An Improved Information and Knowledge Security Risk Management Framework

By
Haleemah Zia
NUST201464167MSEECS63114F

Supervisor
Dr. Shahzad Saleem
Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Information Security (MS IS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(March, 2016)

I wish to dedicate my life and my work to the One who Created me. The One in whose Book I have found the greatest of treasures and pleasures. The One who has never returned me empty handed.

Certificate of Originality

I hereby declare that this submission titled **An Improved Information and Knowledge Security Risk Management Framework** is my own work.To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged. I also verified the originality of contents through plagiarism software.

Author Name: **Haleemah Zia**
Signature: _____

Acknowledgment

I want to thank all my teachers, especially my supervisor and all GEC members: Dr. Shahzad Saleem, Ms. Rahat Masood, Dr. Asad Waqar and Sir Ubaid-ur-Rehman for extending continuous support and cooperating with me at every single step, and for believing in my abilities.

I am honored to have been able to work under Dr. Shahzad, someone who values honesty a lot. He is helpful and cooperative beyond expectations and goes out of the way in assisting his students. I have learnt a lot from him especially the fact about always being appreciative of others and highlighting positive things even if they seem little. My sincere thanks goes out to him.

I want to thank Ms. Rahat for understanding my problems and for trusting me throughout my thesis phase. I feel blessed to have had the opportunity to work with someone as hardworking, considerate and accommodating as her. I would not have been able to move an inch in my thesis without her consistent support. She took out time for me even during the busiest of her schedules, kept encouraging me with positive comments whenever I would get worried, always made me feel so comfortable during all Skype and face-face meetings and sometimes appeared to be concerned for my thesis and my success even more than myself.

I also thank Dr. Asad and Sir Ubaid for providing the most intelligent feedback after every milestone or whenever I needed it. Both have been extremely kind to throughout. I cannot miss mentioning Dr. Shibli here either. He has been one of my best teachers, extremely supportive and inspirational. I will always remember him as one of the best teachers I have ever had, and the one whose classes I enjoyed the most.

I can never thank my parents enough. Personally I think, parents are the most beautiful creation of Allah SWT, made to make sacrifices throughout their lives. My (late) mother gave me everything she possibly could in her short span of life. Had it not been for the hard work she put in my early learning stages, I would not have been able to reach this stage of my education. Also, had it not been for the taqwa she did her best to instill inside me, I would not have had all the strength within me. My father, whose sacrifices

I cannot even fathom. I shall never be able to do anything even near to equivalent to what he has done for me. I owe him everything that I have. He has been my greatest support and I cannot emphasize this enough.

I also want to thank my brother. I want to appreciate his kind and selfless nature. All the hours he spent driving me to (the very distant) NUST campus everyday and waiting for me outside till my classes would be over; means a lot, it does! My sincere du'as and wishes for his future and for the rest of my family.

Finally, there are these priceless and world's best friends I have been blessed with; Sarah Mahmood, Sadaf Faisal, Rabia Sultan, Zarmeena, Anum, Hafsa, Fareeha, and Munazza Syeda. They have been one of my greatest support; spiritually, morally and sometimes even technically :-).

Before ending this note, I want to be reminded of the fact (every time I open this book) that none of these people could have benefited me except that it was through the will of Allah SWT. It was Him who had been keeping His Eye of Mercy over me at every single step, removing every single hurdle from my path, inspiring me with ideas and skill for this research. *"And He taught Adam the names - all of them. Then He showed them to the angels and said, "Inform Me of the names of these, if you are truthful. They said, "Exalted are You; we have no knowledge except what You have taught us. Indeed, it is You who is the Knowing, the Wise." (Baqarah:31-32)*

Haleemah Zia

Table of Contents

List of Figures

List of Tables

Abstract

Information security risk management (ISRM) is the process that helps organizations improve their security posture by recognizing and dealing with all risks in an effective manner. It assists security practitioners in identifying critical assets, their vulnerabilities and subsequent threats in a systematic manner. It also builds an understanding of the organization's risk appetite while providing an effective way for educating the management about risks posed to their business and why they should spend on controlling them. Other benefits include improved security awareness within the organization and compliance to many legal and regulatory standards. Currently, there are various risk assessment/management methodologies in use by the industry. These methods ease the ISRM process for an organization by providing step by step tasks and activities and sometimes by providing worksheets and tools too. They provide guidelines and best practices and support organizations in complying with the required standards/laws in the most effective and efficient manner.

Our review of the ISRM literature revealed that much of the research in the past few years has been focused in either of the two directions: (1) comparing and evaluating these methods in an attempt to benchmark them so as to provide organizations a resource using which they may select one method from a pool of many; the one that suits their requirements and fits their context best (2) identifying deficiencies or limitations in these methods or problems that occur while practicing them along with potential solutions.

Regarding the first direction, researchers have performed the comparison not according to a standard criterion but with respect to different factors each time. A comprehensive solution in the form of well-categorized assessment factors was still lacking. As the first contribution of this thesis, we have proposed a framework, "RiskE4" that can be utilized for evaluating risk management methods and improvement techniques based on a structured criterion. RiskE4 constitutes a taxonomy of ISRM assessment factors and a table representing correlation among them. Every organization has certain priorities or limitations that dictate policies regarding their scope

for risk management. Based on those, they prefer risk management methods that suit their needs best. RiskE4 can help evaluate or categorize these methods in future, thereby enabling an easy pick and choose solution for risk practitioners. From a research perspective, it can help researchers evaluate any improvement techniques they propose for risk management. We believe that RiskE4 can create a paradigm for future studies on evaluation and comparison of risk management techniques.

With regards to the second research direction, solutions have been proposed in literature that have addressed one or more deficiencies. A holistic ISRM framework however, that covers all aspects of knowledge protection while sustaining the security of other IT assets was still missing. As the second major contribution of this thesis, we propose a framework called "IKOSST", with the objective to achieve significant improvement in ISRM processes all over the world. The major distinguishing features of IKOSST are (i) introducing collaboration with a knowledge center for improving accuracy of risk estimation and (ii) the inclusion of an extended RACI chart (RACI+) in the asset identification phase. While the first could not have been experimented for obvious limitations, the second has been evaluated by practically trying it out in two different organizations under limited scope. The risk assessment methods/formulas used in both case studies were different in order to demonstrate the framework's interoperability.

The results showed that several new critical assets were identified and threats and risks exposed through the inclusion of RACI+ activity. The framework is not standalone. Rather, it can simply be integrated with any risk assessment method that an organization has previously implemented. We believe that IKOSST can improve the granularity of asset and risk identification by a great extent and also pave way for achieving accuracy in risk assessment.

Chapter 1

Prologue

1.1 Introduction & Motivation

Information Security Risk Management (ISRM) is the process of identifying critical assets of an organization, analyzing vulnerabilities and threats associated with them, the impact of risks that emanate from those threats and determining justified solutions to mitigate those risks. In any public or private sector organization, ISRM ensures smooth running of business processes by reducing all perceived risks to an acceptable impact level. Organizations all over the world strive to enhance their security in order to avoid threats such as leakage of confidential data, intrusion into critical systems, stolen property and damage from natural accidents etc. Various technical, behavioral or strategic solutions can be used to mitigate some of these threats. The process of information security risk management (ISRM) helps analyze the most appropriate and cost-effective controls while providing compliance to many standards that mandate regular risk assessment [1]. These include PCI DSS (PCI Data Security Standard), FISMA (Federal Information Security Management Act), HIPPA (Health Insurance Portability and Accountability Act), SOX (Sarbanes Oxley Act) and ISO 27001 [2]. Currently, there are various risk assessment/ management methodologies in use by the industry. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) developed by the Software Engineering Institute (SEI) at the Carnegie Mellon University (CMU) [3], CRAMM (CCTA Risk Analysis and Management Method) [4] developed by the UK government's Central Computer and Telecommunications Agency (merged into OGC since April 2001) [5], NIST SP 800-30 [6], CORA (Cost-Of-Risk Analysis) developed by International Security Technology, Inc. (IST) [7] are some examples. In order to get compliance certifications, organizations follow standard ISRM practices

as laid down by (one or more of) these methodologies. In the past three years however, researchers have been identifying and publishing the dilemma of organizations being standards-compliant yet not considerably risk free. The reason for this is the presence of certain deficiencies that occur in the implementation of these risk assessment methodologies. Incomprehensive asset identification, inaccurate risk estimation or prediction and infrequent risk assessment are the major limitations identified in literature. Moreover, traditional ISRM methods do not incorporate risk assessment of knowledge assets and have been rendered unsuitable for the purpose.

While the mentioned deficiencies are currently being highlighted by various researchers, there exists no complete and technically approved solution that could adequately fill the gap. The need and importance of knowledge security has just been realized and research in this domain is currently in it's infancy. Researchers are proposing business-process based risk assessment in order to cater for knowledge assets. A holistic ISRM framework however, that covers all aspects of knowledge protection while sustaining the security of other IT assets is still missing. In this thesis, an improved ISRM framework is designed and trialled in two different case organizations. Two major aspects for knowledge security were incorporated in the proposed framework; the protection of competitively-sensitive data as well as client-confidential data from leakage and loss and the mitigation of risks associated with knowledge sharing (sharing of competitively non-sensitive data with the motivation to increase firm's productivity and efficiency, in the context of ISRM).

The framework will aid in security management programs of public and private sector organizations as well as educational institutions. Those that have assets or functions critical to security would be able to benefit. Organizations that already have a risk management process in place can determine the additional activities or change in course required. If the maturity level achieved during evaluation is superior to theirs, they could utilize this work for improvement. Organizations that do not have risk assessment method implemented would be able to use this one in order to enhance their security level and comply to relevant standards such as ISO 27001.

1.1.1 National Need

Pakistan needs to keep up with all other nations of the world in the field of information and technology. Assets within government or private organizations must be kept secure so that the country to be guarded from security risks of all nature. The introduction of a risk assessment framework, one that covers all previous gaps and is practical and economical enough to be implemented in organizations across the country, would help improve the

Figure 1.1: Components of ISRM defined in ISO 27001 Standard

overall security posture. By managing risks appropriately at the enterprise level, the country would be able to achieve better progress in the IT sector. Pakistan's overall status in the field of IT would be elevated.

1.2 Information Security Risk Management

Risk is defined by NIST as, "a measure of the extent to which an entity is threatened by a potential circumstance or event" [6]. Risk management, in general, is a complete process of identifying and quantifying risks so as to realize and minimize their impact to the best possible level. Four main objectives of ISRM mentioned in [8] are; risk identification, risk assessment, risk treatment and risk review. ISO 27000:2005 [9] defines a risk management process to be composed of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and risk review (Figure 1.1). NIST SP 800-30 [6] defines it in the form of risk framing (maps to context establishment of ISO standard), risk assessment, information and communication flows (risk communication in ISO), risk response (risk treatment and acceptance in ISO) and risk review.

In the context establishment phase, organizations are advised to define a clear purpose for implementing ISRM (such as legal compliance, preparing for business continuity etc), develop a strategy for responding to risks, determine their particular criterion for accepting risk and define the overall scope (functions or processes to be considered, identifying assumptions and constraints, threat sources or events to be considered etc).

Risk assessment is the major and most integral part of ISRM and is sometimes referred to as a whole process in itself (as information security risk assessment- ISRA). In ISO 27000:2005, risk assessment is divided into risk analysis and risk evaluation. Risk analysis is further divided into risk identification (the identification of assets, threats, existing controls, vulnerabilities and risk consequences) and risk estimation (calculating risk impact (severity of consequences in organizations; financial, on reputation, legal or

others) and likelihood (probability of occurrence) levels). In risk evaluation, the risks estimated in the previous step are compared to the acceptance criteria decided during context establishment. Two approaches utilized for risk estimation are qualitative and quantitative. Exact values are assigned in the latter approach whereas in the former, a range of estimated values are used to assign risk levels such as high, medium or low.

Risk treatment phase deals with the suggestion of response strategies which can be risk mitigation/reduction, risk acceptance, risk transfer or risk avoidance. Risk review involves monitoring the overall process afterwards for any changes in assets, threats or vulnerabilities and risk communication is about relaying the results to the decision makers and other stakeholders.

1.3 Aims and Scope

Security management is an exciting field with risk management being one of the major domains related to it. Organizations all over the world are striving to enhance their security in order to be safe from multiple existent and emerging threats such as cyber-terrorism, leakage of confidential data or intrusion into critical systems etc. Various technical, behavioral or strategic solutions can be used to mitigate some of these threats. For the overall security program of the organization to be cost-efficient, aligned to business motives and be managed in a systematic order, risk management processes play an integral role. The project aims to help the research community as well as the management of organizations improve their security programs. This would be achieved by not only making the ISRM more efficient, effective and comprehensive but also by integrating knowledge management security within the same process. To the best of our knowledge, the framework developed is the first of its kind.

Two main objectives have been achieved:

- **Objective 1:** Review of ISRM literature revealing researchers' interest in identifying deficiencies and areas of ISRM for improvement. Critical analysis of proposed solutions revealed the need for a more comprehensive solution and one that has gained confidence through practical experimentation as well. A framework with the name IKOSST is proposed that attempts to bridge the major deficiencies identified in literature. The framework is practically tested for validity.

- **Objective 2:** Review of literature to reveal the assessment measures that researchers have taken in order to evaluate ISRM approaches/methods. The literature study revealed that a comprehensive and intelligible

criterion was lacking. A taxonomy by the name "RiskE4" has been developed that categorizes ISRM methods' assessment factors and hence paves way for a standard assessment criteria.

No tool or development technique has been utilized in this thesis. The purpose of this research was to propose and practically experiment improvement activities within ISRM methods. IKOSST is not limited to any one particular method but it is a generalized technique that may be integrated with any method, whether automated through technical software solutions or not.

1.4 Research Contributions

The two major research contributions of our thesis are as under:

- A research paper entitled, **"RiskE4: An intelligible yet comprehensive framework for evaluating Information Security Risk Management Techniques"** is under review with Elsevier journal "Computers and Security" (at the time of writing this thesis document). Our contribution in this paper is twofold. First, we propose "RiskE4", a framework that comprises a taxonomy of ISRM requirements along with a discussion on correlation among them. The framework, we argue, can not only be used to categorize ISRM improvement areas but also serve as a baseline for comparing various risk assessment methods. Our second contribution stems from a profound literature survey of the techniques proposed for ISRM improvement and their analysis in accordance with the proposed framework. The techniques are also analyzed for their level of maturity, in terms of the extent to which they have been practically tested or the kind of processing required before they can be adopted by the industry.

- A research paper entitled **"IKOSST: An intelligence driven knowledge and information security risk assessment framework"** is under draft (at the time of writing this thesis document). In this paper, our contribution includes the proposition of an improved risk assessment framework named "IKOSST". We believe that IKOSST is a single solution to many major ISRM deficiencies identified in the past. It enhances ISRM effectiveness manifold while affecting efficiency only slightly. IKOSST proposes the inclusion of an extended RACI activity in the asset identification phase. Experimentation revealed significantly

positive results. While the activity consumed maximum two-three extra hours, it improved the understanding and granularity level of risk identification process significantly. The second integral part of IKOSST is the inclusion of a knowledge center (KC) that works on the principles of cyber threat intelligence. KC aims to collect and propagate intelligence related to emerging threats and attacks thereby improve accuracy in ISRM.

1.5 Limitations

In order to limit the extent of this work, we have confined our research from several aspects:

- Risk assessment has been performed in two separate organizations but the scope has been kept limited to few processes each. Furthermore, the experimentation performed in Govt-Sector Organization (named "GreenCo" in this document) is limited by the rules and regulations, project timelines of the organization's enterprise wide ISRM project spanning of two years.
- A taxonomy of assessment factors has been proposed. It is foreseen as a first step towards categorizing different ISRM methods (such as OCTAVE, CRAMM, Mehari etc.) so that organizations may be able to pick and choose with confidence, one that matches their needs best. Major ISRM improvement techniques have been evaluated according to RiskE4. A thorough comparison however, of standards using RiskE4 was out of the scope of this work. How the framework may be utilized and built upon for setting standards in future, has been mentioned under "Future Work" in Chapter 7.
- Some strategic suggestions have also been incorporated within the IKOSST framework. Their nature is such that even after practical enforcement in any particulate organization, results would not be evident until ten years of enforcement. These could not have been practically tested, so their scope has been kept limited to theoretical claims and evaluation.

1.6 Thesis Organization

This document comprises of five chapters. Moreover, the thesis constitutes of six documentation-based deliverables. Three of these have been provided as part of Appendices while the other two (which contain the risk assessment

results of the two organizations) have been left out due to their sensitive and confidential nature. A brief outline of the six chapters and each Appendix is provided below.

- *Chapter 2* discusses our first research contribution i.e. the framework proposed (RiskE4) based on several assessment factors found in the literature for evaluating any ISRM method, approach or technique. This chapter is intentionally kept in the beginning as the literature review is evaluated based on RiskE4.

- *Chapter 3* acknowledges the work of previous researchers in this domain. It provides a discussion and critical analysis of the research performed in the past few years, found in the literature. he chapter also presents an evaluation of some of the major improvement techniques proposed in the literature, in the recent past. The evaluation is performed according to RiskE4.

- *Chapter 4* presents the research methodology undertaken over the course of this thesis. The chapter discusses the systematic process utilized in order to achieve the objectives under different phases of the research.

- *Chapter 5* discusses the case studies of two organizations used for the purpose of testing the proposed framework IKOSST. It gives a brief introduction of the two organizations and the methodology used. It introduces our second major contribution of the thesis.

- *Chapter 6* discusses the results of IKOSST experimentation, its evaluation and validation.

- *Chapter 7* concludes the work and gives discusses possible future directions.

- *Appendix A* provides the first deliverable of our thesis, the Specification Report for IKOSST. This report explains the framework while describing each step.

- *Appendix B* provides the second deliverable of our thesis, the User Manual for the ISRM Method used in the first case study.

- *Appendix C* provides the third deliverable of our thesis, the User Manual for the ISRM Method used in the second case study.

Chapter 2

Assessment framework for ISRM Methods

2.1 RiskE4:An intelligible yet comprehensive framework for evaluating ISRM Techniques

Various standard ISRA/ISRM methodologies exist that can be utilized by security professionals planning to enforce risk management in their organizations. Recently, there has been a debate in the literature about identifying, realizing and bridging the limitations that exist while practically implementing any of these methodologies. Attempts to improve ISRM either theoretically or practically have been made from different perspectives. In this context, a fine-grained criterion for evaluating ISRM could help identify the major areas of concern that have been studied recently and others that haven't. Moreover, such a criterion could help industries determine their priorities and potential areas for improvement. Research in the previous few years has focused on improving ISRA/ISRM from different aspects. In our research, we propose a framework, "RiskE4", for assessing an ISRA/ISRM method. The framework is composed of two components: a taxonomy based on 4E's (Effectiveness, Efficiency, Economy and Ease of use) and a correlation table. Each of the two is described in a separate subsection below.

2.1.1 The taxonomy

The taxonomy for evaluation criteria is illustrated in Figure 2.1. The root node is labeled with the objective of this taxonomy i.e. assessing an ISRA method. Level 1 nodes (just below the root node) mention each of the 4 E's while level 2 nodes (just below level 1 nodes) list the determining factors for

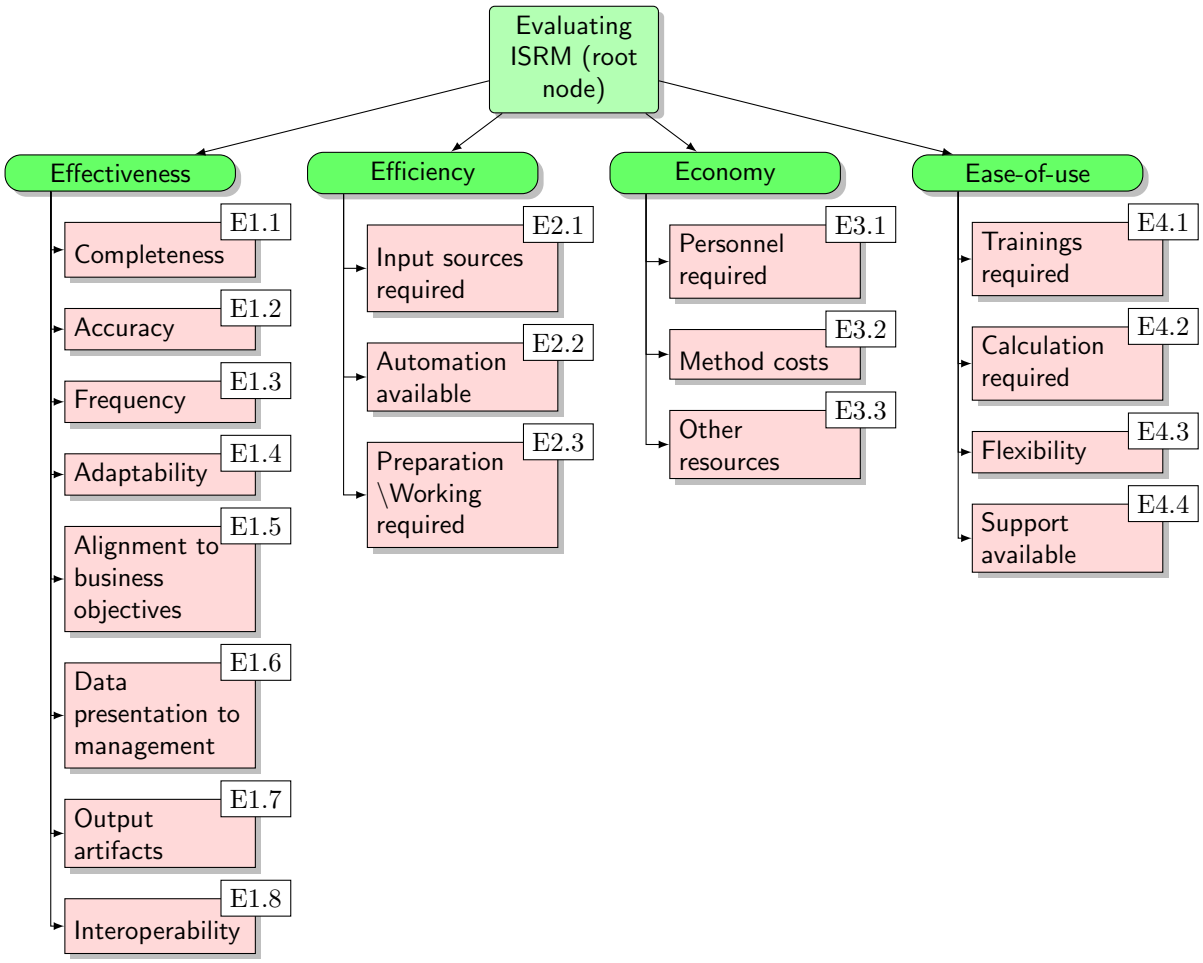

Figure 2.1: RiskE4 taxonomy: Evaluation criteria for ISRM method

each of their parent node (one of the four E's).

2.1.1.1 E- 1 Effectiveness:

Organizations with sensitive assets, where security is one of the most critical issues, would need a risk management process as effective as possible. Government organizations such as those belonging to defense or health sector as well as private sector companies with highly confidential data (either client-confidential or competitively sensitive citeahmad2014protecting) would fall in this category. There are several factors on which the *effectiveness* of any risk management method may depend or through which it may be deter-

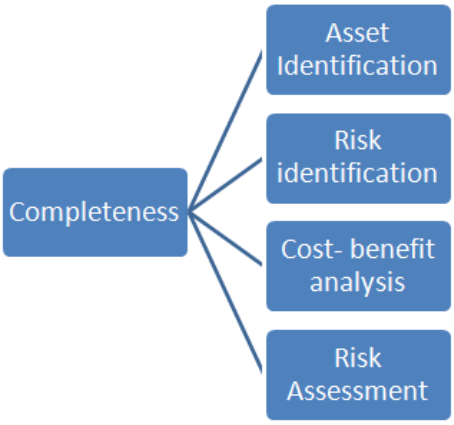

Figure 2.2: Four aspects for completeness of ISRM

mined. Each of these is described below:

E- 1.1 Completeness: We define an ISRA method's completeness with respect to four major steps which are asset identification, threat identification, cost-benefit analysis and overall risk assessment (figure 2.2).

Asset Identification: There has been a significant discourse in literature with regard to completeness of asset identification. Research [10, 11, 8, 12, 13] has pointed out that asset identification process in current methods is not rigorous enough. Whereas the identification process of technical and physical assets also needs to be enhanced, researchers have emphasized much over the lack of knowledge assets' identification [10, 11, 12]. Knowledge is defined in literature as "a fluid mix of framed references, values, contextual information and expert insight" [14] and it is generally categorized as either tacit or explicit knowledge. Explicit knowledge is the one that can be codified such as in reports or manuals etc. Tacit knowledge is not codified however, and resides in people either in the form of ideas or skills. [12] point out that tacit knowledge can be of two forms, individual or distributed. Organizations that deal with sensitive information need risk management method to effectively address tacit knowledge security. Information may get leaked either deliberately by disgruntled employees or accidentally by retiring employees, employees moving to other companies or through inexperienced employees who lack maturity and may leak information in informal communication.

An ISRA method's completeness would therefore depend on the type of assets that it considers for assessment. The more the assets that can be identified utilizing a certain method, the more effective it would be.

Risk Identification: For a risk management method to be an effective

one, the risk identification must be complete in the sense that it should cover all threats/ threat scenarios and vulnerabilities for any particular asset. Confidentiality, integrity or availability of any one particular asset may be exploitable in a number of ways and some of these might even be unprecedented. An effective risk management process would attempt the recognition of as many threat scenarios as possible. Moreover, any risks due to complex relationships amongst assets, emerging risks (new risks being identified out in the wild) and any complex attack scenarios would also need to be identified [8].

Cost-benefit Analysis: An effective risk management method would also be complete with regard to the cost-benefit analysis. This refers to balancing the risk mitigation strategies with the costs required for their enforcement. This cost may not be just financial. For instance, knowledge sharing in organizations is encouraged at large [15, 16, 17] but it can result in leakage of sensitive information as well. Applying mitigation strategies for leakage, such as keeping knowledge deliberately tacit or reducing its sharing would diminish the benefits that were perceived for knowledge sharing [10]. An effective risk management method would consider all these factors and attempt to balance the benefits perceived from the activity through which risks can emanate with all financial or operational costs needed in order to mitigate them.

Risk Assessment: Finally, an effective risk management method would be complete if it addresses all steps necessary to reach (technically) sound conclusions. Different steps involved in an ISRM method have been mentioned in Chapter 1. A method's completeness may be assessed by considering its approach to all those steps i.e. whether all have been addressed or not and to what extent.

E- 1.2 Accuracy: We define accuracy of an ISRA method with respect to four major steps; asset identification, risk identification, cost-benefit analysis and risk estimation (figure 2.3).

Asset identification, risk identification and cost-benefit analysis: These three factors were described under the requirement of them being complete in E1.1. It is imperative however, that an effective ISRA would not just identify maximum assets, risks and cost-benefit factors but accurate ones as well. This implies that assets identified would be those that do require risk assessment. Vulnerabilities, threat scenarios and hence risks identified would actually exist for that particular asset and finally the costs identified would also not just be complete in their nature (analyzed from all angles) but be accurate as well.

Risk Estimation: This refers to the method's accuracy in calculating risk likelihood and impact. Research [8] points out that the risk assessment

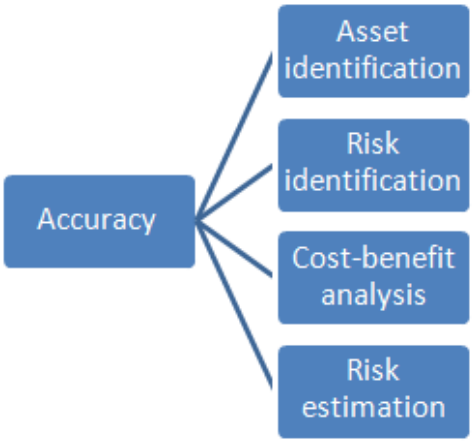

Figure 2.3: Four aspects for accuracy of ISRM

in current methods is based on inaccurate estimates rather than accurate predictions derived from evidence. Risks cannot be predicted with utmost certainty but an effort to make estimates as accurate as possible is required for the overall assessment process to be effective.

E- 1.3 Frequency: An ISRM enforced in any organization would also need to be updated, reviewed and monitored at frequent intervals. In-fact, ISO 27005 and NIST SP 800-30, both define the monitoring or reviewing process within the ISRM cycle as an essential component. An effective ISRM process would therefore be one that employs some strategy for necessitating effective reviewing and monitoring as well.

E- 1.4 Adaptability: As mentioned, ISO and NIST standards suggest risk management to be performed frequently with all necessary updates incorporated in the latest cycle. An organization that plans to have an effective risk management in place would need to monitor and review it at frequent intervals. However, the volume or nature of security requirements may change with time. New assets, vulnerabilities or threats may evolve. For instance, new machines or new software management systems may get introduced in a hospital. A manufacturing company may launch new products or cease to produce old ones. New competitors may emerge for a telecom vendor. All these factors mean changed security requirements. An effective ISRA method would be one that adapts easily to all such changes without requiring too much time or resources. The initially enforced process would have the ability to be tailored according to changing needs.

E- 1.5 Alignment with business objectives: Whereas security would be a major concern for many organizations, none of them would still be willing to compromise on a shift or detriment to their mission statement. An effective risk management method would therefore be one that keeps security in alignment with the business objectives [18].

E- 1.6 Data presentation to management: The findings and controls suggested by the ISRM team must be presented in an effective manner to the management so that the latter may understand the significance of required actions; why they are necessary and to what extent [9]. Some methods provide report formats that the ISRM practitioners may utilize while presenting their findings to the management. The better the presentation, the more effective would be its impact in convincing the management for the enforcement of required controls.

E- 1.7 Output Artifacts: An ISRM method that necessitates complete documentation is likely to be more effective in the long run. Lessons learnt from one cycle (review cycles as discussed under E- 1.3 and E- 1.4) can be utilized and acted upon in the next one if complete documentation is developed at that time. Also, the more structured and systematic the documentation, the easier it would be to utilize in future. For instance, reports supported by visual representations, figures, tables or structured worksheets maintained during the process would be more effective compared to ones comprising just lengthy text.

E- 1.8 Interoperability: An ISRM method that integrates well with other business or security solutions would increase the benefits it provides to the organization. For instance, an organization enforcing ISRM might already have COBIT (Control Objectives for Information and Related Technology [19]) deployed for IT governance or ITIL (Information Technology Infrastructure Library [20]) for service management. A method that does not disturb the other functions of an organization or is able to leverage them for itself is termed interoperable here. The overall security program would be bound together and aligned in an effective way.

2.1.1.2 E- 2 Efficiency:

Efficiency or time required is one of the areas where any risk management method would be evaluated or be required to be improved upon. Some organizations might require ISRM to be fast so that personnel or other resources are engaged for as little time as possible (so that they can get free to perform

other business tasks). Others might require results as quickly as possible within limited time. They may require achieving compliance or improving their security posture before a certain deadline based on their business needs. In this regard, it is vital that the efficiency of an ISRM process be assessed. Factors that determine efficiency of a particular risk management method are described below.

E- 2.1 Input sources required: An ISRM process always requires input information about assets, vulnerabilities and threats etc. Information may be obtained from two main sources: documents or people. If the process demands information from sources easily accessible, such as freely available organizational documents, it would be relatively fast to obtain, making the overall process more efficient. On the other hand, a process that requires information from people is likely to have delays as dependency on stakeholders' availability would be introduced. Information required from external stakeholders (stakeholders from outside the organization) would mean further delays. Also, an organization that has not established complete, easily understandable and effective documentation or has not made it easily accessible to employees might need to avoid an ISRM method that depends too much on information obtained from such documentation.

E- 2.2 Automation Available: A method supported with automated tools is likely to help the risk practitioner speed up the process. Tools may be able to suggest asset, vulnerability or threat lists, suggest which risks may emerge from a particular threat source or help calculate probabilities/ likelihoods. Reducing manual work from all these or other tasks would help achieve quick results.

E 2.3 Preparation/Working Required: The amount of planning required while enforcing ISRM may also vary with different methods. We categorize these into strategic, technical or operational, each of which are briefly described below.

Strategic (before beginning ISRM): A method may require revision in policies or significant management support before beginning the process.

Technical (before beginning ISRM): Requirement for any software installations or configurations, workstation setups etc would come under this category.

Operational (before, during or after ISRM): Some methods require interviews or survey questionnaires for risk assessment. In this case, practitioners would need to prepare questions in accordance with their organization's scope and context. Methods that require complex workarounds or calcu-

lations, greater details of risk assessment steps or preparation of extensive documentation would likely be slower than those that do not.

2.1.1.3 E- 3 Economy:

An organization would always need to set aside a certain budget for the implementation of ISRM. Added security is usually perceived as a cost burden by business managers [21]. Depending on the nature of business and its security requirements, some managers would be looking for an ISRM method that demands the least financial budget. It should be noted that the expenditure being considered here is only the one necessary for ISRM implementation (such as buying proprietary tools, having to pay for specialized staff etc) and not the one that occurs later for the mitigation of risks.

Factors involved in determining how economical an ISRM method is, are described below.

E- 3.1 Personnel Required: Depending on the steps or complexity involved, different methods' requirement for staffing could be different. The more the employees required for the activity, the more it would cost the organization. Moreover, the need for extensively trained practitioners or those with specific specializations (requirements such as IT knowledge, security knowledge, business knowledge etc) would further increase the cost burden. Some tools also necessitate the involvement of external experts. For instance, authors of [22] mention that OCTAVE requires the utilization of internal staff only but CORA [7] requires external risk experts.

E- 3.2 Method Costs: The method itself, the tools that support it or the documentation required for its understanding may not be free of cost. Some methods such as OCTAVE Allegro are completely free to use whereas others such as CRAMM require payment for tools as well as supporting documents.

E- 3.3 Other Resources: There may also be a requirement for other proprietary tools or any software to be used with the method. Utilization of other business resources may also vary with different methods. Some methods may require more workstations compared to others. Requirement for extensive hard copy output (e.g. in CRAMM full review cycle [5]) would also raise the costs accordingly.

2.1.1.4 E- 4 Ease-of-use:

This is another factor on which an ISRM method may be assessed upon. An organization that does not have trained or experienced practitioners nor is it willing to afford them for one or more reasons, would be interested in a method known for its ease of understanding. Accordingly, this would also be one of the areas on which existent risk methods may be improved upon in future.

Factors that may determine how understandable or simple to use any particular method is, are briefly discussed below.

E- 4.1 Trainings Required: A method that requires practitioners to first get trained about the steps involved or the methodology utilized would not be understandable in its true essence without those trainings. It is to be noted that, trainings or experience mentioned here are those required specifically for the purpose of learning the usage of the method/ tool and not the ones required for a general understanding of ISRM. The latter is a determining factor (E- 3.1) of economy.

E- 4.2 Calculations Required: Some methods are based on complex formulas for calculating risk impact, likelihood, costs etc. Others are based on easy or simple ones. For instance, authors of [22] mention that in order to calculate expected loss value, OCTAVE uses no mathematical calculations but a simple expected value matrix whereas ISRAM (Information Security Risk Analysis Method [23]) uses a very complicated formula. Usually quantitative risk methods would require more calculations compared to qualitative methods but even within quantitative ones, the level of complexity involved may vary.

E- 4.3 Support available: The amount and type of support available for a risk method would significantly impact its usability. Detailed, step-by-step usage guidelines provided in simple language would increase the usability of a method. Moreover, some methods come with support in more than one language. For instance, CRAMM is available in English, Czech and Dutch languages [4]. Support additional to just the basic manual shall further positively impact usability. For instance, CORA's system software license includes a telephone Help Desk facility as well as an on-site start-up support. (Both of these are licensed but here we discuss usability exclusive of any other requirement such as economy.)

E- 4.4 Flexibility: A method that can be tailored according to varying

		Brings an increase (↑) or decrease (↓) in:			
		E1	E2	E3	E4
An increase of	E-1.1	↑	↓	↓	↓
	E-1.2	↑	↓	↓	↓
	E-1.3	↑		↓	
	E-1.4	↑			
	E-1.5	↑		↑	
	E-1.6	↑			
	E-1.7	↑	↓	↓	
	E-1.8	↑		↑	
	E-2.1	↑	↓	↓	
	E-2.2	↓	↑		
	E-2.3	↑	↓		↓
	E-3.1			↓	
	E-3.2			↓	
	E-3.3			↓	
	E-4.1		↓	↓	↓
	E-4.2	↑	↓		↓
	E-4.3	↑	↑		↑
	E-4.4	↑	↑		↑

Table 2.1: Correlation Table: Showing effect of all factors

needs of different organizations is here referred to as a flexible one. Some methods provide such flexibility within them and hence organizations can use them according to their scope or context. For instance, CRAMM gives the options for full or rapid reviews. An organization may utilize full review option while implementing it for the first time and then rapid reviews for some of the regular reviews. This makes the method more usable overall. Other examples could be flexibility in worksheets (e.g. OCTAVE provides the options for user-defined fields and sheets as well) or tools (e.g. user may add threat scenarios to the lists provided by a tool).

2.1.2 The correlation table

The factors discussed above may not just have an effect on only one of the requirements (one of the four E's) but on others too. An increase in any one may bring an increase or decrease in other three E's as well. In Table 2.1, we have illustrated these interdependencies. An increase in one control factor (mentioned in left most column) is analyzed for its effects on other E's (e.g. what would be the effect of increasing completeness on efficiency, economy

and ease-of-use). For factors where a confident judgment was not possible, the fields have been left blank. The effect of each individual factor on the three other 'E's is explained below (excluding the parent requirement) e.g. E1 is the parent requirement for E- 1.1, so the latter's effect on E2, E3 and E4 is explained in this section. Its effect on E1 has already been explained in section 2.1.1.

2.1.2.1 Effect of Effectiveness factors on Efficiency, Economy and Ease-of-use (E-1.X → E2, E3 and E4):

- E- 1.1: The more comprehensive an ISRM method is, the slower would it be, the more the costs involved and lesser the usability. It would take in more input information, require more processing and an understanding of all factors involved (different assets, threat scenarios etc). Downward arrows, displaying decrease of E2, E3 and E4 are hence shown in the table.

- E- 1.2: Accuracy would also be increased by utilizing more input sources, expert practitioners and complex formulas. All these are factors that decrease efficiency and usability and increase the financial burden (specialized or trained practitioners required for using complex calculations). Downward arrows, displaying decrease of E2, E3 and E4 are shown in the table accordingly.

- E-1.3: More frequent reviews would increase the cost requirement. Downward arrow for E3 is shown in the table, accordingly. Its effect on E2 and E4 is not completely discernible, as depicted by the empty fields in the table.

- E- 1.5: The techniques proposed for increasing ISRM alignment with business objectives are based on enhanced business process documentation [24] and the utilization of business process models for asset identification [25]. Development of such models or documentation is likely to increase costs, even if on a small scale. An arrow showing increase of E3 is shown in the table accordingly. The blank fields for E2 and E4 are a depiction of the fact that confident judgment on the effect of E- 1.5 on efficiency and usability is not possible. These may only be realized by experimenting with the techniques in practice and observing their effect.

- E- 1.4 and E- 1.6: Concrete analysis of the effects of increased adaptability, better presentation of results to management on efficiency, economy and ease-of-use is not possible. It would depend on the techniques utilized and their effects as observed in practice. As such, no techniques for these two factors were found in the literature from past three years at least, making the analysis difficult to be performed. The fields have therefore been left blank in the table.

- E- 1.7: Time and cost would both be required in order to develop output artifacts. Effect on usability is not definite as it would depend on the methods' ways of helping develop the artifacts (report templates, worksheets etc). The table has been filled accordingly i.e. decreased E2 and E3 and a blank field for E4.

- E- 1.8: The technique proposed in literature for enhanced interoperability is the same as that for enhanced alignment with business process objectives. Analysis is therefore similar to that performed under E- 1.5.

2.1.2.2 Effect of Efficiency factors on Effectiveness, Economy and Ease-of-use (E-2.X → E1, E3 and E4):

- E- 2.1: Collection from a greater number of input sources is likely to increase effectiveness as a better assessment could be made when information from various sources is available. It can increase completeness and accuracy of ISRM. However, it may decrease its usability since the practitioner would need to understand the requirements from different sources and comprehend all the information collected in varied forms. A concrete judgment about its effect on cost cannot be made as it would depend on the nature of sources. The table has been filled accordingly i.e. increase and decrease of E1 and E3 respectively and a blank field for E4.

- E- 2.2: Automated tools to increase efficiency would most likely be at the cost of decreasing its effectiveness (as depicted by the downward arrow in table, for E1). Not everything can be automated so some compromise in decreasing the granularity of the process would be there. Also, greater amount of human control and supervision can help tailor a method to the organization's context. The effect on usability and economy would depend on the complexity and cost of the tool respectively. Hence the fields for E3 and E4 have been left blank in the table.

- E- 2.3: Preparations for better strategic solutions, interviews or questionnaires are expected to increase ISRM in effectiveness but decrease its usability. Complex formulas would make the estimates more accurate but such formulas and calculations involved would require greater understanding as well. E1 is therefore shown to increase whereas E4 to decrease, in the table. Financial requirements may or may not be there hence no solid judgment is provided for economy, leaving a blank field in the table for E3.

2.1.2.3 Effect of Economy factors on Effectiveness, Efficiency and Ease-of-use (E- 3.X → E1, E2 and E4):

- E 3.1, E3.2 and E 3.3: The effect of all four economy factors on efficiency, effectiveness and ease-of-use is not plainly deducible as it would vary from scenario to scenario. For instance, extensive hardware or software involved may or may not affect effectiveness as it would depend on the nature of its usage. Similarly, its effect on usability is also not definite as it would also depend on the type of technology involved or its complexity. Similar reasoning applies for other three economy factors as well.

2.1.2.4 Effect of Ease-of-use factors on Effectiveness, Efficiency and Economy (E- 4.X → E1, E2 and E3):

- E- 4.1: Tools or methods that necessitate training for their understanding would require more time and finances for such trainings hence a decrease in efficiency and economy is seen (as shown by downward arrows for E2 and E3). Effect on E1 is not definite as the training being considered is specifically for the usage of the method and might only be required because of the complexity of the method. Other simpler methods may be utilized with equal amount of effectiveness and without requiring any training. The field for E1 has been left blank accordingly.

- E- 4.2: Complex calculations involved are expected to increase accuracy but require greater amount of time. Therefore, an increase in effectiveness (E1) and subsequent decrease in efficiency (E2) is shown in the table. The field for E3 has been left blank since the impact

on cost would depend on the type of calculations. If they require any equipment or software that is of monetary value, then an increase in E3 would result. But this might not be necessary, depending on the type of working mandated by the method.

- E-4.3: Increased flexibility may increase efficiency as the method could be tailored according to requirement and with ease, without extra working required (upward arrows for E1 and E2). Its effect on effectiveness and cost is not definite (blank field for E1 and E3).

- E- 4.4: Greater amount of available support would help the practitioners deploy the method in true essence, thereby increasing effectiveness. It would also reduce the complexities involved in understanding and hence increase the efficiency. Effect on cost would depend on the way the support is being provided (e.g. charged telephone help desk facility or free on-line chats). The field for E3 has therefore been left blank.

  It can be discerned that the factors that improve effectiveness decrease efficiency and make the process more costly and difficult to be used. Those that enhance efficiency reduce effectiveness but decrease costs and increase usability as well. Wherever usability is increased, efficiency increases and the method is expected to become more economical but less effective. There are only two anomalies to this occurring at E- 4.3 and E- 4.4; greater support and flexibility increases usability but is likely to increase effectiveness as well. Overall, it may be said that efficiency, economy and ease-of-use are directly related to each other and inversely to effectiveness.

Chapter 3

Literature Review and Analysis

3.1 ISRM Improvement Techniques

In the past three years, there has been significant discourse in literature with regard to improving the current IRSM methods. It is evident that the solutions proposed target ISRM improvement by focusing on one or few of the assessment factors described in the taxonomy of "RiskE4" framework. In our research, we analyze how other factors within the taxonomy could also be affected. Moreover, solutions that present an exploratory study have been categorized as a hypothesis; those that entail abstract level flow of activities as theoretical models, and those that describe detailed steps for enforcement in an organization as a practical framework. This categorization translates to the amount of processing required before the proposed techniques can be adopted by organizations. Practical frameworks may be adopted as such or after thorough testing. Theoretical models would first need to be mapped on to step-by-step methodologies in order to provide a systematic ISRM process. Practical testing may then prove helpful, before officially introducing the method to the industry. For proven hypothesis however, further study would be required in order to explore the techniques that may support them. It therefore follows that techniques categorized as practical framework require the least processing and hypothesis the most, before they may practically be availed by the industry.

The overall criterion is illustrated in Figure 3.1 and a summary of the findings from ten major publications is presented in Table 3.1. An overview of these publications along with a brief mention of their analysis (from Table 3.1) follows.

Authors of [8] point towards three deficiencies of current ISRM methods: (1) consideration of inadequate risk sources, (2) inaccurate risk assessment

Improvement technique	Primary factor	Others that may be affected	Level of study	controls involved	Testing
A situation awareness model for information security risk management [8]	E-1.1, E-1.2, E-1.3	E-2.1	Theoretical Model	Strategic, Operational	None
Genre-Based Assessment of Information and Knowledge Security Risks [11]	E-1.1		Practical Framework	Strategic, Operational	Practically
Incorporating a knowledge perspective into security risk assessments [12]	E-1.1	E-1.5, E-2.1, E-2.3	Hypothesis	Strategic, Operational	None
Information security risk assessment: towards a business practice perspective [13]	E-1.1	E-1.5, E-2.3	Hypothesis	Strategic, Operational	None
A holistic risk analysis method for identifying information security risks [26]	E-1.1	E-2.3	Theoretical Model	Strategic, Operational	None
An integrative model of information security awareness for assessing information systems security risk [27]	E-1.2	E-1.5	Hypothesis	Strategic, Operational	Theoretically (through survey questionniares)
Using Business Process Model Awareness to improve Stakeholder Participation in Information Systems Security Risk Management Processes [24]	E-1.2	E-1.5	Hypothesis	Strategic, Operational	Theoretically (through interviews)
Overview of Enterprise Information Needs in Information Security Risk Assessment [28]	E-2.1	E-1.1, E-1.8	Hypothesis	Strategic, Operational	None
An extension of business process model and notation for security risk management [25]	E-1.5	E-2.1, E-1.8	Hypothesis	Strategic, Operational	None
Developing contextual understanding of information security risks [29]	E-1.2	E-2.3	Hypothesis	Strategic, Operational	Practically
A data-driven assessment model for information systems security risk management [30]	E-1.2		Theoretical Model	Strategic, Operational	Practically

Table 3.1: Analysis of improvement techniques proposed in literature

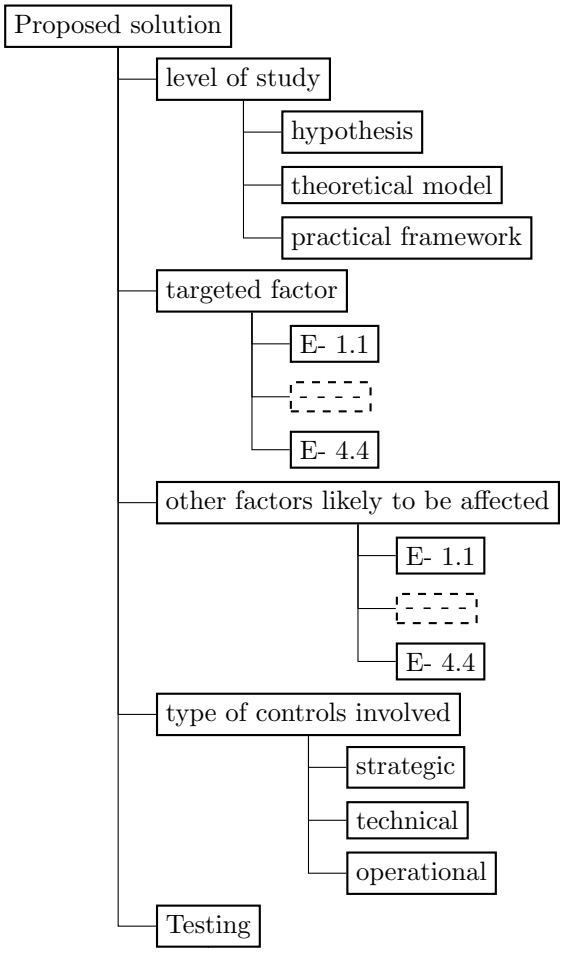

Figure 3.1: Criteria for analyzing improvement techniques from the literature

based on assumption rather than evidence, (3) infrequent follow ups. They propose a Situation-Awareness based Information Security Risk Management (SA-ISRM) model. How effectively their proposed model gaps the mentioned deficiencies however, can only be realized once it has been tested practically. The model has certain limitations which if realized in practice, would bring back all the mentioned deficiencies. For instance, if the decision maker is vague about his requirements, critical information is not accessible or the collection process is not systematic, the first two deficiencies would still remain. The authors claim the removal of the third deficiency by the fact that their SA-ISRM process requires timely feedback by the decision-maker. However, this also depends on the competency of the decision maker, the efficiency of the whole process (which depends on many factors such as the

provision of information from external or internal stakeholders), the extent to which the decision maker is bound to follow the process and how effectively the analysts consider his feedback and apply it to the next cycle. From the taxonomy of RiskE4, the proposed model is to enhance completeness (E-1.1), accuracy (E-1.2) and frequency (E-1.3). Continuous feedback mechanism and collection from various sources in the model, may affect E- 2.1 negatively.

Authors [11] point out that the current risk assessment methods do not identify and assess knowledge assets. As a solution to this (E- 1.1 from taxonomy of "RiskE4"), they propose a model in which they adopt a genre-based method (GBM) for identifying knowledge assets in an organization. They integrate it with the Octave-Allegro (OA) method for risk assessment and mitigation steps. The GBM approach that they propose begins by first defining stakeholders for the overall process. Risk areas and scope are then prioritized and producers and output of information identified. As a fourth step, they categorize knowledge assets into "kinds/types/genres". Developing genre properties, identifying genre containers and performing risk mitigation constitute the fifth, sixth and seventh steps respectively. Researchers of [10] improve the same model by adding cost-benefit analysis and incorporating business perspective. Neither of the two approaches however, don't give separate consideration to tacit knowledge assets. Tacit knowledge is not coded but can still be lost or leaked by changes in human resource or by social engineering attacks [31].

Researchers [12] discuss the importance of securing knowledge assets and the unsuitability of the current risk identification methods for this purpose. They define tacit knowledge as one that can reside in people's minds (individuals or collectively in groups/teams), in materials and in processes. In their study, they have applied OCTAVE-S to a company and found that the method does not successfully identify knowledge assets. The authors propose that knowledge be identified through a business-process based approach whereby interviews are conducted with the relevant staff. Core knowledge could be identified by analyzing business processes. Securing tacit knowledge would be a challenge in itself as coding all knowledge (even non-confidential) might not be possible due its complex nature. The research targets completeness in ISRM (E- 1.1) but can be expected to increase alignment with business objectives as well (E- 1.5). Also, preparation would be required for interviews (E- 2.3) and the input requirements may also increase (E-2.1).

Researchers [26] discuss the limitations of traditional ISRA methods. While the latter are popular (their expertise easily available), widely accepted and rich tool-supported, they do not consider people and processes as assets. The holistic ISRA method that they propose attempts to include

people, processes and information. The method consists of ten steps. Core business functions, critical business processes and critical information systems are identified in the first two steps. In the third step, an architecture diagram helps identify supporting infrastructure and develop a list of assets while a data flow diagram (DFD) specifies users, processes and information flows in the fourth step. The DFDs identify confidential information in the fifth step, based on which the list of IT assets is updated in the sixth. In the remaining steps, values of assets are determined, risk scenarios predicted, threats and vulnerabilities identified and impact estimated. Detailed steps for practically enforcing the technique are not given however, neither is the approach evaluated in any form. Also, tacit knowledge assets are once again not considered. The proposed model attempts to improve ISRM through enhanced asset identification (E- 1.1) but since data flow diagrams for business process are used, it can be expected to increase alignment with business objectives (E- 1.5) as well. The diagrams would need to be prepared, hence affecting E- 2.3.

The limitations of traditional ISRA methods are also discussed by authors of [13]. These methods hold a very technical view of information assets and hence fail in identifying other intangible assets, the authors claim. Even the business process approach [26], which aims to improve the collection process and identify an organization's critical knowledge assets would not consider informal / unofficial copies of assets such as those made during daily office activities of photocopying, transferring to USBs, emailing or taking print outs etc. Risks can emerge depending on how knowledge is applied and used in the course of a business process. The business practice perspective proposed in this research is based on interviewing employees so as to identify their day to day activities and how any of them can produce assets or copies of assets. The interviews would include questions related to employee's knowledge requirement. Once again, the main objective is to enhance completeness (E-1.1) but E- 2.3 is likely to be affected as well due to reasons discussed earlier.

The research article [27] is about the positive impact of increased security awareness on the assessment of security risks on an organization. Authors classify security awareness into technical knowledge, organizational impact and attacker assessment. Technical knowledge comprises knowledge about the design of malicious attacks and the existence of system vulnerabilities. Organizational impact is related to knowledge about criticality of different assets and the impact of risks on the organization. An understanding of attacker motivations and behavior (methods used for exploitation) falls under the third category, "attacker assessment". A review of the literature led them to four hypotheses (H1-H4). H1-H3 state that knowledge of the three mentioned domains enhances security awareness whereas H4 asserts that the lat-

ter further leads to a better assessment of security risks. Receiving responses to survey questionnaires from 428 IS practitioners and applying statistical tests to them, validated all four hypotheses. The authors also found out that awareness of organizational impact and attacker profile benefits ISRA more as compared to technical knowledge. The research points out the need for increased organizational and security related awareness in order to improve ISRA/ISRM but does not explicitly explore ways to achieve this. The objective is to increase accuracy of assessment (E- 1.2) but with greater organizational knowledge, the process can be better aligned to business objectives as well (E- 1.5).

Authors of [32] investigate the effect of stakeholders' awareness of business process model on an ISRM. They interviewed five stakeholders, assessed their knowledge of business processes and then asked them about their involvement in ISRM of the organization. Their findings led to the development of four hypotheses: (1) stakeholders with complete awareness about business processes contribute positively to risk analysis, (2) any stakeholder unaware of a certain business process would use his knowledge about another business process, which in his view would be related to it, (3) stakeholders' awareness of business process documentation greatly impacts their contribution in ISRM and (4) selection of stakeholders must be based on the above three in order to increase the process in completeness and efficiency. The researchers conclude that organizations must strive to make business process artifacts more comprehensive and available to all stakeholders. They also suggest that security risk analysis results be included in these documents so that stakeholders involved in ISRM for the first time can also make use of lessons learnt from previous ISRM processes. The proposed hypotheses are for achieving better accuracy in ISRM (E- 1.2) but increased awareness of business process documentation would also help increase alignment with business objectives (E- 1.5).

The relationship of a certain Enterprise Architecture (EA) model (ArchiMate) with different ISRA methodologies is studied by authors of [28]. The authors argue that alignment between ISRA methods and EA Framework can reduce the costs involved since much of the information required for ISRA can be gathered from other parts of an IT governance framework. They studied input information required by 12 risk assessment methodologies and mapped them to concepts in ArchiMate, in order to explore the extent to which the latter may aid ISRA. The authors conclude that most of the concepts do relate with ArchiMate and hence EA documentation could serve as a valuable source of identifying assets in ISRA. The model was proposed to increase efficiency by reducing input collection sources (E- 2.1). It may however, negatively impact completeness (E- 1.1) as all assets might not be

identified through EA. The approach could especially miss out tacit knowledge assets. Interoperability (E- 1.8) may increase as the same model can be aligned with other processes.

Researchers [25] discuss the benefits of utilizing a business process model (BPM) for ISRM. They use a specific model, "business process model and notation" (BPMN) as an example of a BPM and "IS security risk management (ISSRM)" for demonstrating ISRM concepts. Aligning the concepts from both, they propose a security version of BPMN. To explain their concept, they apply it to a case study of an on-line registration process for an Internet store. User registration is considered a BPMN business process and its security concerns are identified. Specific threats for confidentiality, integrity and availability are considered. The vulnerabilities that can lead to those threats and their position in the BPMN model are identified. Based on the controls that can help mitigate those threats, they propose an extension to the BPMN model. Assessing theoretically, the authors mention that their model has certain limitations such as incompleteness (not all concepts of ISSRM and BPMN are aligned), under-deficiencies (some concepts aligned but their rationale not clearly defined) and redundancies (the mapping is one one-to-many or many-many). The focus of their work was to enhance alignment with business objectives (E- 1.5) and to increase interoperability (E- 1.8) but a decrease in the required input sources can be anticipated (E- 2.1).

Authors of [29] propose that every stakeholder's opinion about an organization's assets and vulnerabilities must be incorporated in an ISRM process. Every stakeholder (technical as well as managerial) would view a particular asset and its threat profile differently. Incorporating them all would yield more accurate and efficient assessment results. In-fact, documenting the views of a problem through cognitive maps[1], they claim, would help develop more *appropriate and flexible* security policies and controls as well. To support their argument, the authors interviewed three professionals of an organization that had recently suffered a security breach, asking them about their opinion of the possible causes that led to the breach. Each one of them revealed a different view according to their own experiences and encounters with the company's systems and policies. The authors present three cognitive maps in their paper, one for each stakeholder. The purpose of these is to show that valuing each stakeholder's perspective can allow the organization to identify greater number of vulnerabilities and threats and more accurate ones as well. Within the taxonomy, the approach targets to achieve bet-

[1] "A cognitive map consists of nodes and relations an individual uses to develop his/her understanding in specific problem space" [29]

ter accuracy (E- 1.2). Building cognitive maps would however require more preparation as well (E- 2.3).

In [30], authors propose risk identification through "generic algorithm" whereby rules are developed that help analyze factors that contribute to risks and the extent to which they play this role. The purpose of their work is to improve ISRM by considering vulnerability propagation through multiple paths. A Bayesian network is developed to define risk factors and determine causal relationships among them. For risk analysis, probability of occurrence and severity of consequence of each risk in the Bayesian network is calculated. Based on the results, vulnerability propagation paths are calculated through another algorithm (ant colony optimization). Decision making would be based on these calculated probabilities, the authors suggest.

To validate their model, they carried a case analysis. Risk factors were identified and risk rules developed for risk identification of a Chinese financial services firm. A Bayesian network was developed in accordance with the results of risk identification and historical data collected for the company (including 200 cases). The authors conclude that their model has the ability to improve accuracy (E- 1.2) in ISRM.

3.1.1 Summarizing literature findings for ISRM improvement

The analysis about how the techniques affect other taxonomy factors is in harmony with the correlation table (Table 2.1) of RiskE4. Wherever effectiveness is attempted to be enhanced, the other three factors decrease. Similarly, an enhancement in any of the three reduces effectiveness and so on.

There have been significant efforts for enhancing ISRM alignment with business objectives but the main focus of researchers in the past few years has been "completeness of asset identification". None of the proposed techniques covers all the aspects of asset identification; either tacit knowledge assets are not taken into consideration or some compromise over the identification of technical assets is made. Whereas it is obvious that a model achieving the best of all taxonomy factors is not feasible, one achieving complete asset identification can be proposed in future and tested in an organization through practical enforcement.

3.2 ISRM assessment factors

The main intention behind developing this framework is to provide ISRM researchers, a criterion with which fine-grained deficiencies in ISRM methods can be identified and all future improvements can also be holistically evaluated. In this context, it was vital to explore and understand literature regarding ISRM methods' comparison and examine the criteria according to which researchers have assessed different ISRM methods previously.

Authors [33] established a framework for the assessment of risk analysis methods. Their framework addresses the completeness of a method from three different perspectives: A method would be complete if (1) it addresses the domain of information technology completely i.e. network devices, hardware, and documentation etc in its set of countermeasures (2) it addresses the domain of information security completely i.e. threats emerging from different human and natural sources (3) its risk approach is complete i.e. no essential step within the risk assessment cycle has been missed. All three points have been addressed in "RiskE4" under E- 1.1 Completeness. The first has been catered for under the completeness of asset identification (when assets from different IT domains are addressed, appropriate controls would also be included), the second one under risk identification and the third one under risk assessment (Fig 2.2).

Researchers [34] define an effective risk analysis as "timely, effective, complete, consistent and understandable". Researchers [26] used the same abstract level criteria for evaluating their proposed holistic risk analysis method. In the framework proposed in this paper, timeliness is captured in taxonomy factor E2, effectiveness, completion and consistency in E1 and understandability in E4. The framework doesn't just discuss these at abstract level but rather classifies them in a structured way while providing determining factors for each.

Researchers in their paper [35], also use certain criteria while comparing six different ISRA methodologies. Their criteria can be summarized in the form of six main questions; whether the risk assessment model requires (1) management support, (2) experienced qualified and trained practitioners, (3) business, operational or IT documentation, (4) whether it is adjustable according to organizational context, (5) what deliverables does it produce and (6) how many asset categories does it consider. In our proposed framework, questions (1) and (3) have been incorporated in taxonomy factor E2, questions (4), (5) and (6) in E1, whereas question (2) is a part of E4.

Authors [36] have compared three risk assessment methodologies based on: (1) how many steps the method includes as part of risk assessment (E-1.1 completeness in RiskE4) and (2) the amount of documentation available (E-

4.4 available support in RiskE4). According to authors of [28], the success of an ISRA can be gauged using three factors: context suitability (E- 4.3 in RiskE4), validity or reliability (E- 1.2 in RiskE4) and the quality and quantity of the input information that it takes (E- 2.1 in RiskE4).

Researchers propose a framework for comparing risk assessment methods in [22]. They base their framework on a criterion consisting of five major questions: (1) whether the method is applied to a single asset or a group of assets. The authors state that the methods that apply to a group of assets are faster (i.e. increasing efficiency by minimizing preparations/ working involved (E-2.3 in RiskE4's taxonomy)); (2) the amount of work to be performed before risk assessment (E-2.1 in RiskE4's taxonomy); (3) whether it requires external people as experts or not. This is stated as a tradeoff between cost and expertise in their paper. However it may not truly affect effectiveness as an organization might have enough expertise sitting within the organization. In that case, a mandatory requirement for external experts becomes an extra cost burden (captured in E 3.1 in RiskE4's taxonomy); (4) whether it utilizes mathematical formulas or an expected value matrix. (E- 4.3 in RiskE4's taxonomy); (5) whether the risk assessment results are relative or absolute i.e. whether the exact difference between risk rankings can be inferred from the results. The authors do not explicitly explain this factor but it can be deduced that the nature of results would be a direct consequence of the input values and mathematical formulae utilized.

The work of [37] is also about factors to be considered when comparing different ISRM methods'. They mention cost (E- 3 in RiskE4's taxonomy), adaptability (E- 1.4 in RiskE4's taxonomy), complexity of results presented to the management (E- 1.6 in RiskE4's taxonomy), completeness (E- 1.1 in RiskE4's taxonomy), consistency (E- 1.3 in RiskE4's taxonomy), usability (E- 4 in RiskE4's taxonomy), credibility (E- 1.2 in RiskE4's taxonomy) and automation (E- 2.2 in RiskE4's taxonomy) as the factors to be considered for a method's evaluation. Other factors considered are with respect to the organization planning to enforce ISRM e.g. their structure, security philosophy and size etc. These are not applicable to our work as RiskE4 analyzes ISRM methods explicitly, irrespective of other factors.

It is evident that none of the above articles consider all factors. RiskE4 brings them all together under a structured/ well-classified taxonomy and enhances the overall criterion as well.

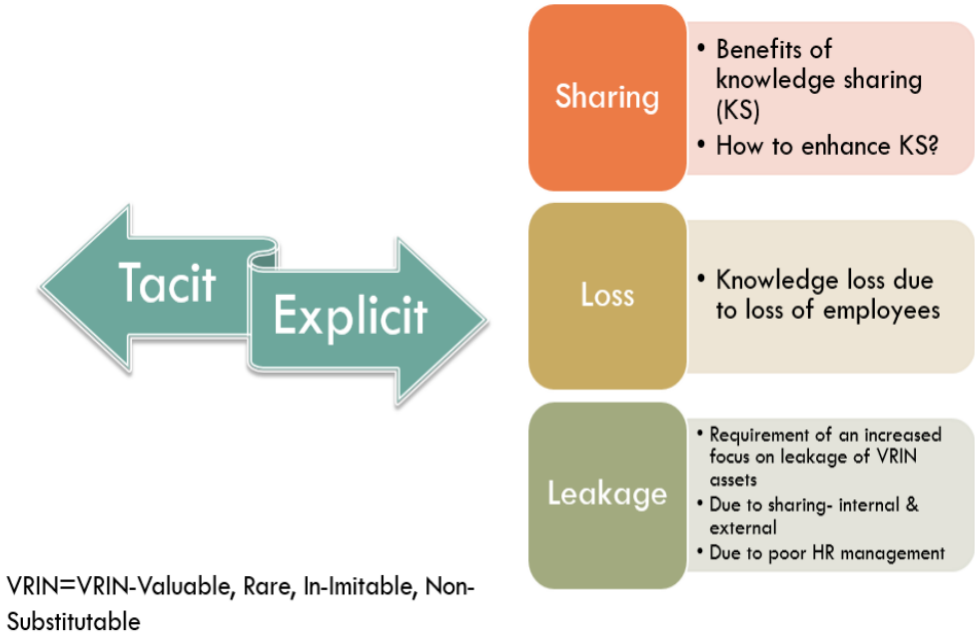

Figure 3.2: Knowledge Management Literature: Summary

3.3 Knowledge Management

The focus of researchers in knowledge management literature has been in three major directions as illustrated in Figure 3.2, while keeping tacit and explicit knowledge distinguished.

Researchers, in [38], explore the existence of various knowledge protection strategies in different organizations and use their findings to suggest the need for a strategic level knowledge management framework. They begin by stating that the current literature lacks any considerable data on strategic guidelines or mechanisms that an organization should employ in order to safeguard its critical information. In their research article, they define four main knowledge protection areas and provide protection mechanisms that support each of these.

The first area, Strategic-level Management Initiatives, includes the identification of what to protect and the policies and guidelines dictating how to do so. The second area, Operational-level Knowledge Protection Processes, enables the implementation of the policies defined by the first one through operational procedures. These can include classifying knowledge according to its sensitivity level and its protection through mechanisms such as restricting access or making it either explicit (to avoid loss) or tacit (to protect its confi-

dentiality). The third area, Supporting Technology Infrastructure, is rather simple and common i.e. the usage of different tools and technologies for the sake of knowledge protection. The last one, Legal Structures for Knowledge Protection leverages legal bounding or documentations (non-disclosure agreements or patents) for the same purpose.

Authors of [10] present a knowledge security risk management (KSRM) framework. They discuss the importance of protecting tacit and explicit knowledge in an era when knowledge sharing is being encouraged and tools for its support are being developed. Knowledge leakage can lead to risks that cannot be undone such as the loss of reputation or knowledge based competitive advantage for competitors.

The KSRM process that they define comprises 7 steps. The first is the identification of business processes or problems that initiate KSRM. Stakeholders responsible for conducting these processes and those responsible for KSRM would also be identified in the same phase. The second one focuses on the identification of knowledge assets based on their importance towards business. They propose that identification of knowledge assets can be made easier and more comprehensive by first identifying knowledge sharing tools and then analyzing usage of each (who is sharing what through it). In the third step, threats arising from technical operation of the tools as well as those arising from human errors would be identified. Involving employees in this step will make it easier and more effective. In the fourth phase, risks are analyzed using a risk matrix. Cost-benefit analysis (as described earlier) is proposed to be carried out throughout the KSRM process, but as a separate phase (fifth) as well. Knowledge protection, they mention, has subtle indirect costs as well such as loss of communication. The sixth phase is the implementation of risk mitigation strategies. The controls should include technical as well as administrative ones. Effectiveness of mitigation strategies and changing risks should be monitored and evaluated in the seventh phase.

The authors gathered reviews of five security professionals by asking them to implement the model theoretically and keeping social media as the knowledge sharing tool in main focus. Overall, the responses indicated acceptance of their model as a well balanced one. A more accurate evaluation of this model is possible after practically implementing it in an organization. The process can be enhanced by provision of automatic tools or worksheets and the framework could be made holistic in future, by incorporating traditional benefits of ISRM as well as other aspects of knowledge management.

The research article [31] is about quantifying knowledge loss risk in terms of the consequences it can have towards an organization. The authors focus on losing knowledge through the loss of its sources i.e. employees. They

mention that this can happen due to reasons such as job mobility, retirement, health issues and so on. They also state that just because knowledge has been documented, it doesn't necessarily imply that loss of its author will not have an impact. The document (in any form e.g. a database) might not be understandable without the assistance of the resource that produced or compiled it.

A method for calculating knowledge loss risk, in particular context of nuclear organizations was developed in a research prior to this one. The authors use that method but tailor it so that it can be generalized to any organization. The formula devised for risk calculation is "Risk (knowledge loss)= P(loss of human knowledge source)* C (loss of perfect human knowledge source)* Q (quality of human knowledge source)". The first factor in this formula captures the likelihood of losing a particular resource. The authors propose a 10 point scale for evaluating this probability which ranges from definitions (10) = "employee is definitely at the risk of leaving" to definition (0)= "there is no reason to believe that the employee would leave". The second factor illustrates the consequences of losing a perfect knowledge source. A 10 point scale is again proposed which ranges from "employee is key resource and no replacement is possible" to "no reason to believe that losing employee would harm in any way". The third factor in the formula acknowledges the quality of source which can be determined from factors such as "perceived time to lose knowledge" or "current health of employee" etc. MBA students (who were experienced professionals as well) evaluated this model and found it workable and generalized.

Only a single factor (loss of human resource) contributing to knowledge loss is considered in this paper. Other factors such as physical loss of documentation, employee's willingness to share or utilize knowledge should also be considered for a complete framework for KSRM to be developed.

In their article [39], authors discuss the importance of balancing the benefits achieved by knowledge sharing and the risks associated with it. They describe the difference between data, information and knowledge. Data are raw and unanalyzed patterns that are input to processes. Processing and mathematical / statistical analysis of data leads to the formation of information. Interpretation of the latter and the experiences or expertise of each individual linked with it forms knowledge. It is argued that effective knowledge management does help mitigate risks but increased flow of knowledge between organizations gives rise to other knowledge-based risks as well. Knowledge risks are classified in this paper with the hope that it would help bring about secure knowledge management in relative future.

Knowledge sharing can be asymmetric or a symmetric one. In symmetric collaboration, all organizations participating in a knowledge sharing network

are equally dependent on each other whereas asymmetric collaboration refers to the scenario when any one organization dominates others i.e. its requirement of receiving knowledge from others is significantly low but itself, it can be a valuable source of knowledge for others. Proximity refers to the fact that organizations located geographically close to each other develop stronger trust levels and can share knowledge more effectively (due to similarity in culture and language). The risks associated are lesser due to this but the possibility of security breaches increase, the authors argue. Furthermore, deliberate sharing by company, by an individual employee and non-deliberate sharing (e.g. informal conversation) all give rise to different risks with different impacts. Lastly, the range of risk which can be either restricted to a department, to one or two companies or to the whole network.

The authors mention that organizations must estimate the benefits perceived from knowledge sharing and evaluate them in comparison to the risks that they pose. They conclude that this framework is just one step forward and must be coupled with other efforts if a holistic knowledge risk management (KSRM) framework is to be developed.

Authors of [40] review the literature on the topic of knowledge protection and present a review. The authors mention three areas of knowledge protection which are (1) prevention of knowledge spillover e.g. as a result of over sharing or leakage in any way (2) reduction of knowledge visibility and (3) knowledge loss that can occur due to retiring or moving employee. Performing a COBIT-like methodology for forming a knowledge protection framework, the authors categorize what needs to be protected (knowledge related to people skills, processes or product information), why it needs to be protected (three areas of protection mentioned) and how protection can be ensured (legal, organizational or technical measures). The authors mention that the area of tacit knowledge protection is currently under-researched and needs to be explored further. The authors also argue that knowledge protection along with information security strategy should be considered an integral part of risk management and be linked the same way.

Authors of [41] have proposed a framework for managing knowledge security risks in an organization. The first major step of their framework includes identification of knowledge assets within sharing practices or collaboration technologies. Knowledge can be stored in people (individuals or groups), in artifacts (practices, technologies, repositories) and organizational entities (units, organizations and inter-organization networks). The authors define knowledge value in terms of its ability to enable the organization in sensing and responding to opportunities and threats in business environments, its possession by competing organizations (how rare it is) and the ease by which the latter may reproduce or acquire it. Other steps include identifying vul-

nerabilities and threats to knowledge assets, estimating risk likelihood values through expert judgment and calculating the overall value based on their combined input. In the end, security policy is developed so as to mitigate these risks or bring them to an acceptance level.

Researcher [42] discusses the importance of integrating the fields of knowledge management and information security. As part of his editorial, he expresses the rising need for securing knowledge assets at three levels, product, processes and people. The products level deals with securing codified or explicit knowledge. These can be secured by tagging, segmenting or compartmentalization (marking confidentiality levels or access privileges). Knowledge protection at people level is discussed in his editorial with the aspect of trainings workshops and presence of counterintelligence (CI) teams. They mention that the CI teams preempt threats and their mere presence can serve as a deterrence for mischief makers. Finally, they mention that the process of knowledge creation (e.g. innovative formulas), its application need also be secured from unauthorized disclosure or modification. The communication of knowledge would need to be monitored.

In [43], researchers highlight the importance of enhancing knowledge base of all employees in an organization. They argue that making knowledge of IT security common in an organization would lead to the development of better security policies and implementation of better security measures and reduce dependency on employees as well.

The architecture proposed has four main layers. The first layer is about identifying users whose acquiring knowledge can enhance organization's overall security. The second layer, knowledge interface, exhibits knowledge appropriate for the user it is to be acquired by. The third, knowledge description layer, classifies knowledge in the form of ontologies, rules, action schemes or strategies. The knowledge resource, the fourth layer, relates to the different containers from where IS related knowledge can be obtained. This architecture is to be used so as to code tacit knowledge for the purpose of its protection and so that it can be leveraged for improving the organization's security posture.

Authors of [44] emphasize the need for security integration within knowledge management (KM) and explore the level to which organizations and practitioners realize and implement this fact. Their research is based on three stages. They explore the extent of security integration into knowledge management through a literature review, through an analysis of job postings in the second and through survey questionnaires in the third.

For the literature review they analyse papers for their recognition of the need for security in KM, those that applied technical IS solutions to resolve KM issues and those that utilized risk management techniques within KM.

They found out that a small but growing number of researchers recognize the need for security while sharing or transferring knowledge. For the second phase, they explored career portals to examine the requirements listed down by. Out of 39 postings, they found only 5 to have incorporated security requirements. In the third phase, they found out that most organizational leaders do not realize the importance of securing knowledge or information assets. Much attention is being paid to storing and sharing knowledge but not its security.

Authors of [45] explore the risks arising from employee's use of social media (SM), their causes and mitigation possibilities. For their research, they conducted eleven interviews. Identified problems arising from SM included identity theft, scams, phishing, merging of personal and professional lives etc. Identified characteristics of SM that were a cause of these problems included, blurry audience, easily collectible information, generation transition and ultra-fast information distribution/sharing. Their results suggested that employees sharing information on SM usually do not realize or have an idea themselves, of the nature and amount of audience that can access their posts.

Their study also points out that employees sharing their personal views on anything are many a times, associated with the company and that this can severely damage the latter's reputation in many cases. Another risk identified was that many employees use SM to communicate with customers/stakeholders and this can at times, cross boundaries and hence result in a damaged reputation or loss of contracts once again. Employees might share confidential information without realizing the speed with which it would disseminate through the channel under discussion. The fast speed of communication means that damage would be possible to be contain or undone. Some companies also mentioned their fear of employees sharing unfavorable information on SM, such as when there has been some management issue. It was also identified that it is nearly impossible for the management to keep track of each of their employees SM postings.

Mitigation possibilities that the authors identify focus on management decisions. These include questions, the likes of "Who is allowed to share information on SM? With whom and When? Do they realize the impact their posts can have on the company etc".

Researchers investigate the factors that influence knowledge sharing behavior in professionals, specifically in a professional virtual community (PVC) in [15]. They define five hypotheses, the first of which is that professional's intent to share knowledge is strongly motivated by the perceived output. The latter constitutes the expected usefulness (what could be achieved by sharing that specific knowledge), reputation (i.e. to what extent the employees believe that sharing knowledge can improve their importance and credibility

as an individual, in their professional community) and influence of social network ties (H1). The second hypothesis states that the individual's emotions and sentiments also derive their knowledge sharing behavior (H2). The third one asserts that social factors (culture, norms, environment etc) also impact knowledge sharing behavior of PVC members (H3). The fact that members' facilitating conditions (geographical obstacles, ease of use with computer, availability of devices etc) also influence the knowledge sharing behavior, is captured in the fourth hypothesis (H4). These factors were studied by authors of [19] as well, with slightly different terminologies and research model. The authors of this paper claim that their main contribution lies in the study and validation of hypothesis 5, which states that knowledge sharing in PVCs is strongly related to risk reduction expectation (H5).

To test their hypotheses, the authors emailed questionnaires to 200 members of Linked-in groups (a popular PVC) and received 142 valid responses from members who were active in their PVC and experienced in their field of profession. The Linked-in groups were all related to Information security (such as risk management, cloud security, IT security and audit professionals etc). To support their results, the authors applied statistical tests to their findings from the questionnaires. The result was that H1, H2, H4 and H5 were validated whereas H3 was found unsupported/inconsistent.

The authors [16] investigate the effects of different knowledge sharing motivations on knowledge sharing intentions of employees. They claim that in all previous literature, this topic has never been studied with the separation of tacit and explicit knowledge sharing under consideration. As a result, the theories and results provided in the previous literature might be applicable in the context of either one of the two but not both. In their work however, they have studied knowledge sharing of explicit and tacit separately.

The authors categorize knowledge sharing motivations into individual and social ones. Individual motivations consist of organizational rewards, reciprocity and enjoyment. Organizational rewards can be salary bonus or employee appreciation awards. Reciprocity means that the employee will share knowledge with the motivation that he would receive knowledge in return. Enjoyment factor is there when the employee feels happy and content by helping others through sharing knowledge. The authors form five hypotheses (H1-H5) based on theoretical reasoning. The first hypothesis is that an employee willing to share tacit knowledge would also be willing to share explicit knowledge since the latter requires less effort. H2 states that organizational rewards have a positive effect on both tacit and explicit knowledge sharing but more on explicit. Reciprocity, enjoyment and social capital have a positive effect on both more on tacit knowledge sharing according to H3-H5 respectively.

To test their hypotheses, they emailed questionnaires to employees of seven companies and collected responses that revealed the factors that were motivating employees to share explicit and tacit knowledge. Applying statistical tests in order to gain further accuracy, they found that organizational rewards had a very small positive effect on explicit knowledge sharing and a negative one on tacit. Reciprocity, enjoyment and social capital had a positive effect on both but more on tacit knowledge sharing. Amongst these three, they found out that enjoyment had the greatest positive impact on tacit knowledge sharing and reciprocity the least. Based on these results, the authors suggest that providing organizational rewards for knowledge sharing is not advisable since it has a negative effect on tacit knowledge sharing and a very small one on explicit. Organizations should make efforts to create a culture where reciprocity, enjoyment and social capital inhibit more. Enjoyment factor can be enhanced by community activities whereas social capital by analysing the social network of the organization and encouraging employees to participate in activities that improve social ties and trust among them.

Researcher [17] highlights the importance of knowledge sharing in an organization with respect to increased collaboration and competitive advantage. Based on an extensive review of the literature, the authors lay down seven propositions (P1-P7). P1 and P2 state that users trust a social networking site (SNS) more if they perceive greater benefit (P1) and less if they perceive more risk (P2). P3 and P4 are related to the knowledge sharing intention of an employee based on the same risk and perceived benefit. P5 states that when the individuals that make up an SNS, are more in number and greater in importance, knowledge sharing intention of each participant increases. P6 signifies the positive effect of social influence on knowledge sharing intentions i.e. the extent to which social culture/environment encourages individuals to share knowledge. P7 states that knowledge sharing intentions directly impact knowledge sharing behavior.

Chapter 4

Research Methodology

4.1 Thesis Research Methodology

The research was carried out systematically starting from the selection of topic to obtaining results and reaching conclusions. The overall research consists of eight major phases. The first three phases are theoretical where literature is thoroughly studied in order to (i) identify research area and problems (ii)define and categorize the assessment factors used for evaluating and analyzing ISRM methods. In the same theoretical phase, ISRM deficiencies identified in the past and improvement techniques proposed are also studied and critically analysed. The rest of the phases involve designing a framework and testing it practically in an organization. Initially, different propositions from the literature were collected and attempted to be carried out practically. However, each of the techniques had practical limitations and hence it was concluded that a new approach needed to be formulated. This led to the formation of IKOSST framework. The practical implementation, testing and evaluation was then carried out in the form of two case studies.

Each of the seven phases are described in the subsections of this chapter.

4.1.1 Define a Research Area

A study of the latest research in information security management was performed in order to explore the areas that have received the research community's major attention. Latest research papers authored by established researchers and published in best-ranked journals were studied. Research about Digital Forensics, Information Security Management, Security Governance, Incident Response, Knowledge Security and Information Security Culture was studied. Amongst these Information Security Risk Management

and Knowledge Security were found to have a correlation and hence the two were narrowed down for further stuy.

Our thesis contribution revolves around Improving risk management practice in the industry and establishing a concrete relationship of knowledge management with ISRM. We conducted extensive survey and analysis to gather the observations on (i) assessment criterion utilized previously for ISRM methods (ii) deficiencies and improvement attempts in the field of ISRM. Our first thesis contribution is the establishment of "RiskE4" as a comprehensive yet intelligible assessment criterion for ISRM methods while the second contribution is the formulation and testing of "IKOSST" as a major improvement technique for ISRM practice.

4.1.2 Literature Survey

After narrowing down the research area, the second step was to conduct an extensive literature survey of the ISRM and KM literature. Surveying few research articles in the area of ISRM gave the understanding that recent research has been focused towards identifying ISRM deficiencies and providing solutions for them. Having this fact established, further literature review was performed. Articles from quality journals and conferences were shortlisted and studied with the following three questions:

1. What assessment criterion has been used by previous researchers in order to categorize or evaluate ISRM methods or is there a standard criterion present? Is that criterion comprehensive enough? Is the assessment criterion in an intelligible, classified, easy-to-utilize form?

2. What factors have been the focus of researchers for ISRM improvement? How comprehensive are those improvement techniques? Do they provide a theoretical model or a practical framework? What are their limitations and how thoroughly have they been tested?

3. What has been the researcher's focus in the domain of Knowledge security? What attempts have been made to integrate knowledge management with ISRM?

The details of literature survey already been highlighted in Chapter 2. The answers to the above problems led us to identify the research problem.

4.1.3 Formulate Research Problem

After conducting a comprehensive review of the information security management (ISM) and knowledge management literature, the following inferences

were made:

1. *"Surveying the assessment criterion used for ISRM techniques"*: Through a review of the ISRM literature, we were able to observe that researchers have performed the comparison not according to a standard criterion but with respect to different factors each time. Some effort has been made towards providing a framework for ISRM evaluation ([22], [37]) but an organized and comprehensive solution is still lacking. A comprehensive but structured criterion for evaluating ISRM methods and improvement techniques is vital for leading ISRM improvement efforts in a focused and balanced direction. While proposing improvements for any one of the deficient areas, researchers would be able to determine other factors on which the proposed improvement may have an effect. Moreover, the same criterion can be used to compare different ISRM methods so that in future, organizations may be able to determine the pros and cons of each method and then select the one that suits their needs or is in accordance with their limitations.

2. *"Identifying ISRM practices' deficiencies and suggested solutions":* The study revealed that various improvements have been suggested for ISRM. All these have focused on any one aspect/phase within the process and none of them provides a holistic solution. Researchers have mainly focused on either the comparison or evaluation of existent tools and technologies or on utilizing business process model and enterprise architecture frameworks for the improvement of ISRM process. While all these are beneficial, a holistic framework that minimizes the deficiencies identified in the past 2-3 years is still lacking.

3. *"The importance and need for knowledge security"*: Researchers have focused a lot on the advantages of knowledge sharing, creation or management. The need and importance for securing the overall knowledge management process including the aspects of tacit as well as explicit knowledge has just been realized. The field is still under-researched and only few publications have discussed some sort of knowledge security framework or methodologies. Out of them, even fewer are those that discuss knowledge security management as an integral part of the overall ISRM process of an organization and none of those holistically cover other ISRM deficiencies. The aspects of knowledge sharing for an improved ISRM on the one hand and knowledge protection for securing competitive advantage on the other have not been addressed together under one framework. While some researchers focus on the importance of making valuable knowledge readily and sufficiently AVAILABLE,

others express a need for protecting CONFIDENTIAL knowledge from being leaked. A holistic ISRM framework that includes a mechanism for finding a balance between the two is still lacking.

The above conclusions led us to highlight the fact that researchers have been trying to improve ISRM methods in various aspects. The integration of knowledge management has been a vital attempt. A holistic and practical solution however, had been lacking. Through this, the **problem statement** got formulated:
"Knowledge leakage to secure competitive advantage and loss to ensure continued business operations need to be realized as distinguished objectives within ISRM. A holistic framework for ISRM needs to be developed, that ensures the protection of tacit and explicit knowledge while retaining the benefits of traditional ISRM methodologies".

4.1.3.1 Proposition of Assessment Criterion

The output of the literature study was the formation of "RiskE4" which consisted of a taxonomy of assessment criteria factors as well as correlation among them. Moreover, improvement techniques were evaluated according to the criterion set by RiskE4. The type of research used in this phase was "fundamental" research. In this phase, only theoretical propositions were made in order to add to the existing ISRM knowledge. No practical testing was done but rather, an amalgamation of previous ideas and studies led us to the formation of a solution of an existing theoretical problem.

4.1.4 Exploratory Study

Before reaching any solid hypothesis, an exploratory study was first performed, this selection being based on two major reasons:

1. The experience of the researcher matters a lot when it comes to deciding a research method. Since, ISRM is a highly practical field where theoretical/classroom/bookish knowledge is not enough but rather experience is required. Being unexperienced in this field, it was logical to first study the field from organizational perspective, gather observations from practicality point of view and then build some hypotheses for testing.

2. The research is still in it's infancy. To the best of our knowledge, only two-three previous approaches have been proposed with the objective of improving ISRM asset-identification. This again meant that prior to

developing hypothesis and research design, an exploratory study was suitable.

3. An exploratory study helps develop the hypotheses, determine the best research design and data collection methods.

It was certain that ISRM need practically be implemented in a real-time case study in two phases. The first phase would be based on asset identification and risk assessment through standard regular methods while some sort of improvement techniques would be tested in the second phase. It was initially planned that the genre based technique [11] would be tested for asset identification while precision in risk formulas would be tested for risk estimation. However, this need further be explored and hence concrete hypotheses were not developed at this stage.

4.1.5 Develop Hypothesis

The next step was the development of hypotheses for our research on the basis of the extensive literature survey as well as the exploratory study performed. Observations were collected during the first phase, two of the most important of which were, (i) genre based method requires brainstorming again and hence is likely to miss assets (ii) genre based method still would not incorporate fluid assets produced during daily activities (iii) risk estimation can not be improved through increasing the precision of formulas as it introduces even more guess work, reduces efficiency a d ease-of-use by a great extent and above all, may invalidate the results. Based on these observations, the following hypothesis was developed:
The inclusion of an extended RACI activity can significantly improve asset identification is ISRM. It will not only help identify knowledge assets but other fluid assets produced during daily activities as well.

4.1.6 Research Design

This phase was about practically testing IKOSST. This was performed in the form of two case studies. The first case study was from a renowned Pakistani University and its scope was limited to three major processes of a newly deployed Campus Management System. The second case study was that of a public sector organization (the name given GreenCo in this document). The organization was undergoing a two-year enterprise wide risk management process. For the purpose of testing IKOSST and as part of the organization's project, risk assessment was performed for one wing of this organization.

Since IKOSST testing mainly revolves around the improvement of asset and risk identification phase, asset identification was additionally performed for three other wings as well.

Two case studies were selected based on: (i) Data was easily accessible as the researcher was professionally associated with both organizations (ii) Both organizations did deal with sensitive data and hence risk assessment was significant there (iii) One of the two organizations were going through an enterprise-wide ISRM project and hence even more cooperation from the employees was expected.

For experimenting, the following factors were kept in mind:

- IKOSST was first theoretically designed on the whole, and hypothetically tested on paper before involving external sources.
- The scope of research needed that be of an MS thesis level research.
- Data would be collected through interviewing asset owners. Essentially, the asset owners would be performing the asset identification so as to rule out chances of subjectivity in results.
- Risk assessment would be performed according to standard formulas and methods in order to ensure validation of results. On the other hand, strategic solutions would be proposed for improving accuracy in ISRM.
- Documentation of the whole process would be maintained consistently throughout the research so that results may be compared with in the end and anything could be backtracked, if need be.
- Confidentiality of both organizations' data would be kept secured according to the wishes of their managers/related officials.

4.1.7 Project Execution and Data Collection (Empirical Evidence)

The study began as an exploratory research but empirical evidence was collected once the hypothesis had been developed. Data from a total of around 8 major processes was collected before reaching conclusions.

Each of the two case studies was further divided into two phases. In the first phase, risk assessment was performed according to standard methods. An Italian method was used for the risk assessment of GreenCo whereas Octave-Allegro ([3]) was utilized for the risk assessment of a University case

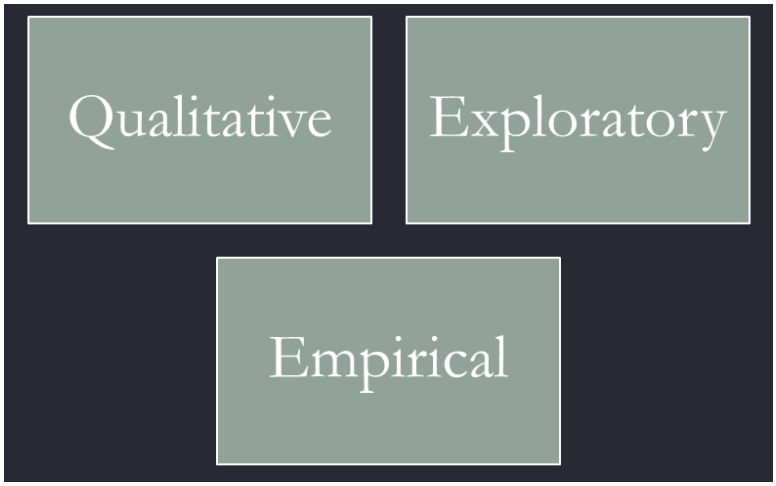

Figure 4.1: Hybrid Research Methods adopted

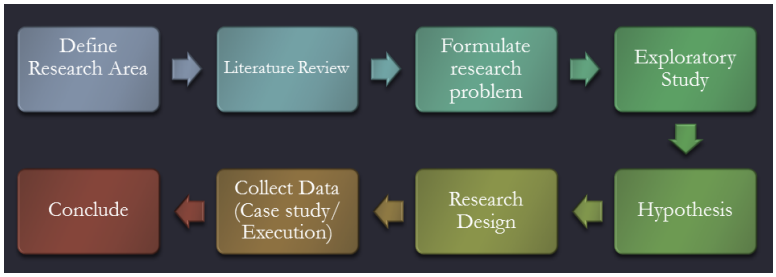

Figure 4.2: Methodology explains the rationale behind methods undertaken and the steps involved

study. In the second phase, the major part of IKOSST i.e. the extended RACI+ activity was performed for five different processes within the same four wings.

4.1.8 Hypothesis Testing and Conclusions

The data collected and analysed was Qualitative in nature. The improvement technique did not involve any numerical data or statistical results. The results from the two phases of asset identification were compared and the hypothesis was positively proven. The results showed that fluid knowledge assets and assets produced in daily activities did get identified through the inclusion of the extended RACI activity. These assets had not been identified in the first phase (regular ISRM asset identification). The latter had been carried out by different asset owners and hence the results can be concluded to be objective.

Figures 4.1 and 4.2 summarize the concepts briefed above.

Chapter 5

Implementation

5.1 Case Study 1: GreenCo

5.1.1 Introduction

GreenCo is a public sector organization that deals with huge amounts of highly sensitive data. The IT Department is the main hub that receives processes and stores this data. The department constitutes of four wings, original names of which have not been mentioned in this document in order to preserve confidentiality. The first one deals with network management of the enterprise, the second one with Application and Web development, the third with database management and the last one with Information Security and Auditing. A structure of the enterprise is illustrated in Figure 5.1. Information Security Wing deals with all the Information Security Management processes which include Enterprise Risk Management among many others.

ISRM had previously been deployed in the IT Department of GreenCo two years back and an Enterprise Wide project is now underway. IKOSST deals mainly with improvement in the asset identification phase through the inclusion of RACI+ Activity, therefore for the purpose of our study and as part of the enterprise project, we performed regular asset identification (populated and maintained a comprehensive asset register) for all four wing. Furthermore, complete Risk Assessment for the Information Security Wing was performed (Risk Register populated and maintained).

The Risk Register/Method (including the formula) that was followed by Greenco is an Italian Standard (through which ISO-27001 has previously been obtained by other companies. Appendix B includes the User Manual produced for the risk register. Each and every step followed within the worksheets is explained therein.

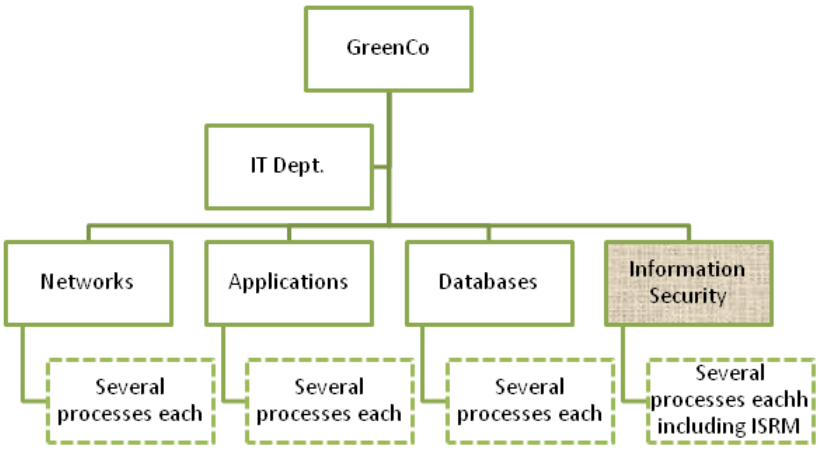

Figure 5.1: Structure: Case Study 1

5.1.2 Risk Management Process

5.1.2.1 The Process Actors

Risk Team: A team of 2-3 personnel from the Information Security Wing of the IT Department for preparing risk assessment policies, procedures, guidelines and worksheets The Senior Information Security Officer (SISO) is part of this team as the Senior most member. Asset Owner: The HoD of each department is represented as the asset owner.

PoC (Point of Contact): A person delegated by the HoD for performing risk assessment of their respective department. At least one PoC was selected from each wing of the IT department with the task of filling asset and (later on) risk register. The risk team was employed with the task of guiding and assisting these PoCs and conducting workshops for their understanding.

Risk Manager: The Chief Information Security Officer (CISO) in-charge of risk team provided relevant instructions.

Decision Maker: A designated person from the top management (such as the Chairman or Commissioner) who will define the risk acceptance criteria and take necessary decisions.

5.1.2.2 Risk Management process flow

The risk management process is composed of the following main stages.

(a) Risk Assessment

(b) Risk Treatment

(c) Risk Communication

(d) Risk Acceptance

(e) Risk Monitoring and Review

The overall Risk Management process is described as under.

1. The decision maker grants the required support and permissions, for initiating the Risk Management process. He/she would also either define the risk acceptance criteria or designate a person appropriate for it and approve his/her output. The acceptance criteria would be communicated to the Risk Manager, who may further communicate it to his team.

2. Each wing would be responsible for the risk assessment of processes under its domain. PoCs or Wing Managers would communicate the results to the Risk Manager, who may further communicate them to the Risk Team.

3. Risk Team, headed by their manager, would be responsible for preparing risk treatment plans.

4. As part of the risk acceptance phase, the Decision Maker would review and approve proposed risk treatment plans as well as the resulting residual risks and record any conditions associated with such approval.

5.1.2.3 Risk Assessment process flow

The process of risk assessment is described as under.

1. The risk team, headed by their manager prepared templates and instructions for maintaining risk and asset registers.

2. The HoD from each department designated a PoC from within his department. The latter would be responsible for performing risk assessment tasks on behalf of the HoD (asset owner). The PoC is the person who is most knowledgeable about the values and security requirements of assets of their department.

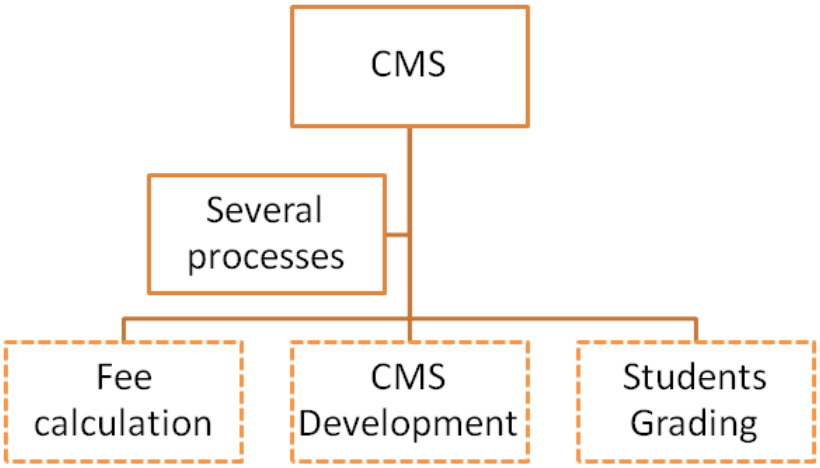

Figure 5.2: Structure: Case Study 2

3. The PoC, using the help of risk team, prepared the asset and risk registers. Essential tasks included listing down assets of their department, assigning them values, identifying relevant threats and vulnerabilities, estimating the amount of risks posed due to those threats and suggesting relevant controls.

4. The output of the risk assessment phase goes into the treatment phase, and those further into the risk treatment phase. The detailed process flows of Risk Treatment and Monitoring phase are intentionally being left out from the purpose of this document. This is to avoid verbosity as these two phases had not begun yet and would take at least two years to do so. Moreover, IKOSST experimentation did not concern with them either

5.2 Case Study 2: CMS(Some Pakistani University)

5.2.1 Introduction

The University has just been introduced with new software by the name of Campus Management System (CMS). This software has been deployed for all schools and campuses of the University and has not only replaced the previously deployed "Learning Management System (LMS)" but also performing several other functions in addition to those being performed by

LMS. Some of these include fee calculation, class scheduling, room booking etc.

For our study, we conducted risk assessment for three processes involving the newly deployed Campus Management System. These processes were (i) CMS Development, Enhancement and Administration, (ii) Fee Calculation Process through CMS, and (iii) Student Grade Calculation through CMS (Figure 5.2. Vulnerabilities were discovered in the first two processes/ their assets. Data collection was also attempted for the process "grade calculation through CMS" but it was found to be in only in partial operation yet and hence risk assessment results were not very comprehensive for this third process.

This risk assessment followed the guidance from the International Organization for Standardization (ISO) provided in Standard 27005:2008, Information technology – Security techniques – Information security risk management. Data supporting this risk assessment was drawn from interviews of focal persons that were identified in the planning phase. The formula given by Software Engineering Institute's Octave Allegro Method was utilized for risk assessment. The risk team defined a risk criterion according to the Octave Allegro Method. Impact areas that can be important to a University were identified and generic descriptions of a high, medium or low level loss in that area provided. Five impact areas were defined in total. The priority levels were assigned in descending order in accordance with the Octave Allegro (OA) formula i.e. the area perceived to be most important for the University is given a priority level of 5 and that perceived least important is on level 1. The vulnerabilities discovered during risk assessment activity, the risks associated with them and an analysis of the latter's impact to the University were recorded in a Risk Register that was created during the risk assessment activity.

Threat scenarios were listed against each asset. Vulnerabilities corresponding to those threats were assigned and risks ascertained. Values for probability of the threat occurring in reality and its impact on the five impact areas were assigned. The overall risk was then calculated according to the OA's Formula. Appendix C includes the User Manual produced for the risk register. Each and every step followed within the risk register worksheets is explained therein.

Unlike, Case Study 1, this case study was not top-management driven. An official risk assessment activity was not underway but rather, risk assessment was performed in silo, only for the purpose of this research. For this reason, Risk Management process is not explicitly detailed for this case study. Risk Assessment process is explained however.

5.2.2 Risk Management Process

5.2.2.1 Process Actors

Focal Person: A person was delegated by the ICT Dir who provided coordination for the complete process and all required information about CMS.

Asset Owners: A person nominated by the Focal Person for each process, from whom most information about the process and assets utilized by it could be obtained.

Risk Team: Risk Assessment was performed by the Student Researcher but under the supervision of Faculty Members.

5.2.3 Risk Management Process flow

The process flow is explained as under.

1. The risk team prepared templates and instructions for maintaining risk and asset registers.

2. The risk team was responsible for performing risk assessment tasks utilizing the information obtained from the asset owners. The asset owners were people delegated by the focal person as someone knowledgeable about the values and security requirements of assets of their processes managed by them.

3. Essential tasks of risk assessment included listing down assets of their department, assigning them values, identifying relevant threats and vulnerabilities, estimating the amount of risks posed due to those threats and suggesting relevant controls.

4. The output of the risk assessment phase goes into the treatment phase, and those further into the risk treatment phase. These has been left out for reasons already explained under Section 5.1.2.3.

5.3 ISRM Phase 2: RACI+ Activity

Appendix A describes the complete IKOSST framework step by step. In the second phase, RACI+ Activity, as described in Appendix A was performed for five processes (from three different wings) of GreenCo and two (CMS Development and fee calculation) for CMS (Case Study 2). The results and

their analysis were recorded in separate sheets “RACI-CMS” and “RACI-GreenCo”.

Chapter 6

Results

6.1 Discussion

For confidentiality reasons, results of ISRM Phase 1 are not explicitly mentioned in this report. It was observed that the inclusion of RACI+ Activity produces many benefits.

Figure 6.3 shows a screenshot of a portion of the RACI+ activity performed for a single process of the CMS case study. Names are hidden for confidentiality purpose. All columns are filled as explained in Appendix A.

Figures 6.1 and 6.2 and 6.4 show how risk assessment information was

Process	Additional assets identified	Additional Threats identified	How/ Why threat got identified?	Vulnerabilities	Probability	Reputation
XYZ	XYZ reports	An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to view confidential information.	Threats to new asset group "XYZ" (e.g. New requests document, QA Document, Server reports, Weekly reports)	Insufficient information security policies. Lack of training of staff. . No cryptographic controls on data.	1	1
XYZ	N/A	An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to modify information.	Threats to new asset group "XYZ" (e.g. New requests document, QA Document, Server reports, Weekly reports)	Insufficient information security policies. Lack of training of staff. . No cryptographic controls on data.	1	1
XYZ	N/A	An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to lose or destroy information.	Threats to new asset group "XYZ" (e.g. New requests document, QA Document, Server reports, Weekly reports)	Insufficient information security policies. Lack of training of staff. . No cryptographic controls on data.	1	1
XYZ	N/A	Accidental disclosure of documents	Threats to new asset group "XYZ" (e.g. New requests document, QA Document, Server reports, Weekly reports)	Insufficient information security policies. Lack of training of staff. . No cryptographic controls on data.	2	1
XYZ	N/A	Loss due to procedure error	Threats to new asset group "XYZ" (e.g. New requests document, QA Document, Server reports, Weekly reports)	Insufficient information security policies. Lack of training of staff. . No cryptographic controls on data.	1	1

Figure 6.1: Screenshot of RACI+ Chart (1)

Financial Loss	Productivity	Education/Research Standard	Safety & Health	Risk Score	Justification/ Current Controls	Risk Rating	Risk Pool	Risk Treatment	Controls (POOL 3)
2	2	1	1	18		MODERATE	POOL 3	Accept	
2	2	1	1	18		MODERATE	POOL 3	Accept	
2	2	1	1	18		MODERATE	POOL 3	Accept	
2	2	1	1	18		MODERATE	POOL 3	Accept	
2	2	1	1	18		MODERATE	POOL 3	Accept	
1	3	1	1	19	No other person consulted.	MODERATE	POOL 2	Reduce	Job rotation

Figure 6.2: Screenshot of RACI+ Chart (2)

Process Name	Process Activities	Responsible (p	Accountable (	Consulted (pers	Informed (person	Sensitivity level of	Confidential knowl	Other stakeh
X	XYZ	UG/PG Staff (HQ)	Supervisor (AD)	DD	Fee section	N/A	Medium	CMS Team, A
X	XYZ	Schools	UG/PG Staff (HQ)	DD	Fee section	N/A	Medium	Nil
X	XYZ	Fee section	Manager (Fee)	Manager (Fee)/ CMS Team	Manager (Fee)	Low	Low	Nil
X	XYZ	Fee section	Manager (Fee)	Manager (Fee)/ CMS Team	Manager (Fee)	Low	Low	Nil
X	XYZ	Fee section	Manager (Fee)	Manager (Fee)/ CMS Team	Manager (Fee)	Low	Low	Nil
X	XYZ	Fee section	Manager (Fee)	Manager (Fee)/ CMS Team	Schools, Students	Low	Low	Nil
X	XYZ	Fee section	Manager (Fee)	Manager (Fee)	Schools, Students	Medium	Medium	Nil

Figure 6.3: Screenshot of RACI+ Chart (3)

Process	Data/ Knowledge	Document or Knowledge?	Data flow identified	Knowledge Flow Identified
X	Payment receipts	Document, Knowledge	X	X

Figure 6.4: Screenshot of RACI+ Chart (4)

	Process 1	**Process 2**
Additional assets	Yes	Yes
Confidential knowledge/leakage protection	Yes	Yes
Vulnerability identified: Workload management	No underload or overload	No underload or overload
Vulnerability identified: Dependence on one individual	Yes	Yes
Vulnerability identified: Segregation of duties	Yes	No
Risks within activities identified	Yes	No

Table 6.1: Output of RACI+: CMS

obtained from the RACI+ Activity. Each is explained below.

- Additional assets: Asset Identification was performed by interviewing asset owners and brainstorming in phase 2. In phase 2 however, the activity listing identified several granular and fluid assets that were not identified in phase 1.
- Additional vulnerabilities, threats and risks: Additional vulnerabilities mentioned in Appendix A were identified for several processes. Threats and risks arising due to these processes were subsequently identified. Tables 6.2 and 6.1 shows what information was extracted for each process of each case study. Process names are hidden for confidentiality reason.
- Risk assessment was performed with the methodology used in phase 1 i.e. risk was calculated according to the Italian standard formula for GreenCo and Octave Allegro Formula for CMS.

	Process 1	**Process 2**	**Process 3**	**Process 4**	**Process 5**
Additional assets	Yes	Yes	Yes	Yes	Yes
Confidential knowledge/leakage protection	Yes	Yes	No sensitive data in this process	Yes	Yes
Vulnerability identified: Workload management	Yes	No underload or overload	No underload or overload	No underload or overload	No underload or overload
Vulnerability identified: Dependence on one individual	Yes	Yes	No	Yes	Yes
Vulnerability identified: Segregation of duties	Yes	No	No	Yes	Yes
Risks within activities identified	No	Yes	No	Yes	No

Table 6.2: Output of RACI+: GreenCo

- During the asset owner interviews (creation of RACI+ Charts), information about the inclusion of confidential knowledge or documents was also obtained. This identified the flow of knowledge and documents. The specification report explains how this information may further help in mitigating knowledge loss and leakage.

Some additional benefits of the inclusion of RACI+ Activity are mentioned below. Figure 6.5 illustrates all major benefits of IKOSST.

- Ensures integration of security risks into management processes/align-

ment to business objectives. A RACI chart is an activity usually utilized for project management purpose. The chart would be based on each process, keeping in view the business objectives from that particular activity. This would increase alignment between security services and business objectives.

- It would help in project management. Roles and responsibilities for each process would be explicitly defined due to this activity. This is also an objective mentioned in COBIT [46] under objective PO10. It can also help produce Standard Operating Procedures, as identified by the employees of GreenCo.
- It also reduces risk of repudiation since accountability is now explicitly defined.
- Can be integrated with any risk management method.
- It can be utilized by any organization, whether they have previously implemented risk management or not. For the case of former, it would just be added in monitoring stage.
- It enhances organizations security culture and awareness of employees as RACI+ Charts would be made by the process owners/teams. This awareness further increases the results of risk assessment as proven by [24] [32].

6.2 Evaluation

6.2.1 Assessment from RiskE4

IKOSST is evaluated according to the Assessment factors of RiskE4 below. A summary is provided in Figure 6.6. All evaluation in this section is exclusive of the correlation among different factors. One factors is evaluated independent of any effect due to any other factor. Moreover, evaluaton is such that "effect on IKOSST on any generic ISRM method when the former is integrated with the latter" e.g. "IKOSST increases the completeness factor when applied with Octave-Allegro" and so on. In Figure 6.6, the factors on which IKOSST has a positive effect are shown in green while those having a negative effect in red. Factors on which IKOSST has no significant effect are shown in yellow.

Figure 6.5: IKOSST Benefits: Industry point of view

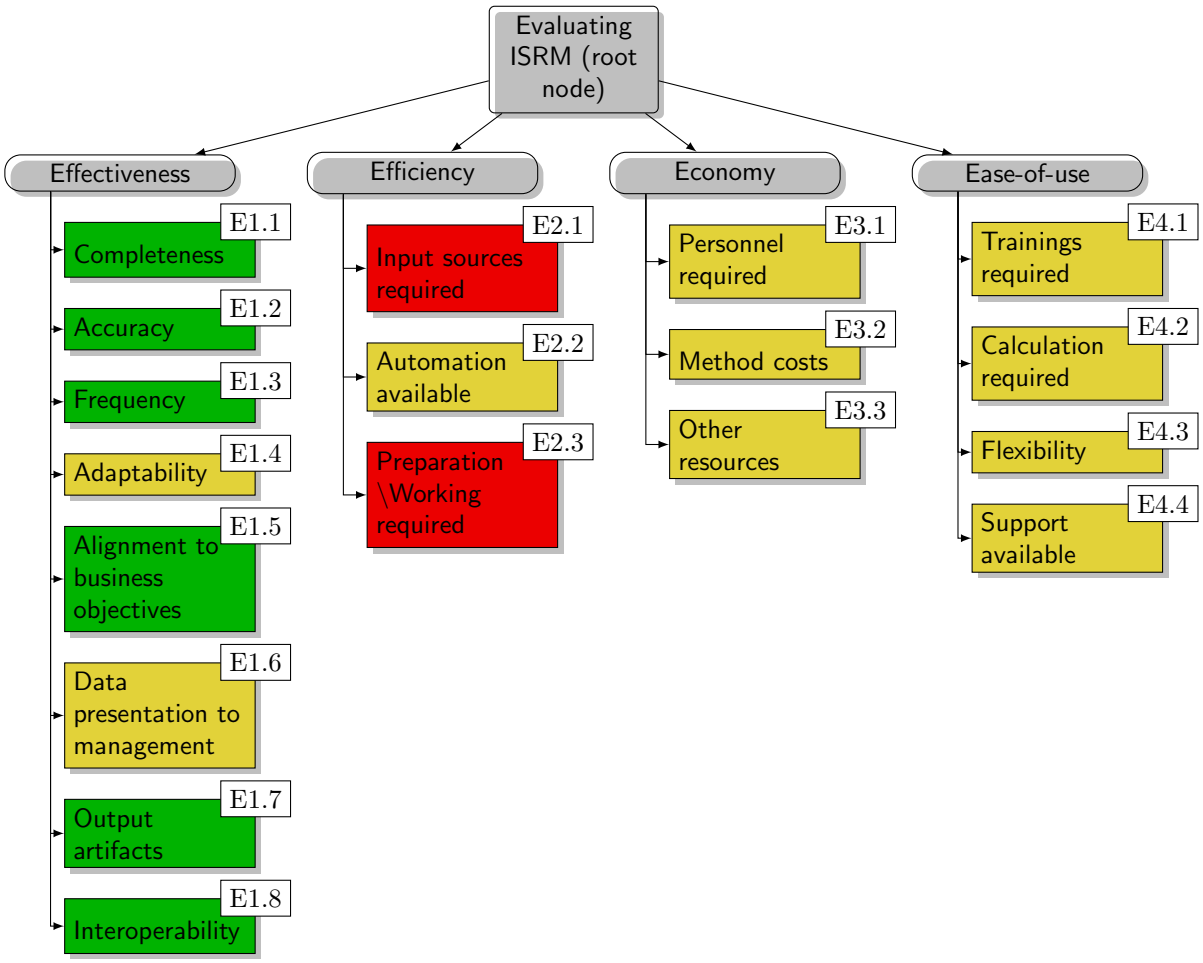

Figure 6.6: Evaluating IKOSST on RiskE4

Figure 6.5 is constructed from the indutry/market point of view i.e. selling IKOSST from the business point of view while Figure 6.6 illustrates IKOSST evaluation from a researcher's point of view.

6.2.1.1 E-1 Effectiveness:

- *E-1.1 Completeness:* Increases as more assets, vulnerabilities, threats and risks are identified.
- *E-1.2 Accuracy:* Increases due to the intelligence input from knowledge center.

- *E- 1.3 Frequency:* Increases due to explicit consideration of the monitoring policies and process.
- *E-1.4 Adaptability:* It does not decrease or increase adaptability. RACI+ Charts would need to re-made only when there is too much of a difference in a certain process, in which case, the whole risk assessment would need to be repeated any way.
- *E-1.5 Alignment to business objectives:* Increases as mentioned in Section 6.1
- *E-1.6 Data presentation to management:* No effect.
- *E-1.7 Output artifacts:* Increase. RACI+ Charts would be maintained which would help in each upcoming cycle or whenever issues arise. Moreover, IKOSST mentions policy and SOP making for risk communication.
- *E-1.8 Interoperability:* Increases as mentioned in Section 6.1. It is not dependent on or restricted to any one method.

6.2.2 Efficiency

- *E-2.1 Input Sources required:* Increase (decreases efficiency). Input for RACI+ activity and KC would be needed in any form.
- *E-2.2 Automation available:* No effect.
- *E-2.3 Preparation/Working required:* Increases as RACI+ might not already be made for all processes. Also, amount of working would increase due to analysis of RACI+ Charts (efficiency decreases). However, in our experimentation, the whole activity consumed around 2-3 hours for each process.

6.2.3 Economy

- *E-3.1 Personnel required:* No effect
- *E-3.2 Method Costs:* No effect. Information from KC cannot be anticipated as either free of cost or paid; therefore its effect cannot be judged in this research.
- *E-3.3 Other Sources of economy:* No effect

6.2.4 Ease-of-use

- *E-4.1 Trainings Required:* No effect
- *E-4.2 Calculations Required:* No effect.
- *E-4.3 Flexibility* No effect
- *E-4.4 Support available:* No particular effect on the underlying ISRM method. However, for IKOSST itself, a complete step-by-step specification document is available.

6.3 Bridging the deficiencies identified in the literature

Table 6.3 shows how IKOSST bridges the deficiencies that were identified in the literature.

Critical analysis of previous initiatives i.e. how none of them comprehensively covered these deficiencies has already been discussed in literature review.

6.4 Validation of Results

The following ensured validation in Risk Assessment results.

- Standard formulas were used. Both the formulas map on to the Risk Formula of ISO 27001 [9]. The formula is: "Risk= $Impact/asset - value \times Likelihood$".
- Asset owners were consulted for asset identification, asset valuation, control assessment/threat identification, RACI+ charts consistently throughout the two phases. This ensured accurate and valid information.

Deficiencies identified in literature	**How IKOSST addresses them**
Omissions in Risk Identification: Risks related to intangible knowledge Assets or fluid assets ([12], [13], [8], [11], [26])	Presence and flow of intangible knowledge identified within process activities (RACI+ Activity)
Omissions in Risk Identification: Vulnerabilities arising out of complex relationships among multiple information assets ([8])	Interaction of multiple assets incorporated in RACI+ Activity
Accuracy: Results not based on evidence ([8])	(1) KC would help estimate likelihood of risks more accurately (2) Evidence and better judgment from RACI+ activity
Risk Assessment infrequent([8])	Risk Monitoring Policy and Process making mandated
Inability to learn from past incidents for the benefit of ISRM ([8])	Risk communication includes communicating relevant information to all stakeholders. Audit reports and information about emerging threats, vulnerabilities or incidents must be communicated to KC. Input from KC would include processed information about past incidents as well.
Knowledge sharing risks not identified ([10], [39], [40], [41], [42], [44], [45])	Knowledge sharing activities and processes would be identified in RACI+. Risks explicit to them would thereby be considered. For e.g. risks due to a certain email activity was considered during our experimentation.
Knowledge loss risks not identified ([31], [40], [43])	Dependence of any one individual would be identified in the RACI Activity. Moreover, a knowledge capture process for this purpose is given In the IKOSST-Specification Report.
Omissions in Risk Identification: Emerging indications of malicious threats, Complex attack scenarios ([8])	The intelligence from KC can help in an ISRM process by giving accurate and timely information about emerging vulnerabilities and threats (input arrow into Risk identification phase).

Table 6.3: IKOSST bridges ISRM deficiencies

Chapter 7

Conclusion and Future Work

7.1 Conclusion

In the first phase of this thesis, we have developed a framework for assessing ISRM methods and improvement techniques (RiskE4). The framework is composed of a taxonomy of evaluation factors and a correlation table that demonstrates interdependencies amongst them. From an industrial perspective, our proposed framework can be used by organizations for evaluating ISRM methods that they have enforced or plan to enforce. From research perspective, the framework can be used to provide a comparison baseline for different standard ISRA/ISRM methods and also for categorizing improvement attempts from the past while identifying areas that have not been addressed but may still be important for any particular type of organization.

In our research, we have surveyed such improvement attempts and analyzed them using the taxonomy. We have also categorized them according to their detail level (hypothesis, theoretical model or practical framework), the types of controls suggested (strategic, technical or operational) and the evaluation method utilized (survey questionnaires, practical enforcement or none). Findings suggest that researchers have focused on introducing knowledge assets' risk assessment in ISRM. However, only few of the techniques have been tested practically in an organization and a comprehensive technique covering all aspects of knowledge risk management is still lacking.

In the second phase of our thesis, we have developed a framework (IKOSST) for the improvement of ISRM techniques. We have experimented this framework under a limited scope in two organizations and obtained excellent results. The main benefits of the framework stem from the inclusion of the RACI+ activity in the asset identification phase although other benefits are also present as discussed in this document. IKOSST bridges all major limi-

tations identified in the literature, at the expense of an extremely minor decrease in efficiency. The overall effectiveness is increased by a much greater extent and there is no significant change in the economy and ease-of-use. The risk team of GreenCo had extremely positive views about the usability and benefits of RACI+ charts. They expressed their wish to utilize them for various other business activities as well.

7.2 Future Work

- RiskE4 can be used as such by researchers for comparing different ISRM methods theoretically or for analyzing the merits and demerits of any future techniques. However, if an organization needs to select an ISRM method based on their priorities, an additional step might be required. From the determining factors, it might not be exactly deducible as to how effective or how efficient a method is. For instance, completeness might be there but not business alignment. What overall impact this has on effectiveness cannot be deduced from the present work. This limitation can be bridged in future by carrying out a research on how much each of the determining factors contributes to its parent factor in the taxonomy (e.g. the extent to which accuracy contributes to effectiveness compared to adaptability). Research can be based on finding the amount of importance organizations give to each factor when striving to deploy an effective ISRM (similar to the approach used in [37]. Also, survey questionnaires to be filled by experienced practitioners or researchers can help reveal the weights for each determining factor.

- The correlation table of RiskE4 has many blank fields which might also be filled by carrying out future research. Once again, survey questionnaires could be one way to do this. Also, the methods deployed in different organizations can be evaluated and the trend of correlation among different factors can then be analyzed based on the results. Comparison of different standard methods (CRAMM, OCTAVE, NIST SP 800-30 etc) based on RiskE4 is another potential future direction.

- Evaluation and results for IKOSST can be made more comprehensive and even more reliable by deploying it in an enterprise-wide case study. A theoretical survey about its ability to improve ISRM may be performed in future once again through questionnaires targeting experienced risk practitioners.

Appendix A

Specification Report: IKOSST

A.1 Overview

Information security risk management (ISRM) is the process of identifying, analyzing and quantifying risks posed to an organization. It builds upon by identifying vulnerabilities in the organization's assets and depicting threat scenarios that may result due to those vulnerabilities. Deficiencies or inaccuracies in the ISRM process can be critical as it may result in a false sense of security or overconfidence. This report aims to enhance the ISRM process in an attempt to reduce the deficiencies identified by the research community at large, and to bring an overall improvement within the process. The flow/ process of Risk management given in the International Organization for Standardization's (ISO) Standard 27005:2008, Information technology – Security techniques – Information security risk management is taken as a reference model and extensions are proposed within particular steps of this process. It is assumed that the reader of this report has some basic knowledge of information security and risk management.

A.2 Purpose

The purpose of this report is to propose and theoretically explain a framework, "IKOSST (an Improved Knowledge and infOrmation Security riSk managemenT framework)" that reflects an improved ISRM process. It is intended that this report be used as a guideline by the Information Security industry and research community for achieving better results in ISRM. From a high level perspective, the following improvements are anticipated:

(a) A wider scope for asset identification that includes fluid/ dynamic information and knowledge assets, apart from the static ones inherent in the

current ISRM methodologies.

(b) Enhanced accuracy in threat identification and risk estimation

(c) Ensuring that monitoring/ review is performed after the completion of first ISRM process, at intervals specified in International Organization for Standardization's (ISO) Standard 27005:2008, Information technology – Security techniques – Information security risk management

(d) Ensuring that risk communication/ feedback dissemination is carried out with relevant stakeholders,

A.3 Scope

IKOSST is generic and intended to be applicable to all organizations regardless of type (e.g. commercial enterprises, government agencies, non-profit organization), size (e.g. small, medium, large) and nature (health, financial, telecommunication, logistics or manufacture etc.).

A.4 Normative References

[**ISO-27000**] ISO/IEC 27000:2014 Information technology Security techniques Information security management systems - Overview and vocabulary;

[**ISO-27001**] ISO/IEC 27001:2013 Information technology Security techniques Information security management systems Requirement;

[**ISO-27005**] ISO/IEC 27005:2008 Information Technology Security Techniques Information Security Risk Management;

A.5 Non-normative References

[**NIST-SP-800-150**] Johnson, C., Badger, L., & Waltermire, D. (2014). Guide to Cyber Threat Information Sharing [draft].NIST special publication, 800-150.

A.6 Terms and Definitions

For the purpose of this document, the definitions given in [ISO-27000] apply. Some additional definitions are as under.

A.6.1 Accountable

Person who has the authority to take decisions and is ultimately accountable.

A.6.2 Consulted

Person whose contribution is required for the activity.

A.6.3 Explicit Knowledge

Knowledge that can be easily codified (documented/written down).

A.6.4 Informed

Person who has been assigned tasks dependent on the activity. He is kept always informed about the progress of the activity.

A.6.5 Knowledge

Ideas, observations, facts, opinions, skills or expertise residing within an individual's mind acquired through experience.

A.6.6 Responsible

Person who actually performs an activity.

A.6.7 Tacit Knowledge

Knowledge that is difficult to code (document/ write down), but can be transferred to another individual, up to a limited extent through extensive socializing.

A.7 Structure of this Report

Information already present in [ISO-27005] is not repeated, except where necessary in order to avoid ambiguities.

The framework, "IKOSST" is illustrated and explained in Section A.8. [ISO-27005] structures ISRM process' activities by laying out the required input, action, implementation guidance and output for each. In this report, input, output and action for all activities are same as those in [ISO-27005]. Only the implementation guidelines differ and hence only these are explained in the sections that follow.The reader may refer to [ISO-27005] for the meanings of the terms: input, action, implementation guidance and output.

Additional Information is provided in A.8.5 and A.8.6.

A.8 IKOSST Framework

Figure A.1 illustrates the "IKOSST" framework. It is similar to the ISRM process given in [ISO-27005]. Extensions are colored "purple". Arrow directions show the flow of input and output.

A.8.1 Knowledge Center (KC)

This is not an activity but has been mentioned explicitly in order to emphasize its significance with respect to the benefits it may produce. This may be a nationwide, local an or organization specific body. It takes information from Computer Emergency Response Teams (CERT), industry and other sources and processes it to produce accurate and aggregated intelligence (similar to the concept of Cyber Threat Intelligence (CTI). In essence, KC is envisaged to be of the centralized hub-and-spoke architecture described in [NIST-SP-800-150]. The role of KC in ISRM process and the arrow directions to and from KC in Figure A.1 are explained below.

The intelligence from this knowledge center can help in an ISRM process by giving accurate and timely information about emerging vulnerabilities and threats (hence the input arrow into Risk identification phase). Sources such as NIST Vulnerability database, audit reports from different organizations etc. can give information but KC would process it into intelligence. The input arrow into Risk estimation phase is derived by the fact that KC would also help estimate likelihood of risks more accurately, as information from reliable sources would be aggregated and analyzed by experts to convert into intelligence. Risk communication includes communicating relevant information to all stakeholders. Audit reports and information about emerging

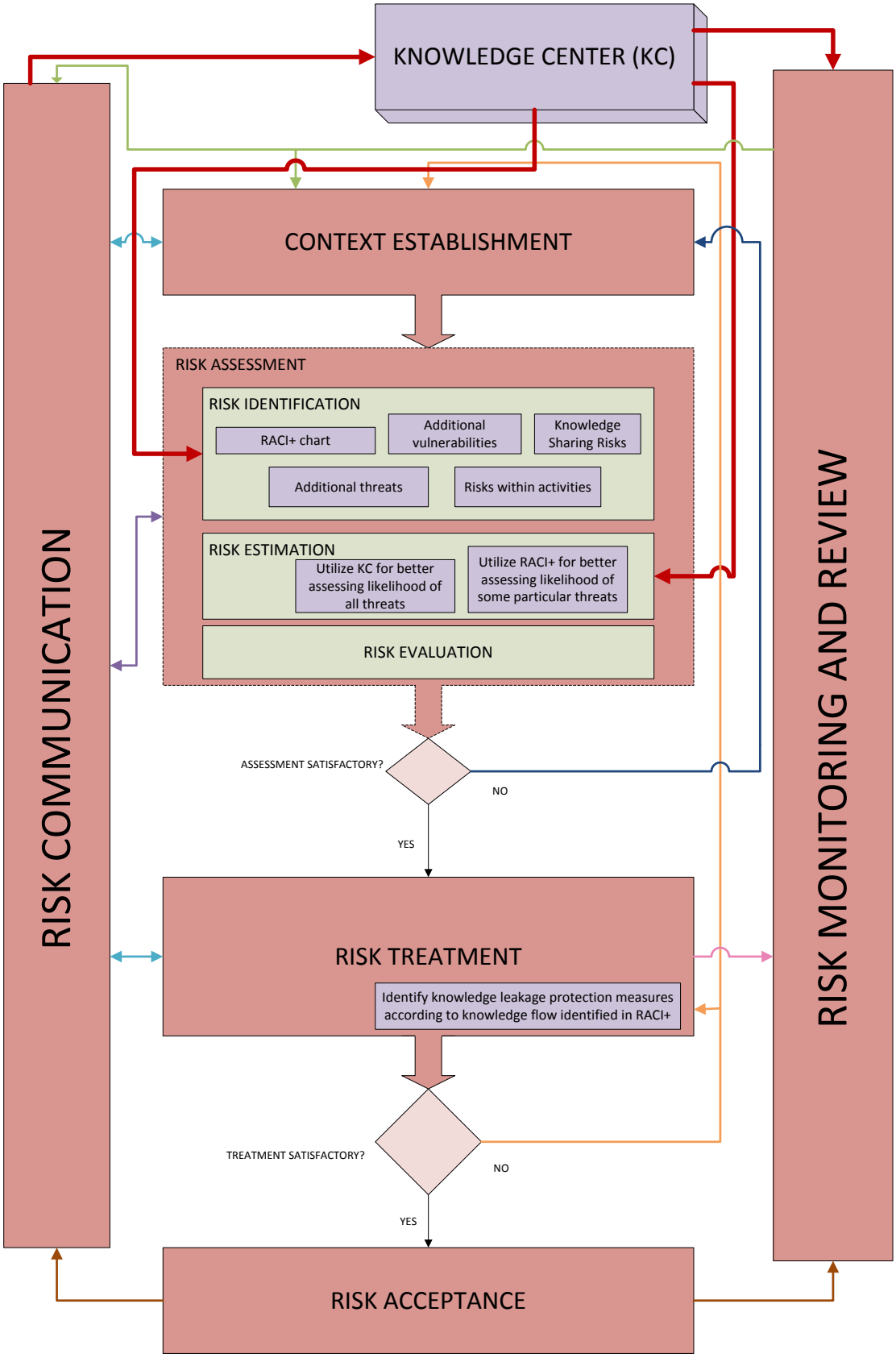

Figure A.1: "IKOSST" Framework

Process Name:							
Activity	Responsible	Accountable	Consulted	Informed	Confidential Documents	Confidential Knowledge	Other Stakeholders
Activity 1							

Table A.1: Example layout for RACI+ chart

threats, vulnerabilities or incidents must be communicated to KC, therefore justifying the output arrow direction from this phase. All these activities are repeated in the Risk monitoring and review stage;hence an input arrow terminates at this phase as well.

A.8.2 Context Establishment

There is no change in this phase compared to [ISO-27005].

A.8.3 Risk Identification

Risk Identification includes "Identification of assets, Identification of threats, Identification of vulnerabilities, Identification of existing controls and Identification of consequences".

A.8.3.1 Identification of assets

Different processes which fall under the risk management scope of the organization should be ascertained initially. The processes can be categorized according to departments/wings. For each process, assets under all other categories can then be listed. Asset identification scope is improved with the introduction of RACI+ chart activity within the asset identification phase. The format of the chart is illustrated in Table A.1. The chart is similar to any RACI chart created for the purpose of project management, except the following two.

Asset identification scope is improved with the introduction of RACI+ chart activity within the asset identification phase. The format of the chart is illustrated in Table A.1. The chart is similar to any RACI chart created for the purpose of project management, except the following two.

- The inclusion of three extra columns (hence the name RACI+).

- Instead of listing the team in the top row, and recording the alphabets R, A, C or I under each name, the latter are recorded in the top row and the team names underneath. This is so done because the extra column, "stakeholders" may include different names for each activity. These names may not be static for the process but may even include entries such as "The whole XYZ department".

The benefits that can be derived from this activity are numerous. Within the asset identification phase, the process of listing activities can help identify fluid/ dynamic assets e.g. emails, documents created within the process etc. Also, some static assets may also be identified that could have been missed out in the traditional asset listing.

Recording the involvement of confidential documents, confidential knowledge and any stakeholders other than those responsible, accountable, informed and consulted in the activity, would help determine the flow of information and knowledge assets within the organization. This would further help determine controls such as the need for compartmentalization, training requirements, legal declaration signatories etc.

Since IKOSST emphasizes input to and out from a centralized knowledge center, the process of "knowledge sharing" must also be considered and a RACI+ chart made for it. The details of this are mentioned in A.8.6.
Note: *The stakeholder field must not be confused with the "Supportive" field in a RASCI chart. The former is meant to record any person who has access to the confidential knowledge or information asset involved in the activity. The "supportive" field may be considered a subset of the "stakeholders" field.*

The rest of the activity would be followed the same way as given in [ISO-27005].

A.8.3.2 Identification of vulnerabilities

With the inclusion of RACI+ chart, some additional vulnerabilities may be identified and some previous ones may be better assessed. Some of these are mentioned in A.2.

The rest of the activity would be followed the same way as given in [ISO-27005], except for the inclusion of the input from the Knowledge Center as described in A.8.1.

A.8.3.3 Identification of threats

Threats corresponding to the vulnerabilities mentioned in A.8.3.2 would be identified (examples in Table A.3). Additionally, the threat of knowledge or

Vulnerability	**Description**
Improper Workload Management	Too many responsibilities on one employee; too less on another; Irrespective of the number of consulted personnel
Lack of proper definition of roles, responsibilities, accountability etc.	Process owner is unable to give names for RACI or the team shows disagreement with his given names and there is no way the process owner can prove them wrong.
Lack of segregation of duties	Other people are consulted for the activity but there is one (or more) individual who is involved in ALL Critical activities of a process. He has all the critical knowledge and access to critical resources.
Heavy dependence on any one individual	Too many activities in which the same person is responsible and very less number of other people are consulted.

Table A.2: Description of additional (or better assessed) vulnerabilities

information leakage can be better assessed by analyzing the knowledge or information flow.

For reader's clarity, the threat of "knowledge loss" and "Activity slow down due to an employee's absence" are distinguished in Table A.4.

Additionally, we also suggest that the following two threats must ALWAYS be considered by organizations when deploying ISRM, and especially when aiming for [ISO-27001] compliance.

- Threat that the organization would not be able to monitor or review ISRM periodically or when major changes in the organization occur.
- Threat that the organization would not be able to communicate relevant information to respective stakeholders. (Both over-communication and under-communication must be considered as threats as both can have a negative impact on the organization's security posture).

Some additional information about the above two threats is provided in Appendix A.8.5. The RACI+ chart may also help identify threats within activities.

The rest of the activity would be followed the same way as given in [ISO-27005], except for the inclusion of the input from the Knowledge Center as described in Section A.8.1.

A.8.3.4 Identification of existing controls and Identification of Consequences

The activity would be followed the same way as given in [ISO-27005].

A.8.3.5 Risk Estimation

This activity would be followed the same way as given in [ISO-27005], except that;

- Input from knowledge Center would help estimate likelihood better
- Likelihood of threats corresponding to vulnerabilities mentioned in Section A.8.3.2 would be assessed better through the picture obtained from RACI+ chart.

A.8.3.6 Risk Evaluation

The activity would be followed the same way as given in [ISO-27005].

A.8.3.7 Risk Treatment

For knowledge leakage mitigation, the data flow identified in the RACI+ chart would play its role while applying controls. The rest activity would be followed the same way as given in [ISO-27005].

A.8.3.8 Risk Acceptance

The activity would be followed the same way as given in [ISO-27005].

A.8.3.9 Risk Communication

The activity would be followed the same way as given in [ISO-27005], except for the inclusion of a formal organization policy and the output to Knowledge Center as described in Section A.8.1

A.8.4 Risk Monitoring and Review

The activity would be followed the same way as given in [ISO-27005], except for the inclusion of a formal organization policy and the input from Knowledge Center as described in Section A.8.1.

A.8.5 Additional Information

A.8.5.1 Risk Monitoring and Review

ISRM literature points out that, organizations fail to monitor or review ISRM at required intervals. This is especially the case when their main purpose of deploying ISRM is to get one-time compliance. However, this can cause security risks as the threat landscape evolves with time. For this reason, "IKOSST" emphasizes the need to realize this failure as a security risk as well. This would oblige the organizations to consider and implement controls that may help avoid such a situation. These may include:

(a) Developing and enforcing a policy for Risk Monitoring that defines roles and responsibilities and the timing for risk monitoring.

(b) Defining and observing a systematic process for Risk Monitoring that defines the activities involved and their order, such as reviewing the risk acceptance criteria, conducting an internal/external audit, recording changes in assets or competitors etc.

A.8.5.2 Risk Communication

Risk communication, especially which involved with the knowledge center may bring in risks too. These can be reduced by defining a systematic process for risk communication. This process must then be considered in the asset identification phase (in an enterprise wide ISRM), and a RACI+ chart must then be defined therein, This would help determine the information/ knowledge flow involved in risk communication and therefore analyze, quantify and treat the risks accordingly.

A.8.6 Knowledge Capture Process

[ISO-27001] does not define any specific control for the threat, "Knowledge/ skill loss". As part of IKOSST, an example knowledge capture process is proposed in this report (Figure A.2).

The following key points explain Figure A.2.

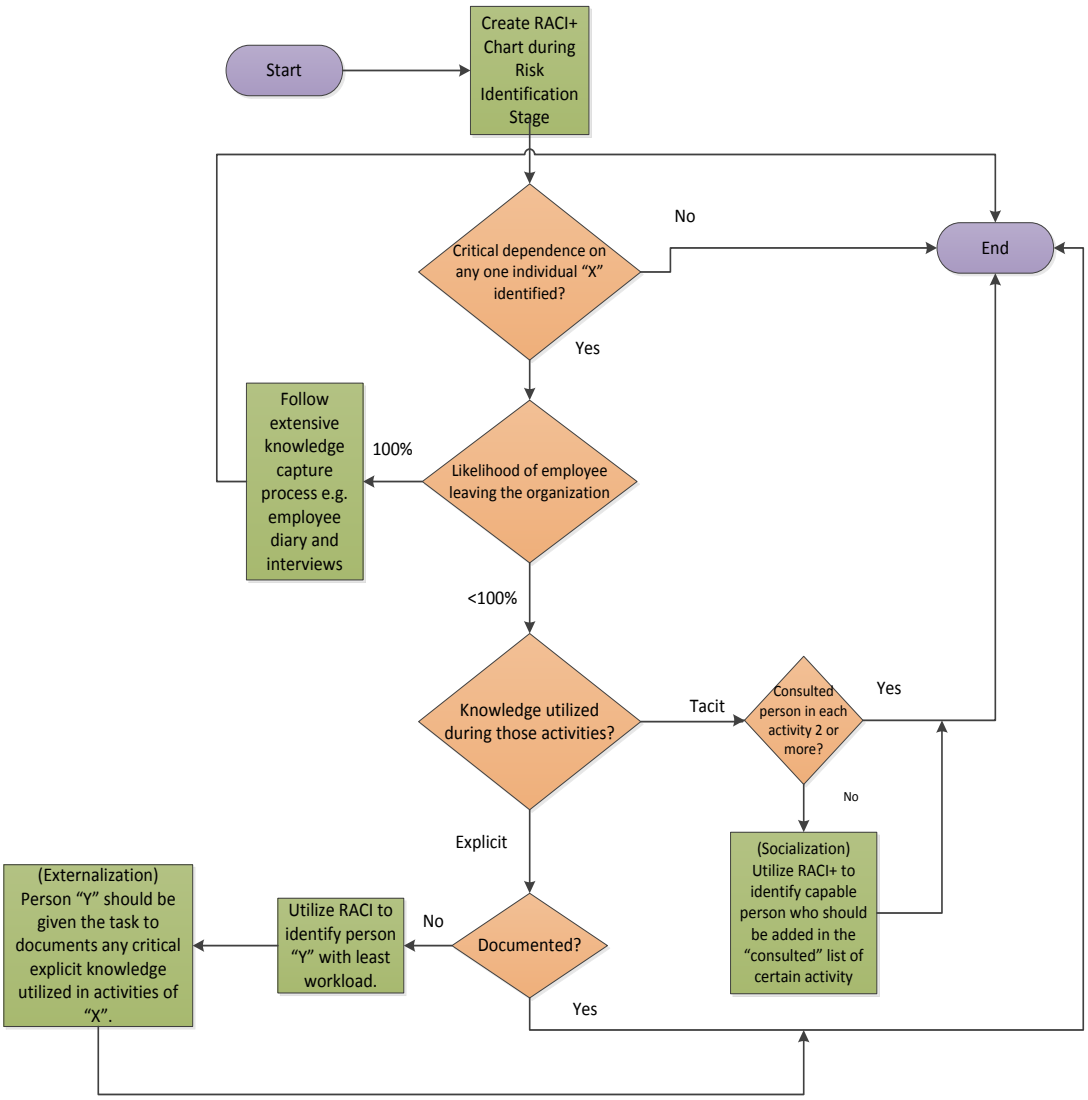

Figure A.2: Example Knowledge Capture Process

1. As a first step, the RACI process would help identify whether any critical process depends too much on a single individual. If yes, knowledge capture process would be needed, else not.

2. If there is 100% certainty of the employee leaving the organization (e.g. if he has already informed of any decision of leaving or the organization has decided his termination etc), then a formal and detailed process of knowledge capture would be required. This can include training a new

hire/ fellow employee, mandating the employee to keep a record of his activities (e.g. in a knowledge capture diary) in his last days, (at least) one person shadows him in all activities and discusses his diary with him, formal interviews (at least one) are conducted with him in order to discuss his work and plan out a strategy of how it would be carried out in his absence.

3. If it is not certain that the employee is leaving the organization, some informal/ less strict process of knowledge capturing must still be in place. This is so because the employee might still leave any time due to any unprecedented reasons. For this, separate strategies for tacit and explicit knowledge would be required each.

4. For explicit knowledge, if it is already documented, then no action would be required. Else, explicit knowledge would need to be preserved in documented form through the methodology of externalization. The task of documenting explicit knowledge may easily be assigned to someone with comparatively less workload (he must have the basic knowledge needed for the process). An example is creating an application manual, or documenting how each customer's query should be handles (in case of customer services process for instance).

5. If tacit knowledge is shared among many individuals, then the chances of losing that knowledge decrease, as many people are aware of the situation/ Else, tacit knowledge would need to be preserved through the methodology of socialization. At least two personnel must be consulted for critical activities. Increasing the number of "consulted" people would ensure preserving.

Note: *The constraints given in Annex F of [ISO-27005] would always also be considered for the knowledge capture process. A cost-benefit analysis would lead the organization to decide about this process (or a similar one) is needed or not. Generally, knowledge capture process would need to be deployed for processes where availability/ smooth working is of more importance than confidentiality (e.g. student fee calculation). On the other hand, a process where confidentiality is of the highest priority, any sort of knowledge capturing would need to be avoided (and knowledge sharing overall reduced by keeping knowledge tacit and compartmentalized (least number of consulted people).*

Vulnerability	**Threats**
Improper Workload Management	• Threats due to a disgruntled employee • Business user errors due to too much workload • Knowledge/ skill loss
Lack of proper definition of roles, responsibilities, accountability etc.	• Repudiation • Inefficient progress of activities
Lack of segregation of duties	• Threats due to lack of segregation of duties; too much power in one hand; Knowledge leakage
Heavy dependence on any one individual	• Activity slow down due to an employee's absence • Knowledge or skill loss

Table A.3: Threats due to additional vulnerabilities

	Knowledge or Skill loss	**Activity Slow Down**
Description	The organization doesn't have an employee with suitable expertise/skill/knowledge for the activity	An experienced and active employee leaves (temporarily or permanently). There are other employees in the organization with appropriate skill to carry on his activities but they are unable to do so, as they were not aware of the progress/ working style of the previous employee (e.g. where he had stored certain file, what methodologies he was using etc.)
Mitigation	Can be mitigated by job rotation	Can be mitigated by increasing "consulted" people in the activity
Estimation	Depends on absent) employees' education and experience	Depends on the number of activities the absent employee was responsible for

Table A.4: Distinguishing knowledge loss from activity slow down

Appendix B

User Manual-Risk Assessment-GreenCo

B.1 Objective

The manual should enable you to use Risk Registers for effective Risk Management, thereby allowing you to identify different types of risks to particular categories of assets of the Commission.

B.2 Method

The risk register in the form of an excel workbook. Steps and guidelines for filling sheets within that workbook are explained below. You can fill the sheets using the information provided in this document along with the general concepts regarding Information Security Risk Management (ISRM). For your ease, some rows of the sheets have been filled with hypothetical data and provided in this document in the form of tables. Where possible, use assets and threats that are specific to your division/department/wing, in order to aid understanding and practice.

B.3 Outcomes

In the worksheets you will,

1. Identify threats to information assets
2. Identify vulnerabilities corresponding to each threat

Value	Security Requirement		
	Confidentiality	Integrity	Availability
3	The dissemination of information has high impact on the business or on the enforcement of existing legislation.	The lack of integrity of information has high impact on the business or on the enforcement of existing legislation.	The asset cannot be unavailable for more than a day.
2	Eventual spread has high impact on the business or on the enforcement of existing legislation	Lack of integrity does not have a high impact on operations or on the enforcement of existing legislation.	It may be unavailable for a day or more , but not more than one week
1	No particular requirements of confidentiality. Classification is public.	No particular requirements of integrity.	Asset may be unavailable for a week or more

Table B.1: Criterion for assigning CIA values

3. Identify controls implemented in your department/wing and assess their effectiveness

4. Calculate risk values

5. Identify risk reduction actions

6. Prepare risk acceptance justifications

B.4 Using Risk Register

B.4.1 Asset Grouping

The "service asset_register" sheet in your excel workbook should contain the columns as shown in Table 1. Fill in this table according to the assets of your department/wing. You may copy the contents of your asset register, whereby you have already listed down the assets, indicated their CIA ratings, determined their type etc.

Guidelines for assigning CIA values are given in Table B.1.

In this sheet, Assets with similar security requirements can be grouped together. Insert the asset names in the "sub-grouping" column and group names in the "Data (Information) and Services" column.

Fill in the "service asset register" sheet in your excel workbook, as shown in Table B.3. You have already grouped your assets in Table B.2. In the service asset register, mention each group only once, in the "Data (Information) and Services" column. Fill in the CIA Values, Assets Values and

Data (Information) and Services	Primary or Supporting Assets?	Type of Asset	Sub-grouping	Description	Classification	Confidentiality	Integrity	Availability	Asset Value	Asset Ranking
ISMS Documents	Primary Assets	Information Asset	Information Security Policy		PUBLIC	1	3	1	3	LOW
ISMS Documents	Primary Assets	Information Asset	ISRM Scope Documents		PUBLIC	1	3	1	3	LOW
ISMS Documents	Primary Assets	Information Asset	ISRM Strategy Document		PUBLIC	1	3	1	3	LOW

Table B.2: Asset Sub Grouping

Data (Information) and Services	Primary or Supporting Assets?	Type of Asset	Classification	Confidentiality	Integrity	Availability	Asset Value	Asset Ranking
ISMS Documents	Primary Assets	Information Asset	PUBLIC	1	2	2	4	LOW
Data Center	Supporting Assets	Physical Assets	SENSITIVE	2	3	2	12	MODERATE
Enterprise ISMS Services				2	3	2	12	MODERATE

Table B.3: Service Asset Register

Ranking for the grouped assets. The "classification" in Column R would be filled according to your organization's asset classification policy.

B.4.2 Risk Identification

Your assets face certain risks if vulnerabilities exist corresponding to particular threats. Therefore, risks are identified by identifying threats and vulnerabilities. The "threats" worksheet in the risk register is similar to Table B.5. Thereby, you have to identify threats and vulnerabilities. Different threats from particular categories have already been listed. Threats from the following categories are identified for each service.

(a) Physical Damage;

(b) Natural Events

(c) Loss of essential services;

Criteria for the evaluation of THREATS	
Value	**Guideline**
1	The threat is extremely unlikely, because of the unattractiveness of the information or the environmental conditions in outline.
2	The threat is likely on average, no more than the normal parameters established by the statistics of the most famous incidents of information security.
3	The threat is likely to occur equal to or more than those usually established by the statistics the most famous incidents of information security.

Table B.4: Criterion for the evaluation of THREATS

(d) Compromise of information;

(e) Technical failures;

(f) Unauthorized actions

(g) Compromise of information

If a particular threat exists for your service, identify any vulnerability that may cause that threat to realize. Assess and add likelihood (probability) of that threat occurring. For threats that do not apply to any assets of your service or for which no vulnerabilities exist, leave the likelihood column blank.Columns F-I have already been filled. They represent Whether the threats affect an asset's confidentiality, integrity or vulnerability. Whether the threat is environmental, human deliberate or accidental For filling in the vulnerabilities, you may pick and choose vulnerabilities given in the "threat-vul pairs" sheet present within the workbook. Vulnerabilities have been mentioned corresponding to each threat. Please note, these are just for a reference. It is suggested that vulnerabilities be ascertained according to the context of your service/process/organization. For assessing likelihood values, please use the criterion given in B.4.

B.4.3 Control Assessment

In the controls sheet of your workbook, fill in the "control assessment" according to the criteria given in Tables B.6. A portion of the "controls" worksheet is shown in Tables B.7 and B.8.

Threat Category	Threat	Vulnerabilities	Likelihood	Justification
Physical Damage	Fire	Equipment sensitivity to temperature	1	Building is protected with Fire Fighting equipment
Compromise of Information	Disclosure	No CCTV, No clear screen policy	2	Approved Information identification, classification and valuation guide

Table B.5: Risk identification

Criteria for the evaluation of CONTROLS	
Value	**Guideline**
3	The control is implemented in a systematic way, in line with the best practices in force and no possible improvements can be identified.
2	The control is implemented in a systematic way, in line with the best practices. However, there are possible improvements.
1	The control is not implemented or is implemented in a non-systematic and uncontrolled way. The control is not applicable (and a justification must be given).

Table B.6: Criterion for the evaluation of CONTROLS

Security controls	Control assessment	Justification	Description	Related documents
5.1.1 Policies for information security	3			Policies, Process, Procedures etc.
5.1.2 Review of the policies for information security	3			

Table B.7: Control Assessment (Columns A-E)

Type of asset						
Primary Asset	**Supporting Asset**					
[Digital /Non-Digital]	**Human Resource /Assets**	**Intangible Assets**		**Physical Assets**		
Information Asset	**Organization /People**	**Software**	**Process /Service**	**Data Center /Record Room**	**Equipment, storage media etc.**	**Building**
x	x		x	x		
x	x		x	x		

Table B.8: Control Assessment (Columns F-M)

Threat /Risk	Risk Owner	Actual risk	Actual Risk Ranking	Security Control	Current Control(s)	Desired risk	Desired risk ranking
Software malfunctio n	HoD	9	MODER- ATE	Separation of development, testing and operational environments	Policy has been approved i.e. Established	3	LOW

Table B.9: Reduction Actions (Columns B-I)

Risk reduction action			
Action	**Deadline**	**Responsible**	**Accountable**
A separation project will start at XYZ date	Month' Year	Personnel XYZ	Personnel XYZ

Table B.10: Reduction Actions (Columns J-M)

B.4.4 Risk Calculation

In the 4 th row of your "risk calculation sheet", insert the CIA values that were obtained for your service. Copy these from the last row of the "asset register".

Copy the "likelihood" values and the "control assessment" values from the "threats" and "controls" worksheet respectively.

The rest of the values in the sheet would be calculated automatically, according to the formulas added.

Generally, the formula utilized is:

Risk = $Likelihood \times AssetValue$; where Asset Value is ascertained from its CIA rating. If an asset/service has CIA value of 3, 3, 2 and a particular threat affects it's confidentiality only, then the asset value in the calculation of the risk due to that threat would become 3. If the threat affects Confidentiality and availability, the maximum of the two would be taken i.e. confidentiality value "3".

Rows 11 to 14, estimate the value of particular controls with respect to each threat e.g. "To what extent is the lack of Control X raising the risk due to threat Y".

B.4.5 Risk Reduction

Record the reduction actions in the "reduction action" sheet. A sample portion of it is displayed in Table B.9 and B.10. You need to suggest reduction actions for risks that cross your organization's acceptance criteria, and which

Threat /Risk	Security Control	Risk level	Risk Ranking	Acceptance justification
Unauthorized use of equipment	Restrictions on software installation	9	MODERATE	For the moment, it would be difficult to have a project for this. To be reviewed next year.

Table B.11: Risk Acceptance Justification

you have decided to reduce by applying controls. Check the corresponding controls and fill in the "security control" in the context of the corresponding threat.

Also fill in any other controls that are being exercised in your department and which may reduce or nullify the effect of the particular threat.

Desired risk ranking is that which can be obtained after the enforcement of the suggested control(s).

Fill in the columns for actions required to enforce the controls, deadline by which the actions should be taken, person responsible and accountable for enforcement of the controls.

B.4.6 Risk Acceptance Justification

Provide justifications for risks that you have not suggested any controls for. A sample is provided in Table B.11.

Appendix C

User Manual-Risk Assessment-CMS

C.1 Objective

The manual should enable you to use Risk Registers for effective Risk Management, thereby allowing you to identify different types of risks to particular categories of assets of the Commission.

C.2 Method

The risk register in the form of an excel workbook. Steps and guidelines for filling sheets within that workbook are explained below. You can fill the sheets using the information provided in this document along with the general concepts regarding Information Security Risk Management (ISRM). For your ease, some rows of the sheets have been filled with hypothetical data and provided in this document. The formulae utilized are those from OCTAVE-S Risk Assessment Methodology of Carnegie Mellon Institute. The worksheets have also been developed similar to OCTAVE-S Worksheets. However, guidelines from ISO-27005 have also been kept under view.

C.3 Outcomes

By the end of this workshop, you will be able to,

1. Identify threats to information assets
2. Identify vulnerabilities corresponding to each threat

Impact area	**High**	**Medium**
Reputation	Reputation is irrevocably destroyed or damaged. It leads to more than or equal to 50% customer loss.	Reputation is damaged, and some effort and expense is required to recover. It leads to 10%-49% customer loss
Financial Loss	Yearly operating costs (or) One-time financial cost increased to the extent that the university cannot bear.	Yearly operating costs (or) One-time financial cost increased to the extent that the university can bear but will result in degradation of services.
Productivity	Staff work hours are increased by greater than 30%.	Staff work hours are increased between 10 % and 29%.

Table C.1: Example Risk Criteria

3. Assign likelihood and impact values

4. Calculate risk values and assign pool number according to OCTVAE-S Risk Matrix

C.4 Using Risk Register

C.4.1 Defining Risk Criteria

The "risk criteria" sheet is the excel workbook is there for recording the impact areas as per requirements given in[1]. An example of impact areas for an educational institute has been filled and shown below.

All the guidelines given in [3] would be followed for defining impact areas, criteria for "High, Medium, Low Risks, and for assigning priority values".

Example criteria have been filled and shown in Table C.1.

C.4.2 Asset Register

The guidelines given in [3] would be followed for recording information about the assets in the sheet "Asset Register". Columns have been prepared for recording information required in [3]. According to organizational context however, columns maybe added or removed. Examples have been shown in Table C.2.

Asset Info		Security Requirements			Most Important Requirement
Asset Code	**Asset Name**	**Confidentiality Requirement**	**Integrity Requirement**	**Availability Requirement**	
S-001	Servers	High. Only authorized personnel can access.	High	High. Must be available 24/7	Confidentiality
S-002	Workstations	Medium	Medium	Medium. Unavailability for up to few hours can be	Availability

Table C.2: Asset Register

Threat	Vulnerabilities	Risk	Probability	Reputation	Financial Loss	Productivity
Fire	No firefighting equipment installed	Unavailability of services and data loss	1	1	2	2

Table C.3: Risk Estimation (Columns F-L)

C.4.3 Risk Estimation

Risk Identification and estimation would be performed in the sheet "risk estimation" according to the guidelines given in [3]. For each critical asset:

- Threats would be brainstormed and recorded
- Vulnerabilities corresponding to each threat would be recorded
- Probability of threat occurrence would be estimated and recorded
- Impact Values (High=3, Medium=2 and Low=1) would be estimated and recorded for each impact area defined in "risk-criteria" sheet.
- Justification for giving probability values would be recorded
- Risk would be calculated according to the formula of Octave-Allegro[3]. The user would not need to calculate anything here as the formula is pre-embedded in the excel sheet.
- Risk Rating and Pool would be calculated for each risk. Formula for these is also embedded in the sheet. However, it may be changed according to organizational context as Octave-Allegro [3] does not strictly define it.

Risk Score	**Justification/ Current Controls**	**Risk Rating**	**Risk Pool**	**Risk Treatment**
9	1. Fire exits 2. Awareness and training 3. Temperature control systems	MODERATE	POOL 3	Accept

Table C.4: Risk Estimation (Columns M-S)

Asset Name	**Threat**	**Threat-ID**	**Risk Owner**	**Actual Probability**	**Actual Risk**	**Desired probability**	**Desired risk**
Servers	Malware	THT-01	Personnel XYZ	Moderate	Moderate	Low	Moderate

Table C.5: Risk Reduction (Columns B- I)

- After risk evaluation, the reduction action chosen would be recorded with each risk entry.

Column "H" (Risk) is optional. It is there for describing the consequence of the threat.

Example data is shown in Tables C.3 and C.4

C.4.4 Risk Reduction

All the risks that have been decided to be reduced/ mitigated through the application of controls may separately be recorded in the "Risk Reduction" sheet, and their controls recorded therein. The "Actual probability" and "Actual risk" (Columns F and G) would come from the Risk Calculation sheet.The "Desired probability" and "Desired risk" (Columns H and I) would be the estimate of the risk's probability and risk value after the implementation of controls. Column "K" would record the practical steps that would need to be taken for the implementation of controls. Example data is shown in Tables C.5 and C.6.

C.4.5 Risk Acceptance

This is an optional sheet for recording the risks that fall under the acceptance criteria. Example data is shown in Table C.7. A column may be added for recording the justification for accepting the risks.

	Risk reduction action			
Recommended Controls	**Action**	**Deadline**	**Responsible**	**Accountable**
Technical vulnerability management (A.12.6 (ISO 27001:2013))	Install centrally managed Threat Management Software	Date XYZ	Personnel XYZ	Personnel XYZ

Table C.6: Risk Reduction (Columns J- N)

Asset Name	Threat	Probability	Risk Ranking	Acceptance Justification
Servers	Damaging of (host) system due a liquid (water) damage	LOW	MODERATE	Risks in POOL 3 are accepted in this phase

Table C.7: Risk Acceptance

C.4.6 Risk Avoidance

This is an optional sheet for recording the risks that have been decided to be avoided and the justification for this decision. If there is no "avoidance" option in the risk treatment criteria decided by the organization in the context establishment phase, this sheet would not be required anyway. Example data is shown in Table C.8.

C.4.7 Risk Transfer

This is an optional sheet for recording the risks that have been decided to be transferred to a third party as well as the justification for this decision. If there is no "transfer" option in the risk treatment criteria decided by the organization in the context establishment phase, this sheet would not be required anyway. Example data is shown in Tables C.9 and C.10.

Asset Name	Threat	Threat-ID	Risk level	Risk Ranking	Avoidance Justification
Servers	Hacking	THT-02	30	High	The company does not have enough resources for professional pen-testing and the applicable controls. Risk is too high and cannot be accepted as such.

Table C.8: Risk Avoidance

Asset Name	**Threat-ID**	**Risk Owner**	**Actual Probability**	**Actual Risk**	**Desired probability**	**Desired risk**
Server	THT-03	Personnel XYZ	High	High	Low	Low

Table C.9: Risk Transfer (Columns A, B, D, E, F, H, I)

External Stakeholder Involved	**Action**	**Deadline**	**Responsible**	**Accountable**
Company XYZ	Prepare contract and SLA with external stakeholder	Date XYZ	Personnel XYZ	Personnel XYZ

Table C.10: Risk Transfer (Columns J N)

Bibliography

[1] D. Shanthamurthy. (2011, May) Risk assessment as per iso 27005. Powerpoint slides. [Online]. Available: http://www.slideshare.net/praveenjvc/iso-27005-risk-assessment

[2] J. Weekes. (2011, February) 5 benefits of conducting risk assessments. Health and Safety Handbook. [Online]. Available: http://www.healthandsafetyhandbook.com.au/5-benefits-of-conducting-risk-assessments/

[3] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Octave allegro: Improving the information security risk assessment process (cmu/sei-2007-tr-012 esc-tr-2007-012)," *Software Engineering Institute at Carnegie Mellon University*, 2007.

[4] ENISA. (2015) Cramm product identity card. European Union Agency for Network and Information Security. [Online]. Available: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

[5] Z. Yazar, "A qualitative risk analysis and management tool-cramm," *SANS InfoSec Reading Room White Paper*, 2002.

[6] S. NIST, "800-30. guide for conducting risk assessments," 2011.

[7] R. Jacobson, "Cora. cost-of-risk analysis. painless risk management for small systems," *International Security Technology, Inc*, 1996.

[8] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Computers & Security*, vol. 44, pp. 1–15, 2014.

[9] B. ISO, "Iec 27005: 2008," *Information Technology–Security Techniques–Information Security Risk Management*, 2012.

[10] I. Ilvonen, J. Jussila, H. Karkkainen, and T. Paivarinta, "Knowledge security risk management in contemporary companies–toward a proactive approach," in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*. IEEE, 2015, pp. 3941–3950.

[11] A. M. Padyab, T. Paivarinta, and D. Harnesk, "Genre-based assessment of information and knowledge security risks," in *System Sciences (HICSS), 2014 47th Hawaii International Conference on*. IEEE, 2014, pp. 3442–3451.

[12] P. Shedden, R. Scheepers, W. Smith, and A. Ahmad, "Incorporating a knowledge perspective into security risk assessments," *Vine*, vol. 41, no. 2, pp. 152–166, 2011.

[13] P. Shedden, W. Smith, and A. Ahmad, "Information security risk assessment: towards a business practice perspective," 2010.

[14] T. H. Davenport and L. Prusak, *Working knowledge: How organizations manage what they know*. Harvard Business Press, 1998.

[15] A. Tamjidyamcholo, M. S. B. Baba, N. L. M. Shuib, and V. A. Rohani, "Evaluation model for knowledge sharing in information security professional virtual community," *Computers & Security*, vol. 43, pp. 19–34, 2014.

[16] Y. S. Hau, B. Kim, H. Lee, and Y.-G. Kim, "The effects of individual motivations and social capital on employees tacit and explicit knowledge sharing intentions," *International Journal of Information Management*, vol. 33, no. 2, pp. 356–366, 2013.

[17] G. Harden, "Knowledge sharing in the workplace: A social networking site assessment," in *System Science (HICSS), 2012 45th Hawaii International Conference on*. IEEE, 2012, pp. 3888–3897.

[18] H. F. Tipton, *Official (ISC) 2 Guide to the ISSAP CBK*. Auerbach Publications, 2010.

[19] C. ISACA, "5: A business framework for the governance and management of enterprise it," *Rolling Meadows: ISACA*, 2012.

[20] V. Arraj, "Itil®: the basics," *Buckinghampshire, UK*, 2010.

[21] R. Schmittling and A. Munns, "Performing a security risk assessment," *ISACA Journal*, vol. 1, p. 18, 2010.

[22] A. Vorster and L. Labuschagne, "A framework for comparing different information security risk analysis methodologies," in *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*. South African Institute for Computer Scientists and Information Technologists, 2005, pp. 95–103.

[23] B. Karabacak and I. Sogukpinar, "Isram: information security risk analysis method," *Computers & Security*, vol. 24, no. 2, pp. 147–159, 2005.

[24] C. Sillaber and R. Breu, "Using business process model awareness to improve stakeholder participation in information systems security risk management processes," in *Conference on Wirtschaftsinformatik*, 2015.

[25] O. Altuhhov, R. Matulevičius, and N. Ahmed, "An extension of business process model and notation for security risk management," *International Journal of Information System Modeling and Design (IJISMD)*, vol. 4, no. 4, pp. 93–113, 2013.

[26] J. L. Spears, "A holistic risk analysis method for identifying information security risks," in *Security Management, Integrity, and Internal Control in Information Systems*. Springer, 2006, pp. 185–202.

[27] R. J. Mejias, "An integrative model of information security awareness for assessing information systems security risk," in *System Science (HICSS), 2012 45th Hawaii International Conference on*. IEEE, 2012, pp. 3258–3267.

[28] M. Korman, T. Sommestad, J. Hallberg, J. Bengtsson, and M. Ekstedt, "Overview of enterprise information needs in information security risk assessment," in *Enterprise Distributed Object Computing Conference (EDOC), 2014 IEEE 18th International*. IEEE, 2014, pp. 42–51.

[29] M. Sadok, V. Katos, and P. Bednar, "Developing contextual understanding of information security risks," in *Human Aspects of Information Security and Assurance, HAISA 2014*. Centre for Security, Communications and Network Research, Plymouth University, UK, 2014, pp. 1–10.

[30] N. Feng and X. Yu, "A data-driven assessment model for information systems security risk management," *Journal of Computers*, vol. 7, no. 12, pp. 3103–3109, 2012.

[31] M. E. Jennex and A. Durcikova, "Assessing knowledge loss risk," in *System Sciences (HICSS), 2013 46th Hawaii International Conference on.* IEEE, 2013, pp. 3478–3487.

[32] C. Sillaber and R. Breu, "Using stakeholder knowledge for data quality assessment in is security risk management processes," in *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research.* ACM, 2015, pp. 153–159.

[33] J. H. Eloff, L. Labuschagne, and K. P. Badenhorst, "A comparative framework for risk analysis methods," *Computers & Security*, vol. 12, no. 6, pp. 597–603, 1993.

[34] J. W. Freeman, T. C. Darr, and R. B. Neely, "Risk assessment for large heterogeneous systems," in *Computer Security Applications Conference, 1997. Proceedings., 13th Annual.* IEEE, 1997, pp. 44–52.

[35] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (isra)," *Journal of Information Security and Applications*, vol. 18, no. 1, pp. 45–52, 2013.

[36] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, nist800-30 and microsoft's security management guide," in *Availability, Reliability and Security, 2009. ARES'09. International Conference on.* IEEE, 2009, pp. 726–731.

[37] S. Lichtenstein, "Factors in the selection of a risk assessment method," *Information Management & Computer Security*, vol. 4, no. 4, pp. 20–25, 1996.

[38] A. Ahmad, R. Bosua, and R. Scheepers, "Protecting organizational competitive advantage: a knowledge leakage perspective," *Computers & Security*, vol. 42, pp. 27–39, 2014.

[39] P. Trkman and K. C. Desouza, "Knowledge risks in organizational networks: An exploratory framework," *The Journal of Strategic Information Systems*, vol. 21, no. 1, pp. 1–17, 2012.

[40] M. Manhart and S. Thalmann, "Protecting organizational knowledge: a structured literature review," *Journal of Knowledge Management*, vol. 19, no. 2, pp. 190–211, 2015.

[41] R. Aljafari and S. Sarnikar, "A framework for assessing knowledge sharing risks in interorganizational networks," *AMCIS 2009 Proceedings*, p. 572, 2009.

[42] K. C. Desouza, "Knowledge security: an interesting research space," *Journal of Information Science and Technology*, vol. 3, no. 1, pp. 1–7, 2006.

[43] A. AlHogail and J. Berri, "Enhancing it security in organizations through knowledge management," in *Information Technology and e-Services (ICITeS), 2012 International Conference on.* IEEE, 2012, pp. 1–6.

[44] M. Jennex and A. Durcikova, "Integrating is security with knowledge management: Are we doing enough?" *International Journal of Knowledge Management (IJKM)*, vol. 10, no. 2, pp. 1–12, 2014.

[45] K. Väyrynen, R. Hekkala, and T. Liias, "Knowledge protection challenges of social media encountered by organizations," *Journal of Organizational Computing and Electronic Commerce*, vol. 23, no. 1-2, pp. 34–55, 2013.

[46] C. ISACA, "4.1, usa, 2007."