations. This paper, therefore, describes in detail the importance of maintaining ethical standards and behavior within an organization.

10.5.2 The role of development and management of physical safety assets.

According to Stevenson, & Sum (2002), under operational capability facilitates the creation of value from resources such as human capital, production equipment, and available technologies is possible. For instance, in the case of planning and managing physical security resources, the integration of the current resources is challenging due to departing of essential managers and personnel affecting measures for continual production and delivery of high retailer products and services. The departure of leading competitors in manufacturing within the United Arab Emirates indicates a deficit of experienced managers who have the technical knowledge and skill to fast-track the production process and mitigating financial losses. Furthermore, their departure suggests challenges in operations management regarding planning and forecasting of increases in consumer demands. Studies conducted by Voss, Tsikriktsis, & Frohlich (2002) inform that organizations with consistent and definitive operations management achieve their goals and objectives efficiently compared to groups without. This translates to having an operations manager who has the capability to integrate several factors of production together. Effective integration and collaboration between departments or various levels within an organization lead to raising the standards of effectiveness thereby resulting in higher performance and profits, (Voss, Tsikriktsis, & Frohlich (2002).

10.5.3 Impact on organizational culture.

Leading studies and research conducted by Stevenson, & Sum (2002) argue that the nature of operations' management in a firm correlates positively with the overall status of an organization. In the initial development of high-value retailer projects, the United Arab Emirates initiated a plan to build a massive hospitality industry that would facilitate diversification from the oil industry. Initial estimates projected annual hospitality to employ a minimum of 500000 human capital opportunities in the next ten years. In the first year of job creation in most PPP sectors, a number of units added to less than 47821 manifesting logistical and production failures revealing a rationale for incorporating planning and managing physical security resources with a whole life cycle approach (WLCC). Since there were prior hospitality bookings by their consumers, this portrayed a negative image due to the erosion of consumer confidence and trust. Inability to deliver on its pledges gave the competitive advantage to competitors.

Major corporations in consumer electronics and automobile in the United Arab Emirates rely on product quality to gain a competitive advantage over rivals and other competitors in the giant retailer projects including the construction industry. Production of superior products is an active business lever regarding profit margins necessitates observance of costs and planning managing physical security resources. Weathering of consumer confidence due to operational challenges that planning and executing physical security resources strive to reduce. Reduced consumer traffic and several online demands of consumer electronics pose challenges to the number of construction units sold due to high costs in the procurement of raw materials, transportation and in a meeting of fixed overheads translating to fewer revenues. Consequently, meeting of deadlines is challenging and retaining of employees is not possible since they shift to organizations posting positive results.

10.6 *Objectives of planning and managing physical security resources.*

10.6.1 Quality Goods and Services.

In studies done by Voss, Tsikriktsis, & Frohlich (2002), companies that have efficient operations management produce quality goods and services that are always appraised by their customers. Streamlined operations and activities of any business need to be streamlined and implemented in a manner that increases performance positively thus, improving the quality of goods and services provided. This translates to dedicated employees and staff who are well motivated and remunerated through staff performance appraisal and payment of reasonable wages. In the case of United Arab Emirates, operations management would ensure excellent and standard quality rationale in planning and manage physical security resources.

10.6.2 Quality Performance Speeds.

Secondly, conducting market research in the process of planning and managing physical security resources increases the speed of production and implementation of projects due to the use of quality and reliable information. The performance of tasks takes the least time possible due to established structures that facilitate not hindrances. Research conducted by Manzoor (2012) indicated that organizations that optimize supply chains and logistics meet the deadlines and demands of consumers. This could be crucial to the United Arab Emirates as improving the speed of performance would relate positively to the number of units manufactured per year in the hospitality industry hence increasing the Gross Domestic Product (GDP). Since the United Arab Emirates sells diversified products in the consumer industry for big retailers, high production speed ensures meeting of deadlines while preserving on product quality. Given these operational demands, Speed regarding customer care delivery provides there are no backlogs at work and prompt action on all customer feedback.

10.6.3 Dependability and Reliability.

Dependability is the crucial third component of planning and managing physical security resources. This arises from the customers need to have deliveries on time. To explain details, consumers of dominant products maintain brand loyalty due to the reliability of the producers to provide services according to the terms of trade and agreement. Delivery of construction materials and hospitality units on time would build trust and confidence with consumers. This would in turn influence award and extension of contracts hence eliminating the going concern. Internal benefits of dependability to a firm includes saving on cost and time. Keeping on time would give room for improving company efficiency, and staff morale.Flexibility is the fourth direct benefit of having careful planning of physical security resources. According to Manzoor (2012, flexibility regarding the development of a WLCC results in cost reduction in the process of creation and innovation of a variety of product and services. Having additional time and finances due to improved dependability and performance allows organizations within the UAE to allocate the extra resources to innovating and creating new products. This is so since the consumer electronics and construction industry have unlimited potential that is yet to be exploited. Organizations through their popularly priced giant retailer products and services are a manifestation of the company's desire to offer their client base a variety of models. Offering a range of standard and quality big retailer products and services is a competitive advantage since consumers tend to choose brands and products from a well-known supplier.

10.6.4 Identifying vulnerabilities in the Production and Service Systems.

Over the last decade, development of robots and automatic assembly lines facilitate mass production and ensuring that products are up to international standards. Production systems consist of computer programs and software that aid the production process by being able to automate planning and scheduling of events and activities. Used by dominant industries manufacturing brands, production systems facilitate the reduction of wastages, correcting inefficiencies and matching available resources to consumer demands and preferences. According to Baines, Lightfoot, Evans, Neely, Greenough, Peppard, & Alcock (2007), the ability of production systems to eliminate wastages arises from the creation of continuous processes in production and allocation of resources leading to increased costs primarily in research and development projects. In the case of organizations dealing with high retailer products and services, the focus is providing security and welfare resources for the use of human capital. In this case, production systems check the available inventories regarding resources necessary for the production and delivery of consumer electronics and other high-value retailer products and services. Checking of the stocks constitutes matching of funds with the level and nature of consumer demands and ensuring that at any given time, the available stock is enough to satisfy the customer demand. If for instance, the product systems software or program detects insufficient resources, production systems robots and automated services reduce the production rate giving the company and staff time to acquire additional resources. Interesting to note that the systems have programmed authority to delay or stop production to allow fixing of broken assembly lines or attend to an injured employee (Baines, Lightfoot, Evans, Neely, Greenough, Peppard, & Alcock (2007).

10.7 *Impact of life-cycle costing (LCC) on Goal Setting.*

Due to the high costs, an organization faces challenges in health care benefit budgets. Since agencies consider health benefits and insurance costs of their staff, their implementation relies on the benefits derived. Folland, Goodman, & Stano (2007), explain that in the provision of laboratory services, organizations utilize life-cycle costing (LCC) in estimation, and prefer to outsource to save costs. Several agencies merge efforts to create funds for a collective medical and benefits project. Use of computer connected infrastructure in a laboratory and ambulance services reduce costs by over $8.09 billion nationally at level 2 hospitals. Moreover, it becomes efficient to serve many employees while reducing time and number of personnel (Folland, Goodman, & Stano, 2007).

Organizational expenses require cautious contemplation since they constitute an ample fraction of the organization’s yearly budget. The World Health Organization (2010) says that the administrative expenses of agencies and private entities exceed tax health care systems getting their funding from though taxation. In the short term, it becomes expensive for organizations to provide employee health benefits and packages since the initial costs weigh health on a budget. Long-term financing of health packages allows a firm to plan to avoid a financial crisis within an organization. Tax-funded insurance projects and initiatives such as the affordable care act offer subsidy, and cheaper policies to the population compared to tailor-made efforts by organizations. This makes tax subsidies a significant contributor to high premiums for workers making them seek alternatives (World Health Organization, 2010).

10.7.1 Placing Control of Health Benefits Costs.

Due to the returns on the cost and time, specific uncertainty jurisdictions, including the UAE enforce laws targeting employers forcing them to provide medical schemes that facilitate insurance to their employees to make their lives easier and reduce their expenses. The UAE, for instance, a bill failed to pass a vote that would otherwise make it mandatory for employers with over 20 employees to subscribe to a health insurance policy (Baicker, & Chandra, 2005). This study shows that employers make most of the decisions. However, industry rules and company costs play a critical role in organizations' decisions to control the size and scope of the expenses.

Wellness and commitment from the organization and employees are crucial in placing control. Wellness arises from the motivation of engaging in practices that reduce employee stresses and safety threats. Having a friendly working environment is the first step in ensuring employees feels appreciated and motivate them to even work harder and smarter towards achieving the companies' goals. Offering employees incentives to avoid harmful habits and behaviour helps to reduce instances of ill health. Berry, Mirabito, & Baun (2010), backs this claim arguing that implementing a health insurance policy with the aim of growing and developing an employee,secures support and a quick adoption rate. For this reason, an employer needs to explain to his employees the magnitude of health benefit costs and why it justifies maintaining the expenses as a low percentage of the firm's revenues.

10.7.2 Health Benefits Packages as Employee Recruitment and Retention Tools

According to Figueras, Saltman, Busse & Dubois (2004), future job seekers consider the nature of health benefits 'packages offered by firms. The same studies show that an organization with the best packages especially those that cover employees' families tend to have preferential treatment. Other research affirms this claim by stating that employees consider organizations with health care funds. This is an informed choice, since any employees of such firms acquire automatic health insurance covers (Figueras, Saltman, Busse & Dubois, 2004).

Globalization of operations product

The first business strategy is the globalization of operations products as organization culture seeks to expand the nature and variety of goods and services. Entry into the consumer electronics production and distribution market attempts to exert influence on consumer trends across the globe while providing quality goods (Walker, Pan, Johnston, & Adler-Milstein, 2005). With plans to expand human capital regarding qualification and skills, organizations can dominate international trade by moving operation on strategic position across the globe.

Reduction of employees

Secondly, an organization's business strategy is the reduction of employees based on performance and product evaluation. Elimination of departmental redundancies such ghost workers would reflect the removal of fixed costs (Walker, Pan, Johnston, & Adler-Milstein, 2005). Costs of maintaining welfare costs for non-productive employees leads to the reduction of synergies, while leading to wastage of additional resources within the various departments in an organization. The role and interaction of business strategy with human resource strategy at the successful agency in the United Arab Emirates are an integration of human capital and other factors relevant to the success of the business. For instance, organization culture relies on the employee to maintain a positive interface with potential consumers. This means that the business strategy of organizations is having good relations and goodwill with likely consumers while the human resource strategy helps to facilitate the real interface.

10.7.3 Enterprise Resource Planning in high-value retailer projects

The organizational culture of organizations seeking to obtain competitive advantage calls on employees to maintain high levels of financial integrity. The use of Enterprise Resource Planning (ERP) for efficient allocation of resources and documentation challenges employee is without technical abilities. Secondly, the organizational culture at relies on Strategic Human Resource Management to monitor and remunerate employee productivity. This use of Strategic Information Systems to manage employees has inherent challenges since the application of scientific principles in managing employees leads to operational deficiencies (Berry, Mirabito, & Baun (2010). Thirdly, the organizational culture improves by way of having a unique set of behaviours and identifiable habits such as compartmentalization of information systems, which has the effect of limiting the flow of information making it difficult to meet organizational objectives. These patterns of behaviour exhibit in an organization's activities and internal structures in various departments. This includes areas such as safety of employees, technological state, how transparency within an organization and working conditions in a group. With such issues in mind, ERP guides organizations in engaging in value-adding activities and initiatives.

10.7.4 Optimum approaches for PSA WLCC analysis.

It becomes easier to relate data with the use of correlation analysis, regression elements, and descriptive statistics to explain the nature of costs by observing the large sets of data in the segment 'generalized method of moments'. Descriptive statistics factor on observable traits such as rate of depreciation and factor affecting the ability of employees to utilize or operate PSA effectively. This is because human errors and redundancies affect the ability to derive utility from PSA.

Correlation analysis explains factors, which are unavoidable, that leads to additional costs or reduction of costs and this data is captured under the 'generalized method of moments' that uses view statistical techniques. Regression elements explain the rationale used to analyze huge sets of data related to PSA and the results appear in the 'generalized method of moments.'

Mathematical techniques used by scholars and practitioners in performing PSA WLCC

This segment uses view analysis, which interprets data explaining the change in prices, costs, and nature of demand due to having varying characteristics and attributes of PSA. For instance, a coefficient of 124.0214 explains the degree of change of demand in high value markets due to changes in prices of PSA. Physical security assets and computer systems. The integration of PSA and computer systems since development and use of technologies leads to improved security and operations of PSA. This segment explains threats to PSA with computer systems such as autonomous control abilities.

10.8 Summary

This chapter encapsulated the overall conclusions, limitations, and implications of the research findings. It began by discussing the literature review findings, followed by the survey results. The results were compared with the current literature to identify the similarities and disparities. Then, the findings from the MC simulation and modeling process for the annual present values (PV) in the LCC model were examined.

It was found that there is a match between the findings from the literature and the present study for the main risk factors of variation, as they originate from five main groups, namely owner/stakeholder, contractor/project system/product issues, staffing, and operation issues. Each of these five groups is the initiation of unknown numbers of various causes. This chapter discussed the influence of these causes on project success criteria in terms of cost, time, quality, and scope according to the respondents. Ultimately, the development of an LCC model enables subject matter experts to identify the risks and the costs of the physical security CCTV cameras that are designed for security projects in the UAE.

CHAPTER 11. CONCLUSION

11.1 Introduction

This chapter concludes the study. The research methodology is defended and propounded in the first section, followed by a discussion of the research objectives presented at the beginning of the thesis. The research limitations are then identified, and the final section subsequently focuses on the contributions to knowledge and suggestions for further research.

11.2 Research Methodology Robustness

A modeling method type of research was conducted. It helped to identify the gaps in the existing research and to articulate and refine the research questions. An extensive literature review was also conducted, covering WLCC techniques employed in the UK, and other European countries, with a special emphasis on PSAs.

A fully referenced questionnaire was developed and used to collect primary research data. The list of questions was classified and clustered according to the source of variations. The questionnaire was distributed to 10 different organizations based on their use of PSAs such as CCTV and other related equipment. In addition, the researcher conducted interviews with local UAE specialises in the use of PSAs, and conducted an online survey. The results showed general agreement in understanding regarding the categorization of PSA components in the UAE.

A significant number of positive responses were received from the potential respondents approached - 68 out of 100. The received data was checked for errors, completeness, and consistency. Incomplete or unanswered questionnaires were excluded from the analysis. Software analysis techniques including SPSS and Easy fit were used to analyze the data. Statistical techniques were applied to the data, including regression analysis modeling to estimate the impact of variations.

A list of the cost of equipment made by the researcher and approved by two companies and the consultancy office at Abu Dhabi Police. The Price used in this thesis was AED per square ft. The area it been considered to protract 25 km sq. ft. i.e. Yas mall project.

An LCC model was developed, taking into consideration the risk and cost factors involved. The easy fit software was used to assess the validity and the statistical significance of the proposed model. The results of the simulations and goodness-for-fit outcomes for the selected output distributions were used for risk and other cost analyses. The results showed best fit to different theoretical probability distributions. To determine the regression significance, a standard error-R2, probability-probability plot, and Q-Q were used to assess the adequacy of the proposed model. The model was also validated for unseen data. Similar standard fitness measures, such as the Anderson-Darling fitting test, were used to assess the probability distribution of both the input cause of various variables and the output from the simulation model. The approaches taken in this study are deemed to be suitable given the unique characteristics of the research framework developed during this investigation.

11.3 Accomplishing the Objectives

<u>Objective 1:</u> To provide the users with a stochastic process to simulate costs deploying continuous probability distribution if the data relating actual costs are not available.

This objective was achieved using the answers to the questionnaire from 10 different organizations. From the results, the cost and risk factors were identified. Initially, there were 84 risk factors, but using CFA this was reduced to 23 variables. These risk factors of variation were extracted and described in detail in Chapter 7.

In accomplishing this objective this study has reached the following conclusions:

- Risk impact estimation should be based on probability independent events
- The majority of PSA risk impact estimates, by the experts, were normally distributed
- The study has identified five new PSA risks clutters -: Ri, Rm, Ro, Ra, Rd.

<u>Objective 2</u>: To enable users to calculate WLCC of PSA investments by using probabilistic methods using stochastic techniques.

This objective was met assuming that the development of a WLCC model is based on risk and cost factors for specific PSAs such as CCTV cameras. One of the main advancements in knowledge provided by this study is the development of a probabilistic model to assess the impact of the risk and cost factors during the WLCC period of security projects in the UAE. This objective was achieved through the development of a WLCC model based on multiple regressions (including SPSS software). The achievement of this objective is presented in Chapter 7.

In accomplishing this objective this study has reached the following conclusions:

- PSA risks were mainly fitted to Burr theoretical probability distribution. These types of distributions are most commonly used to income modelling.
- The CAPEX costs were fitted to ExtValueMin distribution
- The Opex costs were fitted to Logistic distribution
- The WLCC cost was fitted to Weibull distribution
- PSA WLCC cost was found to be sensitive to camera cost and Roo (Risk of operation)
- PSA total PV cost was fitted to Weibull distribution

<u>Objective 3</u>: To incorporate the parametric risk and WLCC model of the PSA through a stochastic process instead of a subjective procedure.

This research objective was achieved by developing a stochastic process for risk factors and the risk adjustments in the different WLCCs. The cost modelling developed by this work was driven by the research gaps identified in the literature review. This objective was achieved in Chapter 6 and 8. The model presents a relationship between annual recurring initial costs, operation costs, maintenance costs, and the risk adjustments between them. The benefit of cost modelling is that it assists security organizations in simulating the WLCC performance and maintaining the impact of variation at a minimum level that can be financially tolerated

In accomplishing this objective this study has reached the following conclusions:

- A large set of data is necessary to develop accurate input probability distributions for the stochastic model
- The risk estimation method is expert depended which include some sort of bias. Thus, real data for risk cost pricing is necessary
- WLCC is sensitive to the discount rate. Thus, selecting an optimum rate over the life cycle period, over 10 years, is a challenging prospect
- WLCC is sensitive to OPEX costs. Thus, accurate estimation of these costs is necessary.

__Objective 4__**: To make it possible to readily compare and evaluate the WLCC of various PSA investments.**

This research objective was achieved by developing a WLCC model based on MC simulation. This is presented in Chapter 9. MC simulation is used to capture the variability and uncertainty that may exist in the variation of the annual present values (PV) over a time period. In this study, the period was 10 years. The WLCC model serves as a vehicle to assess the impact of variation on the project performance.

Next, a present value calculation was applied for each year presented, and a sensitivity analysis was conducted to evaluate risks and uncertainty, as described in detail in chapter 9. The two parameters that could have influenced the data were maintenance costs and the discount rate. The proposed WLCC model correctly follows the variation of these parameters.

Furthermore, a sensitivity analysis was conducted to analyze the effect of the variability of the main input parameters, which assisted in evaluating the data. The results of the analysis show that construction quality has the most impact on LCC, while plan irregularity has the lowest impact. The sensitivity analysis measured the impact on LCC project outcomes of changing key input values about which there is uncertainty.

In accomplishing this objective this study has reached the following conclusions:

- Comparisons should be based on similar discount rates
- Inflation assumptions should be consistent between alternatives
- Period of analysis should be consistent between alternatives
- Due to the stochastic nature of the simulation process the WLLCC probability distribution might be different, thus it might difficult to compare the results. However, the mean and standard deviation can be used for comparison purposes.

11.4 *Contributions to Knowledge*

The contribution of this thesis to the research community is related to the in-depth exploration of its methodological stances. The thesis has demonstrated an LCC approach to the use of PSAs, and especially CCTV cameras. Furthermore, it employed various forms of verification to ensure data reliability. These included follow-up discussions after the interview sessions, confirmation of the case study report by participating organizations, and workshops to discuss the issues raised by the study. This all contributes to a deeper understanding of how these means of verification add reliability to the results of a research study.

In summary, the research contributes to formally estimating the impact of the risk and cost causes of variation in physical security construction projects using a combination of regression and MC simulation techniques. The key contributions of this investigation are the following:

- A model was developed to identify the highest ranked factors that impact the LCC of the PSA CCTV camera.
- Using the developed model, the study argued that the highest ranked factors had the highest impact on the risk and cost analysis.
- A probability distribution was developed and validated for the most important risk and cost factors.
- A multiple regression analysis was conducted to quantify the association between risk and cost factors and their impact based on 10 companies' results.

11.5 *Research Limitations*

The first limitation of this study for both PSAs and life cost cycle is the wide variety of subjects related to these topics. As the sector includes a plethora of subjects and specialisms, it was imperative that the true focus of the study remained intact while addressing the issues raised in a holistic manner. The remaining limitations are the following:

Firstly, the length of time available for the project and the resources available constrained the research to an extent, although iterations and persistent adaptations to the changing dynamics in order to evolve a suitable model mitigated this limitation considerably.

Next, some respondents to the questionnaire may not have understood the points, or exercised due care and diligence when answering the questions. This internal validity concern was mitigated by the researcher through spending considerable time and effort in drafting the questionnaire and painstakingly taking them through the various segments, explaining the components where needed.

Moreover, the ranking of causes of variation was based on data related to companies specializing in PSA, and not on specific projects utilizing these assets. However, the causes of variation were gathered from experts working in physical security projects in UAE, and this research will, therefore, be useful for many users.

Furthermore, he developed LCC model is based on specific risk and cost factors. The data was collected from projects in the UAE only. Additional exploration, including data from different GCC countries, is crucial for the LCC calculation. Hence this relates to external validity issue whereby the derived model may need adjustments to be deployed in different environments.

Finally, for research is needed to overcome these limitations. The next section details the study's contribution to knowledge, while the final section explores some possible areas for future development and research.

11.6 *Recommendations for Further Research*

The research conducted in this thesis provides a solid foundation to build on and to consolidate future research related to PSA LCC models. Several areas have been identified for future research in this field. This list excludes ongoing research identified throughout this study but includes:

- Evaluating other PSAs in the same way as was done in the present study. The model can be used as a benchmark to initiate and develop ideas for such work.
- Investigating the impact of the proposed LCC model not only in the UAE, but also in the rest of the GCC region can be carried out as follow-up research. Thus, there is a need to test whether the LCC model can be used within the same industry in other countries. This may lead to necessary adaptations in terms of risk prioritisation and management, as that would be reflective of different environmental aspects specific to those settings.
- Optimising the number of risk and cost factors in the regression model can be done through further focused work.
- Profiling the cost consequences of each of the risk factor causes in more detail and applications therefore to different scenarios and situations. Will provide extra details and complement the Model and research.

CHAPTER 12. REFERENCES

Abbott, J. (2002). Smart Cards: How Secure Are They? Retrieved from SANS Institute website: https://www.sans.org/reading-room/whitepapers/authentication/smart-cards-secure-they-131

Abu Dhabi Quality and Conformity Council (2017). Abu Dhabi Emirate Guideline for Infrastructure Service Standards, 2nd ed.

Alach, Z.J. (2007). Mapping the elements of physical security towards the creation of a holistic physical security model, Master's thesis, Edith Cowan University. Perth: WA.

Ali, S.M., 2014. Integration of Information Security Essential Controls into Information Technology Infrastructure Library–A Proposed Framework. *International Journal of Applied*, *4*(1).

Alshboul, A. (2010). Information systems security measures and countermeasures: Protecting organizational assets from malicious attacks. Communications of the IBIMA.

Audu, H.A.P., Aniekwu, A.N. and Oghorodje, E.E., 2015. Life Cycle Cost Analysis (LCCA) Delivery Model for an Urban Flexible Pavement. *Journal of Civil & Environmental Engineering, 2015*.

Bahr, N.J., 2014. *System safety engineering and risk assessment: a practical approach*. CRC Press.

Baicker, K., Chandra, A., 2005. The effect of Malpractice Liability on the delivery of Heath Care. *Forum for Health Economics & Policy, 8(4).*

Baines, T, Lightfoot, HW, Evans, S, Neely, A, Greenough, R, Peppard, J, Roy, R, Shehab, E, Braganza, A, Tiwari, A, Alcock, JR, Angus, JP, Bastl, M, Cousens, A, Irving, P, Johnson, M, Kingston, J, Lockett, H, Martinez, V, Michele, P, Tranfield, D, Walton, IM & Wilson, H 2007, 'State-of-the-art in product-service systems' *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture,* vol 221, no. 10, pp. 1543-1552.

Baker, P.R. and Benny, D.J., 2012. *The complete guide to physical security*. CRC Press.

Bakker, J.D., Helmer, J. and Schavemaker, J., 2014. Life-cycle cost management for newly constructed infrastructure. *Aquananotechnology: Global Prospects*, p.223.

Ballad, B., Ballad, T. & Banks, E. (2011). Access control, authentication, and public key infrastructure. Sudbury, MA: Jones & Bartlett Learning.

Bartholomew, D. Knott, M, Moustaki, I. 2011. *Latent Variable Models and Factor Analysis: A Unified Approach*, Wiley.

Basbagill, J., Flager, F., Lepech, M. and Fischer, M., 2013. Application of life-cycle assessment to early stage building design for reduced embodied environmental impacts. *Building and Environment*, *60*, pp.81-92.

Beckers, R., 2015. Safety Design for Containerised Battery Testing Laboratories. *ATZelektronik worldwide*, *10*(3), pp.38-42.

Bell, R.T., Kilcrease, C.L., Amar, A.C. and Dukes-Schlossberg, J.L., Cisco Technology, Inc., 2014. *Utilizing physically unclonable functions to derive device specific keying material for protection of information*. U.S. Patent 8,700,916.

Berry, A. S., Zanto, T.P., Clap, W.C., Hardy, J.L., Delahunt, P.B., MAhncke, H.W., Gazzaley, A., 2010, *The Influence of Perceptual Training on Working Memory in Older Adults.*

Biringer, B.B., Matalucci, R.V. & O'Connor, S.L. (2007). A professional practice guide for protecting buildings and infrastructures. New Jersey: Wiley & Sons, Inc.

Blengini, G.A., Garbarino, E., Šolar, S., Shields, D.J., Hámor, T., Vinai, R. and Agioutantis, Z., 2012. Life Cycle Assessment guidelines for the sustainable production and recycling of aggregates: the Sustainable Aggregates Resource Management project (SARMa). *Journal of Cleaner Production*, *27*, pp.177-181.

Boussabaine, A. and Kirkham, R., 2004. *Whole life-cycle costing: risk and risk responses*. John Wiley & Sons.

Boussabaine, A. and Kirkham, R., 2005. *Whole life-cycle costing: risk and risk responses*. John Wiley & Sons.

Boussabaine, A. and Kirkham, R., 2008. *Whole life-cycle costing: risk and risk responses*. John Wiley & Sons.

Bracco, S., Delfino, F., Pampararo, F., Robba, M. and Rossi, M., 2014. A mathematical model for the optimal operation of the University of Genoa Smart PolygenerationMicrogrid: Evaluation of technical, economic and environmental performance indicators. *Energy*, *64*, pp.912-922..

Brémaud, P., 2013. *Markov chains: Gibbs fields, Monte Carlo simulation, and queues* (Vol. 31). Springer Science & Business Media.

Brown, R.J., 1979. A new marketing tool: Life-cycle costing. *Industrial Marketing Management*, *8*(2), pp.109-113.

Cabeza, L.F., Rincón, L., Vilariño, V., Pérez, G. and Castell, A., 2014. Life cycle assessment (LCA) and life cycle energy analysis (LCEA) of buildings and the building sector: A review. *Renewable and Sustainable Energy Reviews*, *29*, pp.394-416.

Campbell, J.D., Jardine, A.K. and McGlynn, J. eds., 2016. *Asset management excellence: optimizing equipment life-cycle decisions*. CRC Press.

Caputo, A.C. (2014). Digital video surveillance and security, second edition. Oxford: Butterworth-Heinemann.

Catrinu, M. D., & Nordgård, D. E. (2011). Integrating risk analysis and multi-criteria decision support under uncertainty in electricity distribution system asset management. Reliability Engineering & System Safety, 96(6), 663-670.

Chen, H.T., Wu, S.W. and Hsieh, S.H., 2013. Visualization of CCTV coverage in public building space using BIM technology. *Visualization in Engineering*, *1*(1), p.1.

Cheng, P., Aerts, W. and Jorissen, A., 2010. Earnings management, asset restructuring, and the threat of exchange delisting in an earnings‐based regulatory regime. *Corporate governance: an international review*, *18*(5), pp.438-456.

Chung, T., 2014. Improvement of Physical security System Operation. *Journal of The Korean Society of Disaster Information*, *10*(2), pp.282-286.

Creswell, J.W., 2013. *Research Design*. Sage

Curran, M.A., 1996. Environmental life-cycle assessment. *The International Journal of Life Cycle Assessment*, *1*(3), pp.179-179.

Dadashi, N., Stedmon, A.W. and Pridmore, T.P., 2013. Semi-automated CCTV surveillance: The effects of system confidence, system accuracy and task complexity on operator vigilance, reliance and workload. *Applied ergonomics*, *44*(5), pp.730-738.

Dhillon, B., 2013. *Life cycle costing: techniques, models and applications*. Routledge.

Donald, F.M. and Donald, C.H., 2015. Task disengagement and implications for vigilance performance in CCTV surveillance. *Cognition, Technology & Work*, *17*(1), pp.121-130.

Durairaj, S.K., Ong, S.K., Nee, A.Y. and Tan, R.B., 2002. Evaluation of life cycle cost analysis methodologies. *Corporate Environmental Strategy*, *9*(1), pp.30-39.

Ekelhart, A., Fenz, S., Klemen, M. D., & Weippl, E. R. (2006). Security ontology: Simulating threats to corporate assets. In International Conference on Information Systems Security (pp. 249-259). Springer Berlin Heidelberg.

Emblemsvag, J., 2001. Activity-based life-cycle costing. *Managerial Auditing Journal*, *16*(1), pp.17-27.

Emblemsvåg, J., 2003. *Life-cycle costing: using activity-based costing and Monte Carlo methods to manage future costs and risks*. John wiley & sons.

Fay,J. J. (2007). Encyclopedia of security management, second edition. MA: Butterworth-Heinemann.

Fay,J. J. (2011). Contemporary security management, third edition. MA: Butterworth-Heinemann.

Fendrick, A.M., Smith, D.G., Chernew, M.E. and Shah, S.N., 2001. A benefit-based copay for prescription drugs: patient contribution based on total benefits, not drug acquisition cost. *American Journal of Managed Care*, *7*(9), pp.861-874.

Fennelly, L. J. (2013). Effective physical security. Oxford: Butterworth-Heinemann.

Fennelly, L., 2012. *Effective physical security*. Butterworth-Heinemann. Pieters, W., Dimkov, T. and Pavlovic, D., 2013. Security policy alignment: A formal approach. *IEEE Systems Journal*, *7*(2), pp.275-287.

Fennelly, L., 2012. *Effective physical security*. Butterworth-Heinemann. Pieters, W., Dimkov, T. and Pavlovic, D., 2013. Security policy alignment: A formal approach. *IEEE Systems Journal*, *7*(2), pp.275-287.

Ferry, D. J and Brandon, PS (1991) Cost Planning of Buildings, 6th edn., Blackwell Scientific Publications, Oxford

Field, Andy (2013) *Discovering statistics using IBM SPSS Statistics: and sex and drugs and rock 'n' roll (4th edition).*Sage, London.

Finnerty, J.D., 2013. *Project financing: Asset-based financial engineering*. John Wiley & Sons.

Fleischer, J., Wawerla, M. and Niggeschmidt, S., 2007. Machine life cycle cost estimation via Monte-Carlo simulation. In *Advances in Life Cycle Engineering for Sustainable Manufacturing Businesses* (pp. 449-453). Springer London.

Folland S, Goodman AC, Stano M. 2007. *The economics of health and health care*. 5th edition. Upper Saddle River, New Jersey: Pearson Education Inc.

Ford, G., Bartley, T., Igba, J., Turner, A. and McMahon, C., 2013, July. Product Life Cycle Data Management: A Cross-Sectoral Review. In *IFIP International Conference on Product Lifecycle Management* (pp. 58-67). Springer Berlin Heidelberg.

Garcia, M. L. (2006). Vulnerability Assessment of Physical Protection Systems. Burlington, MA: Elsevier Butterworth-Heinemann.

Garner, R. and Scott, G. (2013). *Doing Qualitative Research*. Pearson.

Goldkuhl, G. 2012. Pragmatism vs interpretivism in qualitative information systems research, Macmillan

Gomes, F., & Michaelides, A. (2005). Optimal Life-Cycle Asset Allocation: Understanding the Empirical Evidence. The Journal of Finance, 60(2), 869-904.

Green, A., 2014. Measuring up to maintenance. *Construction Journal*, p.18.

Guinée, J. and Heijungs, R., 2017. Introduction to life cycle assessment. In *Sustainable Supply Chains* (pp. 15-41). Springer International Publishing.

Haimes, Y.Y., 2015. *Risk modeling, assessment, and management*. John Wiley & Sons.

Halfpenny , Peter and Procter , Rob, eds. (2014) *Innovations in digital research methods.* London: Sage.

Hardy, G. (2012). Beyond Continuous Monitoring: Threat Modeling for Real-time Response. Retrieved from SANS Institute website: https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-threat-modeling-real-time-response-35185

Harris, C., Jones, P., Hillier, D. and Turner, D., 1998. CCTV surveillance systems in town and city centre management. *Property Management*, *16*(3), pp.160-165.

Harris, S. (2013). Access Control. In CISSP Exam Guide (6th ed., pp. 97, 98, 157- 277). USA McGraw-Hill.

Hastings, N.A., 2010. *Physical asset management* (Vol. 2). London: Springer.

He, Z. and Krishnamurthy, A., 2013. Intermediary asset pricing. *The American Economic Review*, *103*(2), pp.732-770.

Heijungs, R., Settanni, E. and Guinée, J., 2013. Toward a computational structure for life cycle sustainability analysis: unifying LCA and LCC. *The International Journal of Life Cycle Assessment*, *18*(9), pp.1722-1733.

Hernández-Moreno, S., Ocaña-Ponce, J.A. and Mejía-López, M., 2014. Application of ISO 15686 to estimate service life of a dome built with adobe technology in the city of Toluca, Mexico. *ActaUniversitaria*, *24*(6), pp.16-20.

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. Journal of risk and insurance, 78(4), 795-822.

Interagency Security Committee (ISC). (2015). Best Practices for Planning and Managing: Physical Security Resources: An Interagency Security Committee Guide. Retrieved from https://www.dhs.gov/sites/default/files/publications/isc-planning-managing-physical- security-resources-dec-2015-508.pdf

Irwin, S. (2014). Creating a Threat Profile for your Organization. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492

Jardine, A.K. and Tsang, A.H., 2013. *Maintenance, replacement, and reliability: theory and applications*. CRC press.

Johnston, R. G. & Garcia, A. R., (2002, September 03). Effective Vulnerability Assessments for Physical Security Devices, Systems, and Programs. Retrieved October 9, 2011, from Los Alamos National Laboratory: http://library.lanl.gov/cgi-bin/getfile?00852052.pdf

Kairab, S. (2005). A practical guide to security assessments. Boca Raton: CRC Press LLC.

Kaiser, H.F. *Psychometrika* (1974)

Kaming, P.F. and Marliansyah, J., 2016. Implementation of Life Cycle Costing: A Case of Hostel Building in Kediri, Eastern Jawa, Indonesia. In *Applied Mechanics and Materials* (Vol. 845, pp. 326-331). Trans Tech Publications.

Kerzner, H., 2001. *A Systems Approach to Planning, Scheduling and Controlling*, Wiley.

Kincaid, D., 2013. A starting- point for measuring physical performance. *Facilities*.

Kincaid, D., 2013. A starting-point for measuring physical performance. *Facilities*.

Kingsley-Hefty, J. (2013). Physical Security Strategy and Process Playbook. Oxford: Elsevier.

Kirkpatrick, D., Kirkpatrick, J., 2006. Evaluating Training Programs: The Four Levels, Berrett-Koehler.

Kishk, M., Al-Hajj, A., Pollock, R., Aouad, G., Bakis, N. and Sun, M., 2003. Whole life costing in construction: a state of the art review. *RICS Research Paper Series*.

Ko, Y.S., Park, K.H. and Kim, C.S., 2016. Problem Analysis and Countermeasures Research through Security Threat Cases of Physical Security Control Systems. *Journal of Korea Multimedia Society*, *19*(1), pp.51-59.

Korpi, E. and Ala-Risku, T., 2008. Life cycle costing: a review of published case studies. *Managerial Auditing Journal*, *23*(3), pp.240-261.

Kruegle, H. 2007. CCTV Surveillance: Video Practice and Technology. *Butterworth-Heinemann: Burlington.*

Kumar, U.D., Crocker, J., Knezevic, J. and El-Haram, M., 2012. *Reliability, Maintenance and Logistic Support:-A Life Cycle Approach*. Springer Science & Business Media.

Lam, J. (2014). Enterprise risk management: from incentives to controls. John Wiley & Sons.

Laura, C.S. and Vicente, D.C., 2014. Life-cycle cost analysis of floating offshore wind farms. *Renewable Energy*, *66*, pp.41-48.

Lee, C. and Lee, E.B., 2017. Prediction method of real discount rate to improve accuracy of life-cycle cost analysis. *Energy and Buildings*, *135,* pp.225-232.

Lee, H. *The Triple-A Supply Chain*. 2004. Harvard Business Review.

Lee, J.M., Shilling, J.D. and Wurtzebach, C., 2016. A New Method to Estimate Risk and Return of Commercial Real Estate Assets from Cash Flows: The Case of Open-End (Diversified) Core Private Equity Real Estate Funds.

Lemer, A., 2015. Life Cycle Costing: For the Analysis, Management and Maintenance of Civil Engineering Infrastructure. *Construction Management and Economics*, *33*(8), pp.689-691..

Leontief, W.W., 1937. Interrelation of prices, output, savings, and investment. *The Review of Economic Statistics*, pp.109-132.

Levin, L. (1998). Are assets fungible?: Testing the behavioral theory of life-cycle savings. Journal of Economic Behavior & Organization, 36(1), 59-83.

Li, Y. and Yang, L., 2013. Prospect theory, the disposition effect, and asset prices. *Journal of Financial Economics*, *107*(3), pp.715-739.

Liu, J., Love, P.E., Smith, J., Regan, M. and Davis, P.R., 2014. Life cycle critical success factors for public-private partnership infrastructure projects. *Journal of Management in Engineering*, *31*(5), p.04014073.

Liyanage, J.P., 2007. Operations and maintenance performance in production and manufacturing assets: The sustainability perspective. *Journal of Manufacturing Technology Management*, *18*(3), pp.304-314.

Loughborough University. 2003. Physical Security/Fraud and Information Security Module. Business School; *Professional and Management Development Centre.*

Magni, C.A., 2013. The internal rate of return approach and the AIRR paradigm: a refutation and a corroboration. *The Engineering Economist*, *58*(2), pp.73-111.

Malmenbratt, J. and Brooks, D.J., 2015. CCTV surveillance: The differing aims and functions of CCTV within the corporate stratum.

Márquez, A.C., Márquez, C.P., Fernández, J.F.G., Campos, M.L. and Díaz, V.G.P., 2012. Life cycle cost analysis. In *Asset Management* (pp. 81-99). Springer Netherlands.

Matchett, R. 2003. CCTV for Security Professionals. *Butterworth-Heinemann: USA.*

McCall N, Rice T, Sangl J. 1986. *Consumer Knowledge of Medicare and Supplemental Health Insurance Benefits.* Health Services Research.

McDougall, A. and Woodruff, J., 2016. Physical Security Management. *Handbook of SCADA/Control Systems Security*, p.287.

McNeil, A.J., Frey, R. and Embrechts, P., 2015. *Quantitative risk management: Concepts, techniques and tools*. Princeton university press.

McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value?. Journal of Accounting, Auditing & Finance, 26(4), 641-658.

Melby, J. M., Suhy Jr, A. F., & Parent, B. C. (2005). Apparatus and method for tracking and managing physical assets. U.S. Patent No. 6,952,680. Washington, DC: U.S. Patent and Trademark Office.

Mele, A. and Sangiorgi, F., 2015. Uncertainty, information acquisition, and price swings in asset markets. *The Review of Economic Studies*, p.rdv017.

Miller, K.C. and Beckman, P.C., Amazon Technologies, Inc., 2013. *Integrated physical security control system for computing resources*. U.S. Patent 8,528,101.

Mitrou, L., Drogkaris, P. and Leventakis, G., 2014. Legal and Social Aspects of Surveillance Technologies: CCTV in Greece?. *Perspectives on Surveillance*, p.39.

Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber–physical security of a smart grid infrastructure. Proceedings of the IEEE, 100(1), 195-209.

Nicholson, D., Smith, P., Bowers, G.A., Cuceoglu, F., Olgun, C.G., McCartney, J.S., Henry, K., Meyer, L.L. and Loveridge, F.A., 2014.

Norman, T. (2007). Integrated security systems design. Concepts, specifications and implementation. MA: Butterworth-Heinemann.

Norman, T. (2012). Electronic access control. Oxford: Elsevier Inc.

Norman, T.L., 2014. *Integrated Security Systems Design: A Complete Reference for Building Enterprise-wide Digital Security Systems*. Butterworth-Heinemann.

Norman, T.L., 2016. *Risk analysis and security countermeasure selection*. CRC press.

Nundy, S., Dick, J.J., Chou, C.H., Nocon, R.S., Chin, M.H. and Peek, M.E., 2014. Mobile phone diabetes project led to improved glycemic control and net savings for Chicago plan participants. *Health Affairs*, *33*(2), pp.265-272.

Olenewa, J. (2014). Radio Frequency Identification and Near-Field Communication. In Guide to wireless communications (3rd ed., pp. 392-395). Boston, MA: Cengage Learning.

Oriyano, S. (2014). Physical Security. In Cehv8: Certified Ethical Hacker Version 8 Study Guide (pp. 393-409). Indianapolis, IN USA: Wiley.

Pannell, D., Lampley, D., Ronci, C. and Spence, S., 2015. The Utility Risk Equation: An Interactive Case Study. *Proceedings of the Water Environment Federation*, *2015*(4), pp.1-12.

Patrick, M., Patrick, M., French, N. and French, N., 2016. The internal rate of return (IRR): projections, benchmarks and pitfalls. *Journal of Property Investment & Finance*, *34*(6), pp.664-669.

Peltier, T.R., 2016. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press.

Pikaar, R., de Groot, N., Mulder, E. and Remijn, B., 2016, September. Human Factors in Control Room Design & Effective Operator Participation. In *SPE Intelligent Energy International Conference and Exhibition*. Society of Petroleum Engineers.

Piza, E.L., Caplan, J.M., Kennedy, L.W. and Gilchrist, A.M., 2015. The effects of merging proactive CCTV monitoring with directed police patrol: a randomized controlled trial. *Journal of Experimental Criminology*, *11*(1), pp.43-69.

Pizzol, M., Weidema, B., Brandão, M. and Osset, P., 2015. Monetary valuation in life cycle assessment: a review. *Journal of Cleaner Production*, *86*, pp.170-179.

Proctor, P. E., Byrnes, C., Barber, R., & Foreword By-Moss, J. (2002). The secured enterprise: protecting your information assets. Prentice Hall PTR.

Rahman, S. and Vanier, D.J., 2004. Life cycle cost analysis as a decision support tool for managing municipal infrastructure.

Reason, J., 2016. *Managing the risks of organizational accidents*. Routledge.

Ricks, T.A., Ricks, B.E. & Dingle, J. (2015). Physical security and safety: A field guide for the practitioner. Boca Raton, FL: Taylor & Francis Group.

Ristimäki, M., Säynäjoki, A., Heinonen, J. and Junnila, S., 2013. Combining life cycle costing and life cycle assessment for an analysis of a new residential district energy system design. *Energy*, *63*, pp.168-179.

Ritchie, J., Lewis, J., Nicholls, C. M., Ormston, R. (2013). Qualitative Research Practice: A Guide for Social Science Students and Researchers. SAGE.

Roper, C.A., 1999. *Risk management for security professionals*. Butterworth-Heinemann.

Roper, K., Payant, R., 2014. *The Facility Management Handbook*.

Rose, G.S., Rajendran, J., McDonald, N., Karri, R., Potkonjak, M. and Wysocki, B., 2013, January. Hardware security strategies exploiting nanoelectronic circuits. In *Design*

Automation Conference (ASP-DAC), 2013 18th Asia and South Pacific (pp. 368-372). IEEE.

Ryan, B., Scapens, R. W. and Theobald, M. (2002) Research method and methodology in Finance and Accounting, Thompson, London.

Saltman, R.B., Busse, R. and Figueras, J., Eds., *Social Health Insurance Systems in Western Europe*. Open University Press, Berkshire, 33-81.

Santos, J. and Ferreira, A., 2013. Life-cycle cost analysis system for pavement management at project level. *International Journal of Pavement Engineering*, *14*(1), pp.71-84.

Saunders, M., Lewis, P. and Thornhill, A. (2014) Research Methods for Business Students. Pearson Education Ltd., Harlow.

Şchiopu, P. & Costea, A. (2015). Design of anti-burglar alarm systems. Proceedings of SPIE, 9258, 925817-925817-7.

Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F. and Sommerlad, P., 2013. *Security Patterns: Integrating security and systems engineering*. John Wiley & Sons.

Schuman, C.A. and Brent, A.C., 2005. Asset life cycle management: towards improving physical asset performance in the process industry. *International Journal of Operations & Production Management*, *25*(6), pp.566-579.

Settanni, E., Newnes, L.B., Thenent, N.E., Parry, G. and Goh, Y.M., 2014. A through-life costing methodology for use in product–service-systems. *International Journal of Production Economics*, *153*, pp.161-177.

Shahidehpour, M. and Ferrero, R., 2005. Time management for assets: chronological strategies for power system asset management. *IEEE Power and Energy Magazine*, *3*(3), pp.32-38.

Siergiejczyk, M., Paś, J. and Rosiński, A., 2014, October.Evaluation of safety of highway CCTV system's maintenance process.In *International Conference on Transport Systems Telematics* (pp. 69-79).Springer Berlin Heidelberg.

Siergiejczyk, M., Paś, J. and Rosiński, A., 2015.Reliability and maintenance analysis of CCTV systems used in rail transport. *Journal of KONBiN*, *35*(1), pp.137-146.

Silalertruksa, T., Bonnet, S. and Gheewala, S.H., 2012. Life cycle costing and externalities of palm oil biodiesel in Thailand. *Journal of Cleaner Production*, *28*, pp.225-232.

Smith, D.K., 1999, May. Total life-cycle cost. In *Proceedings of the 8th International Conference on the Durability of Building Materials and Components, Vancouver, NRC Research Press, Ottawa*.

Smith, K., 2013. *Environmental hazards: assessing risk and reducing disaster*. Routledge.

Spielmann, C., Hutter, M., Klein, J. and Singhani, N., Jpmorgan Chase Bank and NA, 2006. *Method and system for managing risks*. U.S. Patent 7,113,914.

Stark, J., 2015. Product lifecycle management. In *Product Lifecycle Management* (pp. 1-29). Springer International Publishing.

Stevenson, W.J., and Sum, C.C., 2007. *Operations Management*, McGraw-Hill.

Stewart, J., Chapple, M., & Gibson, D. (2012). Physical Security Requirements. In CISSP Certified Information Systems Security Professional study guide (6th ed., pp. 572-597,745-774). Indianapolis, IN USA: Wiley.

Straub, D.W. and Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. *MIS quarterly*, pp.441-469.

Sullivan, G.P., Pugh, R., Melendez, A.P. and Hunt, W.D., 2004. Operations & Maintenance Best Practices. *A guide to achieving operational efficiency, Release*, *2*.

Taylor, J.S., Bogdan, R. DeVault, M. 2015. *Introduction to Qualitative Research Methods*, Wiley.

Taylor, W.B., 1981. The use of life cycle costing in acquiring physical assets. *Long range planning*, *14*(6), pp.32-43.

Tesfamariam, S., Sanchez-Silva, M. (2011): *A model for earthquake risk management based on the life-cycle performance of structures, Civil Engineering and Environmental Systems*

Touran, A. and Wiser, E.P., 1992. Monte Carlo technique with correlated random variables. *Journal of Construction Engineering and Management*, *118*(2), pp.258-272.

Traub, P. and Fraser, G., 2013. Safety Assessment Of Cctv For Platform Interface Tasks—Sydney Suburban Trains. *Rail Human Factors: Supporting reliability, safety and cost reduction*, p.300.

U.S. Department of Homeland Security, & Interagency Security Committee (ISC). (2009). Interagency Security Committee Use of Physical Security Performance Measures.

Retrieved from https://www.dhs.gov/xlibrary/assets/isc_physical_security_performance_measures.pdf

Voss, V. Tsikriktsis, N. and Frohlich, M. (2002) *Case Research in Operations Management*. International Journal of Operations & Production Management

Wailgum, T. (2005). Metrics for Corporate and Physical Security Programs | CSO Online. Retrieved from http://www.csoonline.com/article/2118531/metrics- budgets/metrics-for-corporate-and-physical-security-programs.html

Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D.W., Middleton, B. 2005. *The value of health care information exchange and interoperability*

Whyte, A. and Gayner, L., 2013. Life-cycle cost analysis of infrastructure pavement applications in Western Australia.

Wong, N.H., Tay, S.F., Wong, R., Ong, C.L. and Sia, A., 2003. Life cycle cost analysis of rooftop gardens in Singapore. *Building and environment*, *38*(3), pp.499-509.

Woodward, D.G., 1997. Life cycle costing—theory, information acquisition and application. *International journal of project management*, *15*(6), pp.335-344.

World Health Organization, 2010. *Administrative costs of Health Insurance Schemes: Exploring the reasons for their variability*

Wysocki, R., 2014. *Effective Project Management:Traditional, Agile, Extreme*. Wiley

Zamagni, A., 2012. Life cycle sustainability assessment. *The International Journal of Life Cycle Assessment*, *17*(4), pp.373-376.

Zhang, Y., & Wei, B. (2008). Reflections on Implementing Assets Life Cycle Management in Power Grid Corporations [J]. Electric Power Technologic Economics, 4, 016.

Appendix

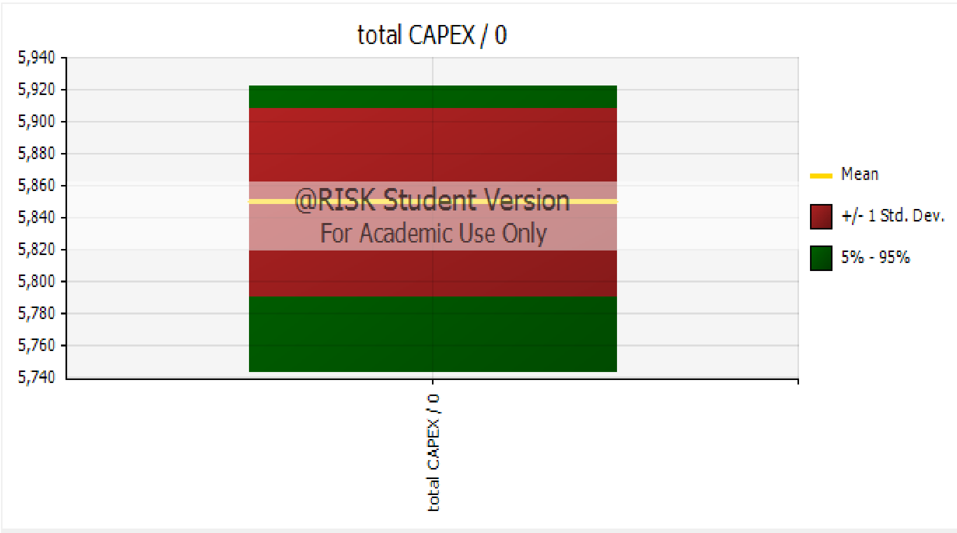


Fig. Trends for Total CAPEX

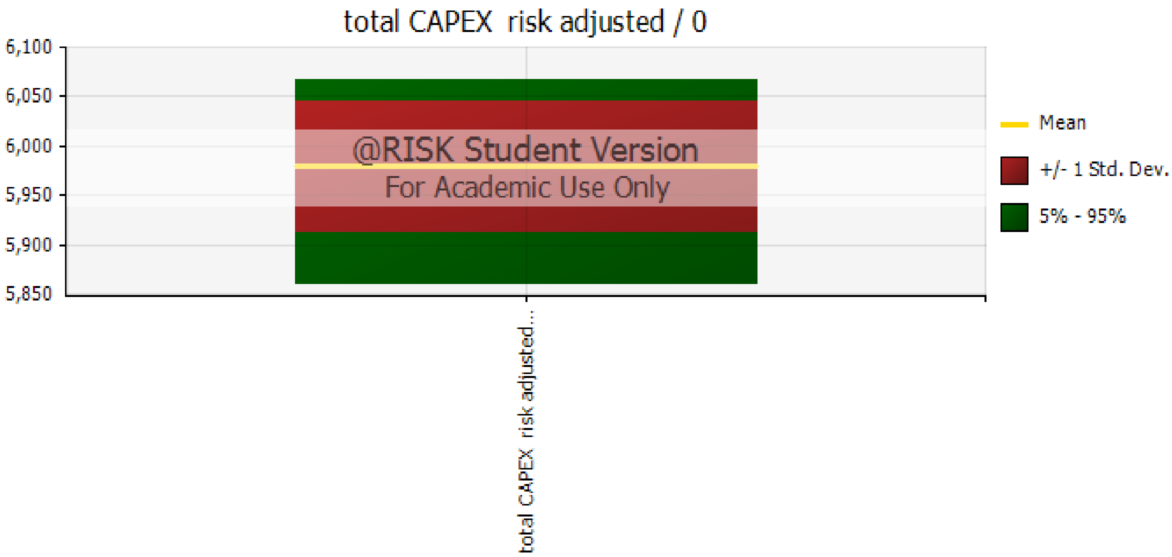


Fig Trends for Total CAPEX with Adjustment

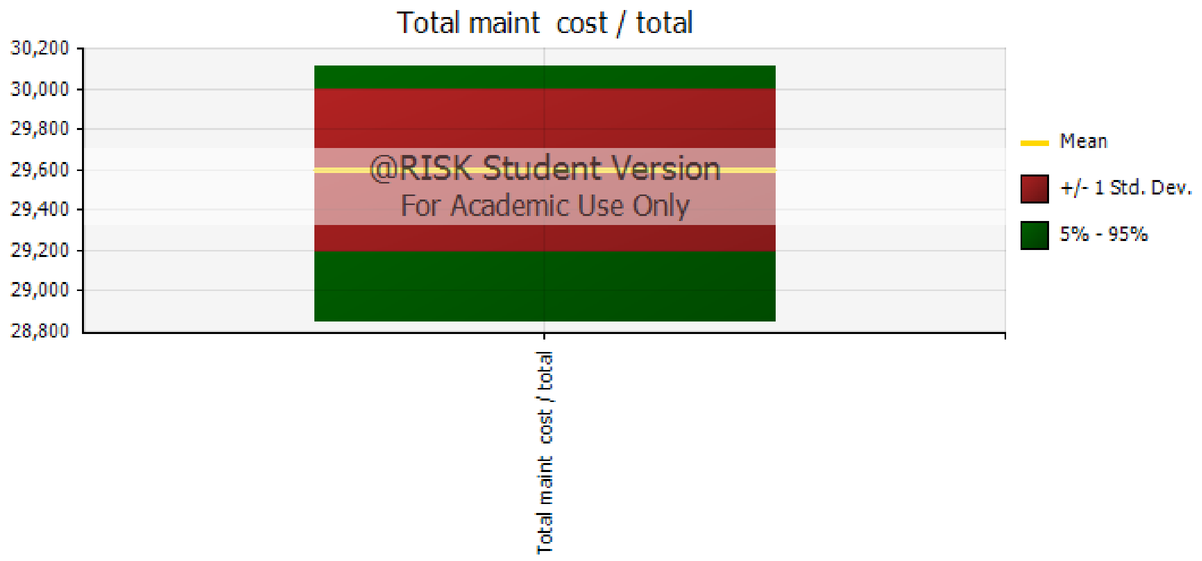


Fig .Trends for Total Maintenance Cost

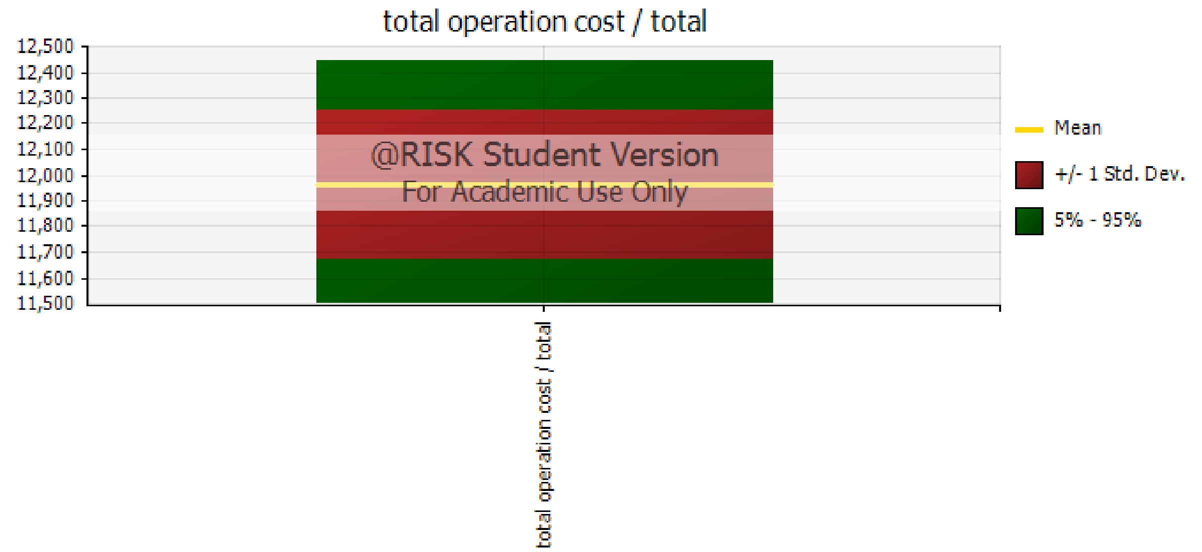


Fig.Trends for Total Operation Cost

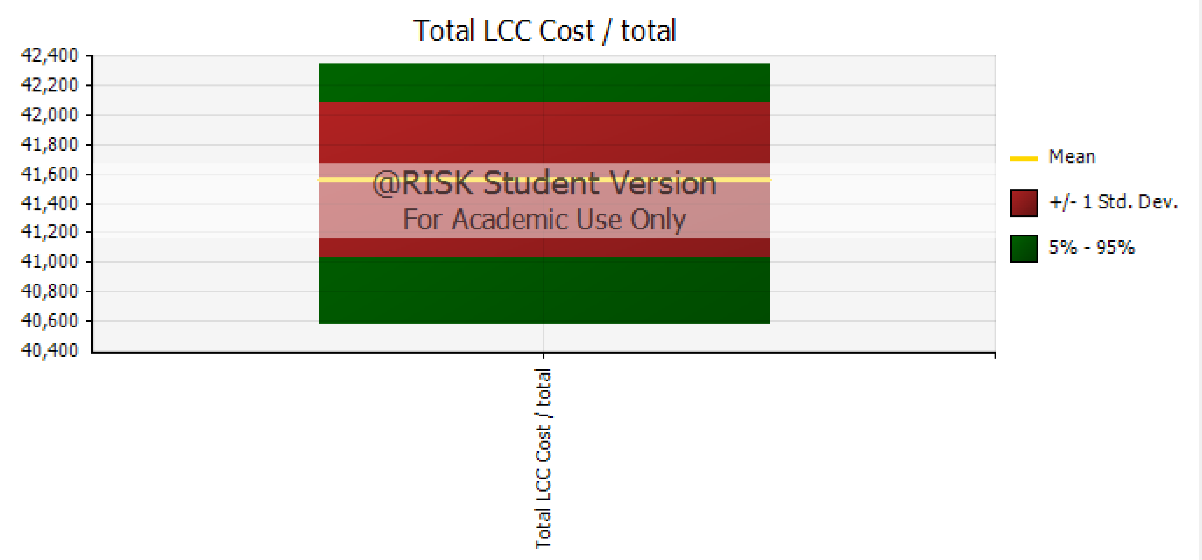


Fig.Trends for Total LCC Cost

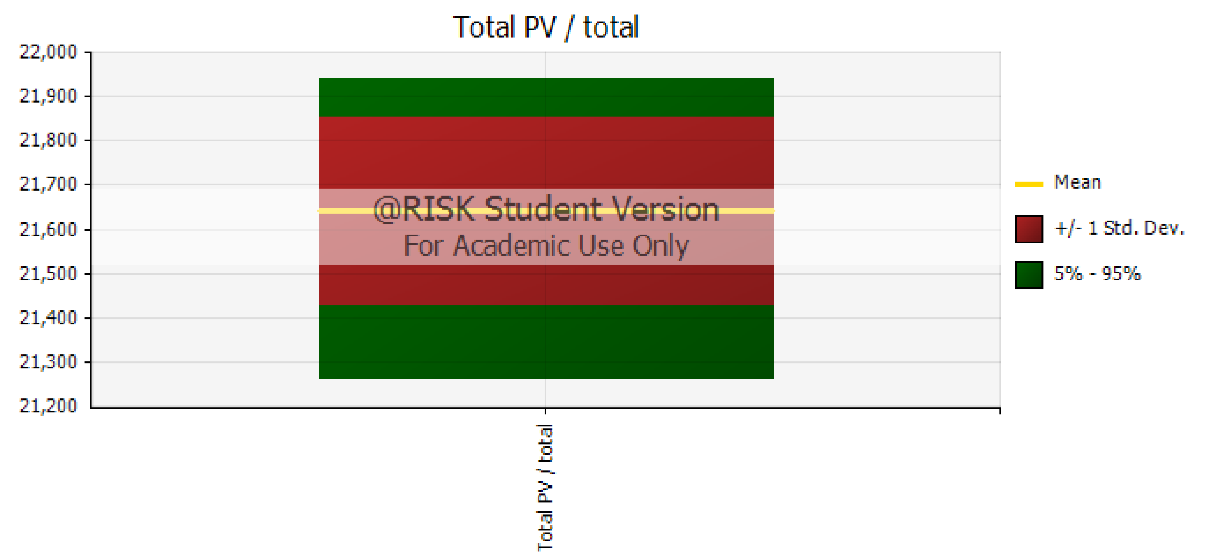


Fig.Trends for Total PV Cost

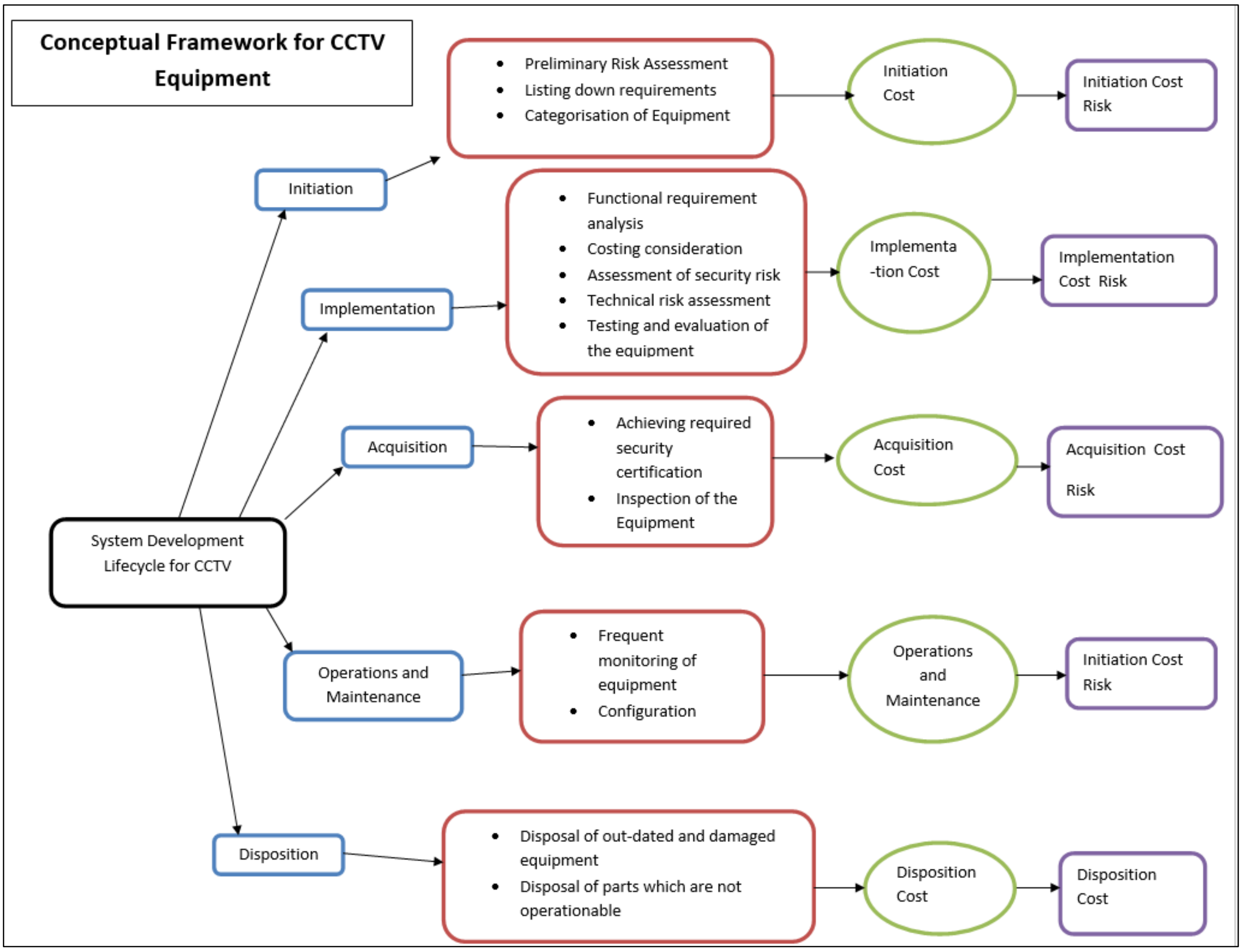


Fig. Conceptual Framework

Consultancy fee	Survey fee	Cameras Cost	Cabling Cost	Switches Cost	Servers Cost	Software Cost	Monitors Cost	Storages Cost	UPS System (	Accessories an	Multimedia C	Civil Work	Installing C
215	255.50	2650	327.5	242	40.3	361	33.15	669	10.94	64.1	251.4	321.23	427.5
217	253.65	2670	325	241	42	364	32.7	664	11.76	63.5	252.82	322.12	428.6
215	255.00	2600	328	245	41	360.95	32.5	668	11.26	62.3	250.02	320.44	428
218	255.31	2625	326	242.3	40.6	360.15	33.8	667.12	10.82	64.3	250.5	321.15	426.8
214	254.00	2500	328.5	243.5	42	362	31.8	666.45	11.88	62.5	251.12	323.2	428.4
215	254.58	2599	326.4	242.8	41.45	364	33.3	669.5	12	63.5	250.2	321.75	425.9
216	255.10	2600	327.1	244.1	44	362.2	33.5	665.25	10.98	64.8	252.68	321.17	427.45
218	256.00	2699	326.2	241.9	41.1	362.25	33.9	668.3	11.24	63.4	251.4	323.45	425.99
217	254.88	2700	326.3	244.4	43.3	360	33.4	667.5	11.78	64.8	251.12	323.78	426.78
216	253.94	2655	325.7	244	43	360.45	32.4	664.75	11.96	64.11	252.25	321.56	427.15

Fig. CAPEX raw Data from the 10 companies

Control room	Transmission Cost	Lay out Cost	Man power	Electricity
171.5	59	17	48.48	41
170.22	56.9	16	48.15	43
170.18	57	16	48.585	44
172.25	58.01	17.5	47.5	41.5
171.58	58.45	17.15	47.49	43
170.62	56.3	16.95	48.1	42.6
171.77	57.12	16.75	47.9	44
170.8	57.61	17	47.47	43.8
172.88	58.69	16.9	48.99	41
171.87	56.56	16.1	48.02	42

Fig. OPEX raw Data from the 10 companies

Correlations

		N Ri1	R i23	R i12	R i10	Ri 19
Ri1	Pearson Correlation	1	.861**	.854**	.917**	.823**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	68	68	68	68	68
i23	Pearson Correlation	.861**	1	.613**	.788**	.504**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	68	68	68	68	68
i12	Pearson Correlation	.854**	.613**	1	.690**	.711**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	68	68	68	68	68
i10	Pearson Correlation	.917**	.788**	.690**	1	.677**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	68	68	68	68	68
i19	Pearson Correlation	.823**	.504**	.711**	.677**	1

	Sig. (2-tailed)	.000	.000	.000	.000	
	N	68	68	68	68	68

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

Figure: Factor Scoring Coefficients for Ri

Correlations

		N Ri2	Ri16	Ri14	Ri18	Ri15	Ri17	i2
Ri2	Pearson Correlation	1	.854**	.786**	.795**	.638**	.652**	625**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	000
	N	68	68	68	68	68	68	8
i16	Pearson Correlation	.854**	1	.700**	.659**	.556**	.433**	389**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	001
	N	68	68	68	68	68	68	8
i14	Pearson Correlation	.786**	.700**	1	.478**	.683**	.455**	357**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	003
	N	68	68	68	68	68	68	8
i18	Pearson Correlation	.795**	.659**	.478**	1	.564**	.406**	308*
	Sig. (2-tailed)	.000	.000	.000		.000	.001	011
	N	68	68	68	68	68	68	8
i15	Pearson Correlation	.638**	.556**	.683**	.564**	1	.433**	156
	Sig. (2-tailed)	.000	.000	.000	.000		.000	203
	N	68	68	68	68	68	68	8
i17	Pearson Correlation	.652**	.433**	.455**	.406**	.433**	1	227

	Sig. (2-tailed)	.000	.000	.000	.001	.000		063
	N	68	68	68	68	68	68	8
i2	Pearson Correlation	.625**	.389**	.357**	.308*	.156	.227	
	Sig. (2-tailed)	.000	.001	.003	.011	.203	.063	
	N	68	68	68	68	68	68	8

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

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

Correlations

		NRi3	Ri22	Ri21	Ri20	Ri8	Ri13
Ri3	Pearson Correlation	1	.905**	.875**	.878**	.502**	.498**
	Sig. (2-tailed)		.000	.000	.000	.000	.000
	N	68	68	68	68	68	68
i22	Pearson Correlation	.905**	1	.793**	.715**	.366**	.369**
	Sig. (2-tailed)	.000		.000	.000	.002	.002
	N	68	68	68	68	68	68
i21	Pearson Correlation	.875**	.793**	1	.776**	.233	.236
	Sig. (2-tailed)	.000	.000		.000	.056	.053
	N	68	68	68	68	68	68
i20	Pearson Correlation	.878**	.715**	.776**	1	.286*	.319**
	Sig. (2-tailed)	.000	.000	.000		.018	.008
	N	68	68	68	68	68	68
i8	Pearson Correlation	.502**	.366**	.233	.286*	1	.215

	Sig. (2-tailed)	.000	.002	.056	.018		.078
	N	68	68	68	68	68	68
i13	Pearson Correlation	.498**	.369**	.236	.319**	.215	1
	Sig. (2-tailed)	.000	.002	.053	.008	.078	
	N	68	68	68	68	68	68

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

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

		NRm1	Rm8	Rm6	Rm5	Rm10	Rm12	Rm1	Rm3
NRm1	Pearson Correlation	1	.757**	.800**	.769**	.767**	.788**	.684**	.701**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000
	N	68	68	68	68	68	68	68	68
Rm8	Pearson Correlation	.757**	1	.647**	.525**	.655**	.349**	.479**	.478**
	Sig. (2-tailed)	.000		.000	.000	.000	.004	.000	.000
	N	68	68	68	68	68	68	68	68
Rm6	Pearson Correlation	.800**	.647**	1	.605**	.481**	.469**	.483**	.557**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000	.000
	N	68	68	68	68	68	68	68	68
Rm5	Pearson Correlation	.769**	.525**	.605**	1	.444**	.537**	.549**	.526**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000
	N	68	68	68	68	68	68	68	68
Rm10	Pearson Correlation	.767**	.655**	.481**	.444**	1	.719**	.524**	.361**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.003
	N	68	68	68	68	68	68	68	68
Rm12	Pearson Correlation	.788**	.349**	.469**	.537**	.719**	1	.469**	.396**
	Sig. (2-tailed)	.000	.004	.000	.000	.000		.000	.001
	N	68	68	68	68	68	68	68	68
Rm1	Pearson Correlation	.684**	.479**	.483**	.549**	.524**	.469**	1	.573**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.000
	N	68	68	68	68	68	68	68	68
Rm3	Pearson Correlation	.701**	.478**	.557**	.526**	.361**	.396**	.573**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.003	.001	.000	
	N	68	68	68	68	68	68	68	68
Rm7	Pearson Correlation	.687**	.498**	.628**	.693**	.227	.501**	.256*	.407**
	Sig. (2-tailed)	.000	.000	.000	.000	.063	.000	.035	.001
	N	68	68	68	68	68	68	68	68

Figure: Factor Scoring Coefficients for Rm

Correlations

		Rm7	Rm11
NRm1	Pearson Correlation	.687**	.755**
	Sig. (2-tailed)	.000	.000
	N	68	68
Rm8	Pearson Correlation	.498**	.411**
	Sig. (2-tailed)	.000	.001
	N	68	68
Rm6	Pearson Correlation	.628**	.530**
	Sig. (2-tailed)	.000	.000
	N	68	68
Rm5	Pearson Correlation	.693**	.380**
	Sig. (2-tailed)	.000	.001
	N	68	68
Rm10	Pearson Correlation	.227	.614**
	Sig. (2-tailed)	.063	.000
	N	68	68
Rm12	Pearson Correlation	.501**	.786**
	Sig. (2-tailed)	.000	.000
	N	68	68
Rm1	Pearson Correlation	.256*	.317**
	Sig. (2-tailed)	.035	.008
	N	68	68
Rm3	Pearson Correlation	.407**	.466**
	Sig. (2-tailed)	.001	.000
	N	68	68
Rm7	Pearson Correlation	1	.477**
	Sig. (2-tailed)		.000
	N	68	68
Rm11	Pearson Correlation	.477**	1
	Sig. (2-tailed)	.000	
	N	68	68

Correlations

		NRm2	Rm13	Rm9	Rm4
NRm2	Pearson Correlation	1	.971**	.840**	.759**
	Sig. (2-tailed)		.000	.000	.000
	N	68	68	68	68
Rm13	Pearson Correlation	.971**	1	.722**	.651**
	Sig. (2-tailed)	.000		.000	.000
	N	68	68	68	68
Rm9	Pearson Correlation	.840**	.722**	1	.569**
	Sig. (2-tailed)	.000	.000		.000
	N	68	68	68	68
Rm4	Pearson Correlation	.759**	.651**	.569**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	68	68	68	68

Correlations

		NRm3	Rm14	Rm17	Rm16
NRm3	Pearson Correlation	1	.802**	.764**	.516**
	Sig. (2-tailed)		.000	.000	.000
	N	68	68	68	68
Rm14	Pearson Correlation	.802**	1	.308*	.277*
	Sig. (2-tailed)	.000		.010	.022
	N	68	68	68	68
Rm17	Pearson Correlation	.764**	.308*	1	.186
	Sig. (2-tailed)	.000	.010		.130
	N	68	68	68	68
Rm16	Pearson Correlation	.516**	.277*	.186	1
	Sig. (2-tailed)	.000	.022	.130	
	N	68	68	68	68

Correlations

		NRo1	Ro6	Ro4	Ro5	Ro2	Ro3	Ro9
NRo1	Pearson Correlation	1	.953**	.931**	.936**	.926**	.795**	.752**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000
	N	68	68	68	68	68	68	68
Ro6	Pearson Correlation	.953**	1	.862**	.862**	.882**	.767**	.629**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000
	N	68	68	68	68	68	68	68
Ro4	Pearson Correlation	.931**	.862**	1	.866**	.856**	.644**	.671**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000
	N	68	68	68	68	68	68	68
Ro5	Pearson Correlation	.936**	.862**	.866**	1	.844**	.715**	.633**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000
	N	68	68	68	68	68	68	68
Ro2	Pearson Correlation	.926**	.882**	.856**	.844**	1	.596**	.698**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000
	N	68	68	68	68	68	68	68
Ro3	Pearson Correlation	.795**	.767**	.644**	.715**	.596**	1	.539**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000
	N	68	68	68	68	68	68	68
Ro9	Pearson Correlation	.752**	.629**	.671**	.633**	.698**	.539**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	
	N	68	68	68	68	68	68	68

Figure: Factor Scoring Coefficients for Ro

Correlations

		NRo2	Ro8	Ro7	Ro13
NRo2	Pearson Correlation	1	.991**	.992**	.978**
	Sig. (2-tailed)		.000	.000	.000
	N	68	68	68	68
Ro8	Pearson Correlation	.991**	1	.987**	.945**
	Sig. (2-tailed)	.000		.000	.000
	N	68	68	68	68
Ro7	Pearson Correlation	.992**	.987**	1	.950**
	Sig. (2-tailed)	.000	.000		.000
	N	68	68	68	68
Ro13	Pearson Correlation	.978**	.945**	.950**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	68	68	68	68

Correlations

		NRo3	Ro12	Ro10	Ro11	Ro1
NRo3	Pearson Correlation	1	.781**	.760**	.676**	.754**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	68	68	68	68	68
Ro12	Pearson Correlation	.781**	1	.820**	.720**	.253*
	Sig. (2-tailed)	.000		.000	.000	.038
	N	68	68	68	68	68
Ro10	Pearson Correlation	.760**	.820**	1	.756**	.220
	Sig. (2-tailed)	.000	.000		.000	.072
	N	68	68	68	68	68
Ro11	Pearson Correlation	.676**	.720**	.756**	1	.124
	Sig. (2-tailed)	.000	.000	.000		.316
	N	68	68	68	68	68
Ro1	Pearson Correlation	.754**	.253*	.220	.124	1
	Sig. (2-tailed)	.000	.038	.072	.316	
	N	68	68	68	68	68

Correlations

		NRA1	RA7	RA4	RA5	RA6	RA3	RA11	RA13
NRA1	Pearson Correlation	1	.917**	.931**	.922**	.907**	.881**	.636**	.553**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000
	N	68	68	68	68	68	68	68	68
RA7	Pearson Correlation	.917**	1	.830**	.818**	.813**	.775**	.516**	.514**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.000
	N	68	68	68	68	68	68	68	68
RA4	Pearson Correlation	.931**	.830**	1	.807**	.913**	.751**	.534**	.449**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000	.000
	N	68	68	68	68	68	68	68	68
RA5	Pearson Correlation	.922**	.818**	.807**	1	.811**	.831**	.501**	.481**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000
	N	68	68	68	68	68	68	68	68
RA6	Pearson Correlation	.907**	.813**	.913**	.811**	1	.727**	.472**	.356**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.003
	N	68	68	68	68	68	68	68	68
RA3	Pearson Correlation	.881**	.775**	.751**	.831**	.727**	1	.545**	.393**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.001
	N	68	68	68	68	68	68	68	68
RA11	Pearson Correlation	.636**	.516**	.534**	.501**	.472**	.545**	1	.281*
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.020
	N	68	68	68	68	68	68	68	68
RA13	Pearson Correlation	.553**	.514**	.449**	.481**	.356**	.393**	.281*	1
	Sig. (2-tailed)	.000	.000	.000	.000	.003	.001	.020	
	N	68	68	68	68	68	68	68	68

Figure: Factor Scoring Coefficients for RA

Correlations

		NRA2	RA8	RA12	RA14	RA10
NRA2	Pearson Correlation	1	.892**	.845**	.698**	.622**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	68	68	68	68	68
RA8	Pearson Correlation	.892**	1	.751**	.585**	.392**
	Sig. (2-tailed)	.000		.000	.000	.001
	N	68	68	68	68	68
RA12	Pearson Correlation	.845**	.751**	1	.567**	.278*
	Sig. (2-tailed)	.000	.000		.000	.022
	N	68	68	68	68	68
RA14	Pearson Correlation	.698**	.585**	.567**	1	.119
	Sig. (2-tailed)	.000	.000	.000		.334
	N	68	68	68	68	68
RA10	Pearson Correlation	.622**	.392**	.278*	.119	1
	Sig. (2-tailed)	.000	.001	.022	.334	
	N	68	68	68	68	68

Correlations

		NRA3	RA2	RA1	RA9
NRA3	Pearson Correlation	1	.751**	.747**	.741**
	Sig. (2-tailed)		.000	.000	.000
	N	68	68	68	68
RA2	Pearson Correlation	.751**	1	.389**	.300*
	Sig. (2-tailed)	.000		.001	.013
	N	68	68	68	68
RA1	Pearson Correlation	.747**	.389**	1	.318**
	Sig. (2-tailed)	.000	.001		.008
	N	68	68	68	68
RA9	Pearson Correlation	.741**	.300*	.318**	1
	Sig. (2-tailed)	.000	.013	.008	
	N	68	68	68	68

Correlations

		NRD1	RD6	RD5	RD4	RD7	RD8	RD12
NRD1	Pearson Correlation	1	.917**	.904**	.874**	.906**	.756**	.644**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000
	N	68	68	68	68	68	68	68
RD6	Pearson Correlation	.917**	1	.848**	.855**	.827**	.645**	.413**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000
	N	68	68	68	68	68	68	68
RD5	Pearson Correlation	.904**	.848**	1	.770**	.797**	.543**	.527**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000
	N	68	68	68	68	68	68	68
RD4	Pearson Correlation	.874**	.855**	.770**	1	.723**	.549**	.486**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000
	N	68	68	68	68	68	68	68
RD7	Pearson Correlation	.906**	.827**	.797**	.723**	1	.738**	.443**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000
	N	68	68	68	68	68	68	68
RD8	Pearson Correlation	.756**	.645**	.543**	.549**	.738**	1	.341**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.004
	N	68	68	68	68	68	68	68
RD12	Pearson Correlation	.644**	.413**	.527**	.486**	.443**	.341**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.004	
	N	68	68	68	68	68	68	68

Figure: Factor Scoring Coefficients for RD

Correlations

		NRD2	RD11	RD14	RD13	RD3
NRD2	Pearson Correlation	1	.883**	.835**	.853**	.623**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	68	68	68	68	68
RD11	Pearson Correlation	.883**	1	.611**	.692**	.494**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	68	68	68	68	68
RD14	Pearson Correlation	.835**	.611**	1	.740**	.305*
	Sig. (2-tailed)	.000	.000		.000	.011
	N	68	68	68	68	68
RD13	Pearson Correlation	.853**	.692**	.740**	1	.262*
	Sig. (2-tailed)	.000	.000	.000		.031
	N	68	68	68	68	68
RD3	Pearson Correlation	.623**	.494**	.305*	.262*	1
	Sig. (2-tailed)	.000	.000	.011	.031	
	N	68	68	68	68	68

Correlations

		NRD3	RD1	RD10	RD9	RD2
NRD3	Pearson Correlation	1	.830**	.752**	.654**	.699**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	68	68	68	68	68
RD1	Pearson Correlation	.830**	1	.437**	.384**	.514**
	Sig. (2-tailed)	.000		.000	.001	.000
	N	68	68	68	68	68
RD10	Pearson Correlation	.752**	.437**	1	.665**	.261*
	Sig. (2-tailed)	.000	.000		.000	.032
	N	68	68	68	68	68
RD9	Pearson Correlation	.654**	.384**	.665**	1	.106
	Sig. (2-tailed)	.000	.001	.000		.388
	N	68	68	68	68	68
RD2	Pearson Correlation	.699**	.514**	.261*	.106	1
	Sig. (2-tailed)	.000	.000	.032	.388	
	N	68	68	68	68	68

SAMPLE OF THE SURVERY

A- GENERAL INFORMATION

- **Respondent's position:**

☐ Public Sector ☐ Private Sector

- **Job title:**

☐ Estimator ☐ Cost Engineer
☐ Project Manager ☐ Security Engineer
☐ General Manager ☐ Security Consultant
☐ Project Engineer ☐ Technician
☐ Control Room Operator ☐ Others
☐ QA Manager

- **Experience in the organization:**

☐ Less than 3 years ☐ 5 years – 10 years
☐ 3 - 5 years ☐ More than 10 years

- **Sizes of the projects involve:**

☐ Less than 500,000 AED ☐ 500,000 – 1,000,000 AED
☐ 1,000,000 - 5,000,000 AED ☐ More 5,000,000 AED

A- The influence of risks on Physical security Assets (PSA) costs:

1. **Please rate the influence/impact of the following initiation risks on the Cost of security systems.**

Risk Factors		Degree of Risk impact on risk cost (1%-72%)	Risk Matrix
1	Wrong budget estimation		
2	Cost overruns due to change of scope		
3	Continual project scope expansion		
4	Delayed on approval		
5	Ill-defined scope		
6	Scope creep		
7	Gold plating		
8	Inter-dependencies are not defined well		
9	Inter-dependencies are not coordinated and approved		
10	Missing critical activities from scope		
11	Not knowing stakeholders		
12	Technology design failures		
13	Risks in Specification Breakdown		
14	Unrealistic expectations of stakeholders		
15	Schedule flaws		
16	Quality management issues		
17	Human resource management issues		
18	Procurement management issues		
19	Time management issues		
20	Poor workmanship quality		
21	Frequent or Delay design change		
22	Contractor factor to platform		

Risk Matrix:

Probability					
VH (90%)	5%	9%	18%	36%	72%
H (70%)	4%	7%	14%	28%	56%
M (50%)	3%	5%	10%	20%	40%
L (30%)	2%	3%	6%	12%	24%
VL (10%)	1%	1%	2%	4%	8%
	VL (5%)	L (10%)	M (20 %)	H (40%)	VH (80%)
	IMPACT				

23	Poor negotiation between different stakeholders		

2. **Please rate the influence/impact of the following implementation risks on the Cost of security systems.**

Risk Factors		Degree of Risk impact on risk cost (1%-72%)	Risk Matrix
24	Change on Management		
25	Wrong timeframe estimation		
26	Change on Laws /Rules		
27	Poor in Project management		
28	Delays due to coordinates with other contractors		
29	Failure to identify complex functionalities and time required to develop those functionalities		
30	Information security incidents		
31	Legacy components lack adequate documentation		
32	Security assets are not maintainable		
33	Lack of Operationalisation		
34	Delays due to physical infrastructure		
35	Unexpected project scope expansions		
36	Product solution is complex to implement		
37	Staff turnover		
38	Insufficient financial resources		
39	Lack of Training on the system		
40	Poor quality management		

Probability					
VH (90%)	5%	9%	18%	36%	72%
H (70%)	4%	7%	14%	28%	56%
M (50%)	3%	5%	10%	20%	40%
L (30%)	2%	3%	6%	12%	24%
VL (10%)	1%	1%	2%	4%	8%
	VL (5%)	L (10%)	M (20 %)	H (40%)	VH (80%)
	IMPACT				

3. **Please rate the influence/impact of the following acquisition risks on the Cost of security systems.**

Risk Factors		Degree of Risk impact on risk cost (1%-72%)	Risk Matrix
41	Lack of funds		
42	Running out of funds		
43	Continually changing requirements		
44	Market development pace rendering products obsolete		
45	Changing priorities		
46	Government rule changes		
47	Hardware & Software defects		
48	Integration issues		
49	Inaccurate Cost forecasts		
50	Exchange rate variability not managed well		
51	Failure to integrate with existing systems		
52	Unavailability of adequate test environment		
53	Failure to integrate components		
54	Security Asset disrupts operations		

Risk Matrix:

Probability					
VH (90%)	5%	9%	18%	36%	72%
H (70%)	4%	7%	14%	28%	56%
M (50%)	3%	5%	10%	20%	40%
L (30%)	2%	3%	6%	12%	24%
VL (10%)	1%	1%	2%	4%	8%
	VL (5%)	L (10%)	M (20 %)	H (40%)	VH (80%)
	IMPACT				

4. **Please rate the influence/impact of the following Operations and Maintenance Risks on the Cost of security systems.**

Risk Factors		Degree of Risk impact on risk cost (1%-72%)	Risk Matrix
55	Lack or poor policy performance for monitoring the system		
56	Poor implementation which leads to Technical risks		
57	Failure to address priority conflicts		
58	Failure to allocate and resolve the responsibilities		
59	Insufficient human and financial resources		
60	Inadequate subject training		
61	Inadequate resource planning		
62	Poor communication in team		
63	Security Assets not fit for purpose		
64	Un-scalability of system		
65	Lack of interoperability		
66	Physical security assets are not compliant with regulatory standards and best practices.		
67	Lack of quality team		
68	Lack of stability		
69	No support from manufacture		
70	Change in operation process and policy		
71	Physical security assets not extensible		

Probability					
VH (90%)	5%	9%	18%	36%	72%
H (70%)	4%	7%	14%	28%	56%
M (50%)	3%	5%	10%	20%	40%
L (30%)	2%	3%	6%	12%	24%
VL (10%)	1%	1%	2%	4%	8%
	VL (5%)	L (10%)	M (20 %)	H (40%)	VH (80%)
	IMPACT				

5. Please rate the influence/impact of the following Disposition Risks on the Cost of security systems

Risk Factors		Degree of Risk impact on risk cost (1%-72%)	Risk Matrix
72	Health, and Safety Risks during process		
73	Selling Costs not feasible		
74	Environment risks		
75	Out-dated and damaged equipment		
76	Recycling cost risks		
77	Environmental Management Costs		
78	Lack of information on disposal of equipment costs		
79	Batteries Risks		
80	Failure to align with systems		
81	Compliance issues		
82	Ambiguity in process		
83	Contaminated waste costs		
84	Civic Amenity Sites costs		

Risk Matrix:

Probability					
VH (90%)	5%	9%	18%	36%	72%
H (70%)	4%	7%	14%	28%	56%
M (50%)	3%	5%	10%	20%	40%
L (30%)	2%	3%	6%	12%	24%
VL (10%)	1%	1%	2%	4%	8%
	VL (5%)	L (10%)	M (20 %)	H (40%)	VH (80%)
	IMPACT				