Integrated Approach to Information Risk Assessment

Ece Kaner

A Thesis

in

Concordia Institute for

Information Systems Engineering

Presented in Partial Fulfillment of the Requirements
For the Degree of Master of Applied Science (Quality Systems) at
Concordia University
Montreal, Quebec, Canada

June 2008

Your file Votre référence
ISBN: 978-0-494-42528-2
Our file Notre référence
ISBN: 978-0-494-42528-2

ABSTRACT

Integrated Approach to Information Risk Assessment

Ece Kaner

The primary intent of this thesis is to contribute to information risk assessment process conducted in large organizations, by addressing important aspects within the process, its principles, the steps followed within a structured methodology. In this thesis, first, the existing methodologies, best practices, standards, and tools in information risk assessment are compiled and evaluated according to well-defined criteria. Besides this evaluation, an integrated information risk assessment methodology is developed that uses the high potential of the previous methodologies and addresses their identified deficiencies. The new methodology is validated with a case study.

Acknowledgements

I am grateful to all the people who have provided valuable contributions to this work, starting with my supervisor Professor Dr. Brigitte Jaumard and Acting Director of CIISE Professor Dr. Mourad Debbabi whose direction and guidance helped me to shape this work, Professor Dr. Amin Hammad and also to the departmental staff in CIISE who were very helpful through my thesis work.

I am thankful to have the opportunity to work with highly experienced professionals whom I have learnt a lot from and who have supported me throughout my academic work, starting with Mr. Kenneth Jones, Partner in Pricewaterhouse Coopers Advisory Practice in Toronto; Dr. David Jacobson, Director in Emerging Technologies in Pricewaterhouse Coopers Advisory Services Practice in Toronto; Mr. Denis Normand, Director of Information Security in SNC Lavalin, Montreal. I also thank Dr. Vedat Verter, from McGill University, Dr. Baris Balcioglu, from University of Toronto and Dr. Alpay Ozcan from Washington University for their friendship and support.

I would like to express my gratitude to my friends in Montreal who have been a tremendous support and finally to my dear family, my parents and my sister for their generosity, compassion and love.

Ece Kaner, on June 4th 2008

To My Mother

Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Motivations

In an increasingly uncertain world where people expect continuous quality service, information risk management is a necessity to ensure business resilience for all organizations. Those organizations that realize this need and decide to take proactive measures to ensure their information systems are capable of supporting continued operation of critical services, are capable of providing the legal and regulatory requirements of their operating environment, and meeting the expectations of their stakeholders.

In addition to assessing information risks, it is essential to provide cost effective approaches, with practical solutions and timelines, to protect the information assets against the negative impacts of the risks. In this respect, information risk assessment is known as a good practice and is carried out by organizations, on a periodic basis. This requirement is further enforced with respect to the regulatory environment.

Despite its necessity, extensive use and benefits, there is no single widely accepted definition of information risk assessment terminology or a method on how it should be

conducted. In this respect, the primary objective of this thesis is to contribute to information risk assessment by improving the state of the art in terms of methodology.

The challenge many organizations face is to prioritize the information risks and to propose an optimum protection strategy which is both adequate and cost effective, with the limited budget dedicated to security and impossibility of protecting each and every information asset of every department. An information risk assessment conducted within a structured framework on a periodic basis helps to prioritize the risks to information assets of the organization and take countermeasures to reduce the risks.

1.1.1 Need for Assessing Information Risks

Despite the fact that there have been significant improvements in the practice of information security practice; organizations still face wide variety of security incidents that have significant impacts upon them. There are also increasing regulatory requirements in terms of information security. The increasing need for information risk assessment depends on various factors. As outlined by Information Security Forum, some of these factors are listed as:

- New technologies and advancements in information security practice;
- Increasing number of threats and vulnerabilities;
- Increasing complexity and connection requirements of the organizations;
- Regulatory environment and its requirements;
- Expectations of management in performing more effective security programs;
- Increasing knowledge in information security in every level of staff that emerges a cultural change towards information security risk awareness.

Today's organizations are highly dependent upon information. While organizations are spending the effort to minimize the frequency and magnitude of incidents, hackers and other threat sources work on the opposite side to diminish the positive results of these efforts on the organizations. E-crime watch survey conducted, by US Secret Service and CERT [19], provides data on the type of threats experienced and impact of e-crimes.

In the complexity of today's organizations, information assets used by different departments are interrelated with each other through the IT infrastructure. Protecting all of these assets is very challenging, almost impossible. Information risk assessment is a tool to prioritize the risks so the organization is able to concentrate on high risk areas.

The regulatory environment is more demanding and creates an external pressure to comply with established regulations. The Sarbanes-Oxley Act [54] in the USA, corporate governance codes of practice; Turnbull in the UK [53] require management to demonstrate that reasonable actions are taken to manage and control risks including information risks. Senior management is asked to take precautions to manage information security risks more effectively, with the scarce resources and budget in information security. The IT Security budget is usually a part of the Information Technology Department's budget. However, independent of the size of the budget, it is expected that the information assets of the company are protected with effective security programs. In addition to this expectation, the investment decisions of the information security are being asked to be justified with its benefits.

The cultural change towards being aware of the information security risks has emerged from an increasing trend of interest from employees inside the organization and pressure from senior management. Events such as hacking, phishing, viruses, theft are major issues

and receive publicity, which diminishes the reputation of the organization. Media coverage on these issues ensured that they are recognized on a wider scale.

With respect to the above factors, we conclude that there is a burden on the practitioners to conduct more effective information risk assessments. For this purpose, information risk assessment methodology is conducted to set the foundation in protecting information assets of the organization.

1.1.2 Benefits of Assessing Information Risks

We also look at the benefits of conducting an information risk assessment. Most of these benefits are stated by Information Security Forum. Information risk assessment is the first step in managing information risks. It classifies critical systems and applications of the organization. It serves as a tool for compliance purposes, providing significant inputs to making informed decisions in managing information risks, preventing over-control as well as under-control and increasing awareness in information risks. It also helps to meet customer expectations, serving as a mechanism to lower insurance costs.

Information risk assessment helps an organization to understand its information risk profile. Risks identified within an organization's risk profile are those that may have potential negative impacts on the organization, which need to be recognized to take appropriate response actions.

The comprehensive assessment of the information risks helps to meet regulatory requirements and provides management with a clear picture of the risk profile within their organization. As a result of the risk assessment, controls applicable to the organization's needs are identified. Additional costs, liabilities, long term potential negative impacts of risks to the organization could be prevented if information risks are properly managed.

Another benefit is to meet legal and regulatory requirements. Organizations face increasing pressure from legislation and regulation, such as Sarbanes Oxley Act in US [54], Basel II [13], and Turnbull in UK [53]. Compliance with regulatory bodies extend to Financial Services Authority in UK, the Securities and Exchange Commission in US, and the Investment Dealers Associate in Canada, who drive organizations to carry out information risk assessments. An effective information risk assessment brings good corporate governance and enables an organization to demonstrate compliance to the regulations. The third parties, such as external auditors of the organization and the regulatory authorities benefit from this experience.

In the absence of an information risk assessment, controls can be implemented arbitrarily, leading to unnecessary costs or points where there is over-control according to the risk level. Information risk assessment provides a structured system, through prioritization of information risks, enabling the selection of appropriate controls as countermeasures for the risks identified and analyzed. This helps to select controls that are cost effective.

A significant benefit of the information risk assessment is increased awareness in information security. As majority of the threat sources are inside the organizations compared to external threat sources, awareness and adequate security knowledge of staff are critical in the smooth running of day to day operations.

In order to optimize supply chain efficiency in a complex supply chain management structure, as well as, to minimize timescales required to get products to the market, require increased collaboration with suppliers. [20] New business initiatives, such as e-commerce solutions enable increased collaboration, but also bring an increased risk of incidents for all parties. Many organizations are aware of these risks and they seek

assurance, specifically from their third party suppliers, via contractual agreements, periodic auditing, or other solutions. If their requirements are not met, customers will be unhappy and potentially seek more reliable suppliers who will provide goods and services to their satisfaction level.

The final benefit is the potential decrease on insurance costs. A cyber attack is perceived as high risk for insurance companies, and is more costly than other forms of insurance. Special e-risk insurance policies may no longer be required to cover the potential losses and liabilities associated with the cyber attacks, for an organization who conducted an information risk assessment.

With respect to the reasons stated and the benefits described, a vast range of activities are taken to ensure that the organization is adequately protected. With limited resources and budget, it is important to set the priorities appropriately and take adequate actions to manage them. Results of an information security risk assessment help to improve information security management in staffing, scheduling and budgeting pertaining to information security.

1.2 Objectives

The objectives of the research can be summarized as follows:

- A survey on the state of the art in information risk assessment methodologies, best practices and tools, accompanied with stand-alone analysis of existing methodologies for large organizations;
- Comparative study of selected methodologies, with analysis of their strengths and potential improvements, based on a set of criteria and scorecard established;

- Elaboration of an integrated information risk assessment methodology that leverages the potentials, improves weaknesses of existing methodologies and introduces new ideas;
- Validation of the proposed methodology through case study.

Our study and proposed approach provides benefits to the following reader groups:

- Academic professionals who are in the field of information security and risk management;
- Information risk management professionals who undertake developing an effective information risk analysis capability within their organization;
- Consultants who conduct a risk assessment within their client organizations; and
- The management tier in the organization sponsoring the information security program.

1.3 Thesis Organization and Contributions

The rest of the thesis is organized as follows:

- Chapter 2 includes a literature review of existing methodologies, tools and best practices in information risk assessment. To the best of our knowledge, we introduce all the existing methodologies, electronic tools, standards and best practices, used in assessing information risks. We detail the underlying phases of each methodology for large organizations and perform a stand-alone analysis by evaluating their strengths and weaknesses. We also discuss typical information risk assessment requirements.

- Chapter 3 is an elaboration of the comparative study of the selected risk assessment methodologies. We introduce a methodological approach designed to conduct a comparative evaluation of different methodologies in information risk assessment. The selected metrics represents the requirements of the present information risk assessment methodologies and helps building a well-defined and integrated methodology based on commonalities, differences, strengths and weaknesses of the present methodologies.

- Chapter 4 is a presentation of our integrated methodology, covering step by step how a risk assessment is to be conducted. Objectives, inputs and outputs of each phase are described, while activities to follow throughout the risk assessment are explained in detail. We construct further on the common points of the existing methodologies, by incorporating the strengths of the reviewed methodologies to the new methodology. We also address the weaknesses of the existing methodologies and propose new ideas in project management and organizational factors.

- Chapter 5 illustrates an example in undertaking of information risk assessment in an organization with a case study, in an attempt to demonstrate the improved quality and management of information risk assessment process.

- Chapter 6 is where the conclusions are outlined.

Chapter 2: State of the Art

2.1 Introduction

Before presenting the results of our literature review, we summarize what an information risk assessment is. An information risk assessment methodology is an approach that structures the assessment of information risks. It consists of a precisely defined sequence of phases including their associated activities, inputs, outputs in the form of a framework for information risk assessment. The objective is to execute these phases during the information risk assessment process, including but not limited to identification of the information assets, the characterization of their associated threats and vulnerabilities, analysis of impacts and likelihood of the incidents, prioritization of risks. It also includes conducting a gap analysis and developing a plan to reduce the risks, followed by reporting the results.

Specifically, an information risk assessment can be defined as a structured undertaking that examines the information risks associated with the information assets of the organization; such as an application and its supporting infrastructure. Within the methodology, we identify threats and vulnerabilities that are applicable to an information asset. Based on the potential impact and likelihood of incidents, appropriate controls are

selected. The controls are used to prevent an incident occurring or to reduce the impact of the incident upon the organization.

In this chapter, we elaborate on structured information risk assessment methodologies for large organizations from a literature review. We also introduce the methodologies used for systems and small organizations, the guidelines, best practices, international standards, and tools in relation to information risk assessment. Herein, we detail the underlying phases of each structured information risk assessment methodology for large organizations. In addition, we provide an evaluation of the strengths and weaknesses of each. Before going into the details of each methodology, we first discuss the requirements of a typical information risk assessment. Some of these parameters apply to other aspects of security, in defining security processes, such as in cyber-forensic processes [15] :

- *Generality:* This requirement stipulates that the process needs to be general to be applicable to a large variety of organizations in different industries, within different information pre-requisites, according to their operating environments.
- *Specificity:* This requirement stipulates that the methodology needs to be specific in order to precisely guide the information risk analyst or the analysis team, in the steps, during the exercise of the risk assessment activities.
- *Documentation:* This requirement stipulates that the methodology has documented information, guiding the user step by step.
- *Iterativeness:* This requirement stipulates that the methodology has provisions to be repeated periodically, within a set period of time. This is necessary to monitor and control the recommended action items and the results of the information risk

assessment from the previous exercise and to understand the level of improvement attained, in information risk management.

- *Sequence:* This requirement stipulates that the methodology allows for a phase to yield its output as input to the previous phase or previous phases. The phases should be in an orderly sequence, to guide the analysts conducting the information risk assessment, as well as those participants involved in the exercise.
- *Tool Support:* This requirement stipulates that the assessment and reporting should be enforced at the tool level, electronically. The tool can be either a set of electronic worksheets to execute the risk assessment or a software tool developed, to aid in implementation and reporting.

In our approach to compiling the literature review, we first reviewed all the published references that we have been aware of. In their selection, we first referred to the working paper [27] published by the European Network and Information Security Agency which includes a consolidated list of the methodologies and standards in relation to information security and risk assessment. Then, we reviewed the sources of each methodology, standard or best practice to learn about each one specifically.

We tapped into the expertise of the professionals within source organizations, through interviews, meetings and enrolling in training programs of those institutions. Our contacts continued with the organizations who have implemented the methodologies and with consultants who conduct information risk assessments, on a regular basis. We reviewed applicable regulations that relate to information risk assessment and information security.

In our literature review, to the best of our knowledge, we did not exclude any published methodologies. The studied methodologies are:

- OCTAVE v2: Operationally Critical Threat, Asset and Vulnerability Evaluation, 2005 [9]

  Source: Carnegie Mellon University, Software Engineering Institute

- IRAM : Information Risk Analysis Methodologies, 2005 [34][35][37]

  Source: ISF: International Security Forum

- CRAMM :Comprehensive Risk Analysis Management Method, version 5, 2003 [39], [30]

  Source: Office of Government Commerce of British government (OGC)

- EBIOS: "Expression des Besoins et Identification des Objectifs de Securite", Release 2, 2004 [24][25][26]

  Source: DCSSI: "Direction Centrale de la Securite des Systemes d'Information, Premier Ministre", France

- IT-Grundschutz: IT Baseline Protection Manual, 2005[29]

  Source: Federal Office for Information Security, Germany

- NIST Standard : SP800-30, 2002 [50], SP800-53 [18]

  Source: National Institute for Standards and Technology

- CORAS Security Analysis Method [48][49]

  Source: EU funded CORAS project, with eleven European partners

- Microsoft Security Risk Management [42], [43], [44]

  Source: Microsoft

We also introduced other methodologies related to information risks. These are excluded from the scope of evaluation due to relevancy to the parameters presented earlier in this chapter in addition to language limitations, structure and scope relevance to our study:

- SARA: Simple to Apply Risk Analysis, 2005 [31]

  Source: ISF: International Security Forum

- MEHARI: (Méthode Harmonisée d'Analyse de Risques Informatique): Harmonized Method to Analyze Information Risks, 2004 [22]

  Source: CLUSIF

- SPRINT: Simplified Process for Risk Identification, 2005 [32]

  Source: ISF: International Security Forum

- FIRM stands for Fundamental Information Risk Management, 2005 [36]

  Source: ISF: International Security Forum

- Austrian IT Security Handbook, 2004 [12]

  Source: Austrian Federal Chancellery

- Dutch A&K Analysis, v1.01, 1996

  Source: Dutch Ministry of Internal Affairs

- MARION: Methodology of Information Risk Analysis and Optimization by Level, 1998

  Source: CLUSIF

- Swedish Information Processing Assessment

  Source: Swedish Information Processing Society

- OCTAVE –s v1: OCTAVE for small to medium sized organizations, 2005

  Source: Carnegie Mellon University, Software Engineering Institute

We also introduced software tools in risk assessment in addition to those electronic tools accompanied within the information risk assessment methodologies in scope of evaluation. The software tools reviewed in relation to information risk assessment are:

- Risk PAC

  Source: CSCI Inc.

- Countermeasures Risk Analysis Software

  Source: Alion Science and Technology

- Riskwatch

  Source: Riskwatch

- BIA (Business Impact Analysis) and LDRPS (Living Disaster Recovery Planning Software)

  Source: Strohl Inc.

The best practices and standards reviewed with respect to information security and information risk assessment are:

- ISO / IEC 13335-2, 2006 (ISO / IEC 27005)

  Source: International Standards Organization, ISO

- ISO / IEC IS 17799 :2005

  Source: International Standards Organization, ISO

- ISO / IEC IS 27001 (BS 77992-2:2002)

  Source: International Standards Organization, ISO

- AS / NZS 4360 : 2004 Australian / New Zealand Standard in Risk Management [11]

  Source: Standards Australia International, Standards New Zealand

- The Standard of Good Practice for Information Security, 2007 [31]

  Source: ISF: Information Security Forum

- COBIT: Control Objectives for Information and Related Technology [21]

  Source: IT Governance Institute

Based on our literature review from here on, we introduce all of the above listed methodologies, tools, and standards, with a description. Our evaluation reflects only those:

- Structured information risk assessment methodologies;
- For large scale organizations;
- With an accompanying electronic toolkit to provide aid in implementation; and
- Published in English language or translated to English language.

Exclusions to our evaluation are: guidelines, standards, best practices, methodologies not published nor translated into English language, not structured towards implementation in large organizations, not general but focused and highly technically oriented in one specific industry specifically, and those methodologies with no accompanying tools to guide a user during implementation.

2.2 Methodologies

2.2.1 OCTAVE

2.2.1.1 Description

OCTAVE stands for the Operationally Critical Threat, Asset and Vulnerability Evaluation. It is developed by Carnegie Mellon University, Software Engineering Institute. It is a qualitative risk assessment methodology. Its last version was published in 2005. OCTAVE is designed for organizations with more than 300 employees. The

OCTAVE methodology consists of three main phases. The first phase starts with building asset based profiles. In the second phase, infrastructure vulnerabilities are identified. In the third phase security strategy is developed.

Phase 1: The objective of the first phase is to understand the organization, its information assets and associated threats. During the first phase, assets that are critical to the organization are defined with their security requirements. The threats and vulnerabilities to these assets are identified. Three level workshops are conducted, first level with senior management, second level with operational management, and third level with staff. During these workshops, current practices in the organization are discussed, and the security awareness in the organization is assessed by the analysis team. A security survey questionnaire [9], referring to the different security practice areas is embodied within the methodology to measure the security awareness of participants.

Phase 2: The objective of the second phase is to assess threats and vulnerabilities of key components that support the critical assets of the organization defined in the first phase. The second phase is a technical assessment. First the key components of the information assets are identified. Then, technical vulnerabilities are examined by the analysis team, or a contractor service in vulnerability assessment. The results are discussed with the participants from IT and business.

Phase 3: The goal of the third phase is to define the impact of a threat occurrence and its likelihood. This is done to prioritize security risks of the organization, in order to develop a security strategy and mitigation plans.

Upon completion of the three phases in information risk assessment, OCTAVE methodology continues with "monitoring" and "control" phases as part of a risk

management process, producing aspects both in risk assessment and risk management. OCTAVE methodology is available with set of worksheets, showing the steps in conducting the information risk assessment.

2.2.1.2 Evaluation

As a reported advantage, OCTAVE has a systematic approach which enables the user to understand an organization's information security issues. Analysis team is formed by the experts both from the business and IT side who work together throughout the risk assessment process. It is the people from the organization who are the ones who direct the information security risk evaluation. They participate actively in the execution of the assessment and setting the security strategy for their organization. Another advantage is in its communication strategies where the participants' opinions are gathered through series of workshops and sessions. A security survey that is customizable for the organization accompanies the methodology.

The methodology scores high in generality as it can be implemented to large organizations with more than 300 people, serving in a wide variety of industries, although it originally started as a project for defense industry and its suppliers specifically. The inclusion of "control" and "monitoring" phases enhances its capability for iteration, but these two phases are not explained in detail like other phases, as they fall into risk management category.

The pitfalls of OCTAVE emerge in its repetitiveness, where some of the steps could be merged in order to make the process less time consuming for the analysis team as well as the participants in the organization. Another pitfall is that it does not have threat list which includes common threats, where users can refer as basis and select the required

inputs, thus more work is required to start from scratch to develop a list specifically for the organization. The methodology is accompanied with worksheets and templates, however, does not have an automatic tool which can provide findings from the worksheets in report format spontaneously. External companies developed their own tools to manage vast amount of information collected.

2.2.2 IRAM

2.2.2.1 Description

IRAM is an abbreviation for Information Risk Analysis Methodologies project. [37] It is developed by the ISF which stands for the International Security Forum. ISF methodologies are SARA, SPRINT and most recently IRAM, which is initiated as a project in order to examine the two methodologies SARA and SPRINT and to determine how they should be updated.

The methodology IRAM consists of three key phases. The first phase is "Business Impact Assessment". The second phase is "Threat and Vulnerability Assessment". The third phase is "Control Selection". Each phase represents a key part of the information risk analysis process, with the objective of identifying information risk and recommending appropriate controls to ensure the risks are adequately mitigated.

Phase 1: The objective of the first phase is to assess the negative impacts of security incidents to the organization. Impacts are defined as those that arise from the occurrence of the threats with the potential to harm the confidentiality, integrity or availability of the assets defined as critical by the organization. The adverse impacts of the incidents to the organization are graded in five different levels. An explanatory comment is provided for each type of impact. The impact assessment is continued with examining the non-

financial impacts, such as impacts to the reputation of the firm. Once the impact assessment is completed, the results are summarized for each critical asset, describing the system and rating the impacts to its security requirements.

Phase 2: The objective of the second phase is to determine threats and vulnerabilities that increase the likelihood of serious incidents occurring in a system. It helps to understand the detailed security requirements for a system and appropriate next steps that need to be taken to protect information. Threat assessment and vulnerability assessment reports are produced at the end of this phase, with detailed security requirements.

Phase 3: The objective of the third phase is to identify the key information risks of the organization. They are categorized as external or internal attacks. Controls that correspond to minimize the risks are identified. According to the risk level and the cost of the control, controls are selected, as countermeasures against risks.

There are electronic tools to support IRAM methodology in its various steps. The first tool is called "BIA Assistant". It enables the information risk analyst to assess the possible business impacts that could arise due to a security incident. The "Threat and Vulnerability Assessment Assistant" tool enables the information risk analyst to assess threats and vulnerabilities, and to determine the likelihood of information incidents and the key information risks in a system. The "Control Selection Assistant" tool allows the information risk analyst to identify, evaluate and select controls to mitigate information risk.

2.2.2.2 Evaluation

As a reported advantage, IRAM is a structured, yet flexible methodology, developed specifically to meet the needs of information risk analysts in its member organizations.

IRAM includes a high level of data collection capability in information security, asking for specific inputs. Its reported advantage is that it is documented and supported by electronic tools providing the practitioners with specificity on how to conduct the information risk assessment and to manage the information accumulated throughout the assessment.

A limitation is the expertise and know how required to provide the necessary inputs to the process, decreasing its generality, increasing its specificity. IRAM is more applicable and widely used in technology companies with a capability to be applied in other industries. The electronic tools of IRAM do not have automatic reporting capability, which may be a time consuming exercise. Another disadvantage is that a security survey is not embodied within the three phases of IRAM, to understand the level of security awareness within the organization. However, "The Standards of Good Practices for Information Security" is a survey tool developed by ISF which is updated periodically, can be used together with IRAM, to reflect updates in information security practice.

2.2.3 CRAMM

2.2.3.1 Description

CRAMM risk analysis methodology is developed by OGC which is the Office of Government Commerce of British Government and stands for Comprehensive Risk Analysis Management Method. Its last version is published in 2003, by Insight Consulting [30]. The CRAMM methodology includes three phases. The first phase is asset identification and evaluation. The second phase is threat and vulnerability assessment and the third phase is the selection of countermeasures and recommendation.

Phase 1: The objective of the first phase is to address asset dependency. It is designed to

address specific questions in relation to the security of the systems being analyzed. For example, it can be useful in identifying the security functionality required for a new application, physical and environmental security at a new site and developing security policies for a new system, determining if there is a requirement for specific controls.

Phase 2: The objective of the second phase is threat and vulnerability assessment. The asset data from the first phase is used to assess impacts of threats and vulnerabilities. Its toolkit consists of a database with 400 types of assets, 25 different types of impacts, 38 types of threats to guide the user. The results are demonstrated via graphs within the software tool. For example, bar charts are available to assess unavailability values.

Phase 3: The objective of the third phase is to determine the risks and their countermeasures. The evaluation for the risk assessment is guided by a series of tools, such as determining the relative priority of controls, recording the estimated costs of implementing the controls, modeling changes to the risk assessment, by "what if" calculations and back-tracking through the risk assessment for justification of specific controls. A "Countermeasure Tree" is used to select relevant controls, classified in different areas, like "Network Management", "Network Monitoring", "Information and Software Exchange Agreements". The status of the control is specified, whether it is to be implemented or if it is already implemented.

There are seven different measures of risk, as well as a countermeasure library that has 3,500 security controls in different aspects of information security. Information security policy templates, operational security procedures come along with the toolkit. Risk assessment data collection screen includes selecting threat type amongst the types of threats embodied within the application, choosing the level of impact, for the selected

asset groups. The level of threat and vulnerability is graded amongst qualitative criteria ranging up to "Very High". Specific comments of the participants can be added to the worksheet.

CRAMM has documented templates to help users to create a wide range of information security documentation. The templates include an information security policy, reported as compliant with ISO 17799, a description of the security management framework, risk analysis report, system security policy. It is reported to comply with the Data Protection Act.

2.2.3.2 Evaluation

A reported advantage of CRAMM is its capacity to audit the suitability and status of security controls on an existing system. Based on its audit capability, it is used by the British government and is preferred by government organizations in UK, as well as businesses within or outside of UK, mostly in Europe.

CRAMM scores high on tool support by providing the capability to conduct the steps of the risk assessment electronically. The application's functionality is helpful to produce comparisons between one assessment and a previous one, thereby allowing users to copy findings from an assessment to another. With a capability to produce results in a report format and visual presentations of data with graphical representation, the tool enables effective presentation to the management. This also provides the capability to quickly sum up interim results to keep management informed during the process, which improves the awareness and sustains commitment to the program. The database has strong attributes in identification of assets and threats, characterization of threats and assessment of exposures and risks. Another advantage together with its tool support is its

availability, in multiple languages in English, Dutch and Czech for a fee, from its vendor Insight Consulting. It is a flexible approach in risk assessment and can be used to look at organizations, processes, applications, systems and to investigate their infrastructures. A disadvantage is its use being limited to mostly in Europe.

A disadvantage of its tool support is its associated license cost and the time required for software training. While the automatic reporting capability diminishes the time consumption in collection and reporting of data, it also requires the time to learn and use the tool efficiently in implementation of risk assessment process.

2.2.4 EBIOS

2.2.4.1 Description

EBIOS stands for Expression of Needs and Identification of Security Objectives [24], [25], [26]. It is developed and used by the French government; General Secretary of National Defense, DCSSI which stands for "Direction Centrale de la Sécurité des Systèmes d'Information". Its use extends into private sector and outside of France. EBIOS guides are maintained by a team of experts from DCSSI, with respect to best practices. EBIOS is reported to provide a global vision to risks and to support the decision making process on strategic plans, as well as the tactical plans in protection of security. The roles and responsibilities in conducting the risk assessment and implementing the preventive actions are designated in between stakeholders. Its last version is published in 2004. The EBIOS method provides the following reported benefits:

- Alignment with the organization's strategic goals;
- Validation in step by step approach;
- Assessment of risks in the system development process;

- Optimized resourcing; and
- Commitment by the stakeholders.

There are five phases within the methodology. The first phase is dedicated to understanding the organization. In the second and third phase, the areas of concerns are discussed and security analysis conducted. Analysis and prioritization of risks are done in phases four and five. Residual risks are also determined in the last phase.

Phase 1: The objective of the first phase is to focus on processes, functions and their related information dependencies. As described in EBIOS, a context study is made to define process, functions and their information assets, in reference to the organization's baseline; related regulations, existing systems and in particular on the overall IS security policy.

Phase 2: The objective of the second phase is to identify needs of the organization which primarily involves the project leader and the authority responsible for information risk assessment in the organization. The concerns of these parties are discussed. The selected security criteria are based on the three usual security criteria: availability, integrity and confidentiality.

Phase 3: The objective of the third phase is to study the threats and detail the areas of concerns. A threat study is conducted to define the specifications for the organization as well as for the specific systems. Threat identification is made based on the attack methods and threat agents. The attack potential of each threat agent is explained. A specific vulnerability per threat is determined and the existing protection profiles are analyzed to understand their conformity to the identified threats and vulnerabilities. In

light of another objective, to measure the effectiveness of the existing countermeasures, they are assumed to be not in place.

Phase 4: The objective of the fourth phase, as reported in EBIOS is to identify security objectives. In this phase, the specifications of the organization and systems are refined and approved with respect to the significance of their objectives. The risks are identified, in the light of the threats formulated. Security objectives are determined and documented.

Phase 5: The objective of the fifth phase is to determine the security requirements which are developed in accordance to the security assurance requirements of the organization.

The inputs to EBIOS are the information systems security policy and the general specifications of the system. An in depth analysis of system specifications is made during the information risk assessment process, as only those systems whose objectives are known are the objects of the security study. The outputs of the study are a master plan for information systems security, a security policy, an action plan for information systems security, the security objectives and the protection profile.

2.2.4.2 Evaluation

A reported advantage of EBIOS is its use in systems which are in their development stage, as well as existing systems. Another advantage is its specificity. Specific studies are made on how to use EBIOS through its five steps, in order to guide a user effectively. A number of documented studies are available to use EBIOS for developing a security strategy and related best practices in information risk assessment and risk management. Another advantage is its capability of tool support, as it allows the system study results to be recorded and the required summary documents to be produced. Its operation allows easy customization of knowledge bases.

Other reported advantages include its capability of involving the audience, as it is also publicized as an awareness tool, for everyone involved in the project of information risk assessment. It has strong attributes in asset and threat identification, characterization of threats, assessment of exposures and risks. A reported advantage of EBIOS is that it provides a flexible and consistent process, which makes it also a negotiating and decision-making tool in information security system process. Another advantage is the consistency it provides by a unifying vocabulary. It is reported to be compatible with information security best practices, such as ISO 17799.

Its use is mostly in public sector and ministries of French government, and in mainly French speaking regions and countries. It is also used in information risk assessment of specific systems, including developing systems.

2.2.5 IT Grundschutz

2.2.5.1 Description

IT Baseline Protection Manual is known as IT – Grundschutz in German. [29] It is developed by Federal Office of Information Security. Its last version is published in 2005. IT-Grundschutz certification (or now: ISO 27001 certification on the basis of IT-Grundschutz) includes inspection of IT security management and IT security safeguards.

IT Grundschutz provides a framework for establishing information security management and presents a method in information risk management. The goals of the organization in IT security are set, with respect to the needs of the business. The threats are listed and appropriate technical recommendations are provided with respect to the security objectives and implementation targets. This is followed with maintenance and improvement process in information security.

IT Grundschutz handbook [29] displays five threat categories. The first category of threats is "force majeure" consisting of sixteen different threat types. Examples are loss of personnel, fire, lightning, burning cables. The second category of threats is organizational shortcomings, which consists of 107 threat types. Examples include insufficient procedures, unauthorized use of rights and uncontrolled use of resources. The third category of threats is human failure threats, consisting of 78 threat types, such as non-compliance with the IT Security guidelines, improper use of IT system, illegal connection of cables. The fourth category is technical failure consisting of 52 threat types, such as disruption of power supply, defective data media, disclosure of software vulnerabilities. The fifth category includes deliberate acts of 127 threat types, such as vandalism, manipulation of data, attacks, theft.

Safeguards are countermeasures against the listed threats. IT Grundschutz [29] provides a list of safeguards. These are categorized into areas of:

- 162 infrastructure safeguards, including physical and electronic safeguards;
- 340 organizational safeguards, such as audit of the hardware and software inventory;
- 51 personnel safeguards such as ergonomic workplace and training on IT security safeguards;
- 255 hardware & software safeguards such as screen lock and password protection;
- 124 network and communications safeguards, such as selection of appropriate network topography and selection of cable types; and
- 96 contingency planning safeguards such as development of a survey for availability requirements and responsibilities in an emergency.

When modeling a set of IT assets, IT Grundschutz recommends that the modules are assigned in accordance with the layer model. This is then followed by validation to ensure completeness. The first layer is the generic IT security aspects from which the primary elements. These aspects are recommended to be controlled uniformly for all IT assets. IT security management, organization of IT operations, training and promotion of staff awareness are noted as particularly important in this case.

The second layer is security of the infrastructure that includes building security, cabling, server room, work place at home, mobile work place, and meeting rooms. The third layer is the security of IT systems. This layer covers security aspects which refer to IT systems and is divided into servers, clients, network components. The fourth layer is the security of the network. This layer is concerned with security aspects in the network which do not only exclusively apply to specific IT systems. The focus is on security aspects which relate to the network connections and communication between the IT systems. The fifth layer is the security of applications, which is the lowest layer of the model, including mapping of the applications, generally implemented as client/server applications.

2.2.5.2 Evaluation

The advantage of IT Grundschutz is in its strong attributes for threat identification and characterization, offering a wide selection of safeguards to choose from the appropriate ones for the organization. The layer approach of the methodology provides an important differentiator which enables completeness check and validation to ensure that the entire system has been completely modeled within a layer approach, systematically following the layers.

It has bilingual capability as it is published in English and German. It extends in scope

into risk management, beyond the scope of information risk assessment, providing recommendations on the implementation of safeguards. Through its documentation, it is specific to guide a user with its structured approach. It is a detailed and technically oriented assignment, requiring expertise to implement, but also providing set of guidelines in security management and information risk.

A disadvantage is that it does not have automatic tools to use during risk assessment which makes it hard to manage the data collection as well as having challenges in the reporting of findings, given the vast number of selection possibilities in its threat and safeguard catalogue. Another partial disadvantage is the knowledge and expertise required to take full advantage of its in depth technical know-how.

2.2.6 NIST Standard: SP800-30 and SP800-53

2.2.6.1 Description

SP 800-30 stands for special publication of 800-30 in risk management, which is a guide in information technology systems, developed by the National Institute for Standards and Technology (NIST) in 2002. In December 2007, NIST published SP 800-53; "Recommended Security Controls for Federal Information Systems", where information risk management and the criticality of a risk assessment in system development cycle are discussed in Section 10. SP 800-53 reduces the nine step process of SP 800-30 into six steps, in information risk assessment. SP800-30 provides guidelines for risk assessment and risk management in computer security. It is based on US regulations. It includes both qualitative and quantitative elements, with graphs and mathematical formulas with references. NIST SP 800-30 [50] and NIST SP 800-53 [18] provide guidance in information risk assessment in a step by step structure as follows:

Step 1: The risk assessment methodology starts with system characterization in its first step where the scope of the effort is defined. In this step, the boundaries of the IT system with its associated resources are defined. When an IT system is characterized, the scope of the risk assessment is established, the operational boundaries are defined, and the information on hardware, software, system connectivity are provided and responsible division or support personnel essential to defining the risk is identified.

Step 2: In the second and the third steps, the threats and vulnerabilities are identified. The threat-sources are defined as any event with the potential to cause harm to an IT system, which can be natural, human, or environmental. Some of the human sources of threats are hackers with motivation to challenge self ego taking actions such as system intrusions, unauthorized system access and social engineering. Another threat source is a person with a revenge motive, involved in a system attack or an industrial espionage by unauthorized access to intellectual property of the organization.

Step 3: The analysis of the threat to an IT system also includes an analysis of the vulnerabilities associated with the system environment. The goal of vulnerability analysis is to develop a list of system vulnerabilities that could be exploited by the potential threat-sources [50]. An example of vulnerability could be terminated employees' system identifiers not being removed from the system.

Step 4: The goal of step four is to analyze the controls that have been implemented or those that are planned to minimize or eliminate the likelihood and probability of a threat's exercising a system's vulnerability. In the updated version of SP 800-53, this step also includes determination of the likelihood, to derive an overall likelihood rating that indicates the probability of a potential vulnerability. The likelihood that a potential

vulnerability could be exercised by a given threat-source is described as high, medium, or low. As per NIST SP 800-30, high likelihood is "the threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective". Medium likelihood is "the threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability". Low likelihood is "the threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised".

With the updated version of SP 800-53, Step 4 also includes measuring the level of risk to determine the adverse impacts of a threat exercising a system's vulnerability. The adverse impact of a security event can be described as "a loss or a degradation of any, or a combination of the three security goals: integrity, availability, and confidentiality". Loss of public confidence, loss of credibility, damage to an organization's reputation are qualified or described in terms of high, medium, or low impacts. The magnitude of an impact is defined in terms of its cost, a serious injury leading to loss of life, impact to organization's reputation or to the organization's mission.

Step 5: Step five is where controls and alternative solutions are recommended to minimize identified risks. Reported factors critical to be considered in identification of controls are effectiveness of recommended options, according to the system capability, legislation and regulation, organizational policy, operational impact, safety and reliability.

Step 6: In step six, the results are documented in a report format.

2.2.6.2 Evaluation

The advantage of NIST SP 800-30 and SP 800-53 are providing specific guidelines, in conducting information risk assessments, yet they are generic and can be applied to

various industries and organizations. The scope includes activities beyond risk assessment, such as mitigation options, strategy and an approach for implementing the controls. Control activities are divided as operational and strategic control activities, which help to determine the duration for action plans through categorization. Cost and benefit analyses and concept of residual risk are included in the guide.

The methodology is accompanied with templates, sample interview questions and a risk assessment report outline, which helps it to make easier to follow. It is accompanied with figures and tables that guide a user throughout the risk assessment process. [50] A risk assessment report template is provided which is helpful in describing the threats and vulnerabilities, measuring the risks, and providing recommendations for control implementation, as a summary of the work.

The disadvantage is that it is not available with computer support, where the templates could be used electronically and reports could be created automatically for the vast number of data collected during the information risk assessment. It is used more as a guideline instead of a methodology.

2.2.7 CORAS

2.2.7.1 Description

The security analysis method, CORAS is developed with the participation of eleven experts from UK, Greece, Germany, and Norway, in a 4-year project between 1999 and 2003. The project is funded by European Union. CORAS includes Australian and New Zealand Standard for Risk Management, in its foundation. It constitutes of the following seven steps:

Step 1: The first step starts with establishing the context. This step involves an

introductory meeting with the participants. Overall goals of the analysis are defined, based on the discussion with the client organization. The security analysis method CORAS is introduced. The scope of the analysis is determined. The meetings and work-shops are planned where information will be gathered. The analysis leader, secretary, representatives of the client, key decision makers are reported as required in CORAS, leaving users and technical staff optional for this step.

Step 2: The second phase is a high level analysis, where separate meetings with client representatives are held. The results of the first meeting are presented and threats, vulnerabilities and threat scenarios are discussed. Standardized notations; UML is used, with explanations on the notations, to ensure understanding by all participants. [49] Activity diagrams, flow-charts are used. Modeling guidelines are available within the CORAS methodology. A region is drawn which logically and physically represents the target of analysis. [49]

Step 3: The third step involves approval on assets and a more precise description of the target to be analyzed. The client approves the target assets and ranks them according to their importance. The "consequence scales" and "likelihood scale" are set for each asset, within the scope of the analysis.

Step 4: Step four includes a risk identification workshop, gathering people with expertise in the evaluation of the target assets. Incidents that may potentially be harmful to the organization are identified, with threats and vulnerabilities. Human threats are divided between deliberate and accidental actions, while non-human threats are analyzed separately. Assets that are not harmed by any of the incidents are taken out of scope, in this step.

Step 5: Step five is risk estimation where each risk is assessed with respect to its likelihood of occurrence. Help of visual diagrams is used.

Step 6: Step six provides a risk portfolio, which is a first estimate of the complete risk diagram provided to the organization. Risk diagrams are modeled, into overall risk matrix, by an explanation on each risk.

Step 7: The last step is devoted to the treatment of the risks, where treatment options are identified addressing the cost and benefits. The step is organized as a workshop. Treatment options are also added to the risk diagram that is developed on the basis of the threat diagram.

2.2.7.2 Evaluation

The strength of CORAS is in its tool support and its illustration that stimulates the process and improves the communication. Drawings, pictures and sketches are used in order to better communicate with the audience during information collection. Each phase has a distinct purpose where different outputs are produced, using graphical security risk modeling language based on UML, as reported in CORAS methodology. It includes a computerized integration tool, and XML mark-up for exchange of risk assessment data and a vulnerability assessment report format, to conduct the information risk assessment review. Another advantage is that a facilitated brainstorming session is conducted within the methodology, as one of the techniques employed in collecting information for risk identification that integrates the audience in the process. Another advantage is its structure in a way that responsibilities and roles of the participants in each one of the seven steps are specified, which helps in resource planning and outlining the initial project plan.

In terms of generality, its use is mostly in Northern Europe and is not an internationally recognized on a wider scale, eg. North America. It requires specific know-how to be implemented with consultancy from its producer. It includes a number of charts and graphics which makes it easy for the user to understand, but also requires time invested in preparation and learning of the method by the analysis team in order to accurately conduct the assessment.

2.2.8 Microsoft's Security Risk Management

2.2.8.1 Description

The Microsoft security risk management process includes a structured four step methodology and is accompanied by electronic worksheets. Microsoft methodology comprises of four phases, where risk assessment is discussed in its first two phases.

Phase 1: In the first phase, risks are identified and prioritized according to the business. The risks are assessed in facilitated discussions by gathering information about assets, threats, vulnerabilities, controls and suggested risk treatment options. Gathering risk data involves two stages: collection of risk data and its prioritization. In gathering risk data, the data collection process and analysis take place. In prioritizing risks, it is important to outline the prescriptive steps to qualify and quantify risks. The data gathering template to identify assets includes threat definition, vulnerability, level of exposure and current controls on the physical, application, host, network and data layers. [42]

Phase 2: The second phase involves identification and evaluation of controls, based on a cost benefit analysis process to select possible control solutions. Solutions are reviewed and evaluated against the functional requirements of systems. Risk reduction amount and costs are estimated, considering "the direct and indirect costs associated with mitigation

solutions". The outcome of this phase is risk treatment options. Summary risk templates and an example are provided within the Microsoft methodology with data. [42].

Phase 3: The third phase includes implementing the controls, by considering people, processes, technology. Mitigation solutions across the business are determined.

Phase 4: The fourth phase is focused in measuring the effectiveness of the information risk management program by monitoring the treatments. Risk scorecard is developed to understand the risk posture and progress. This phase also covers the ongoing process of identifying new, potential risks, to provide the expected degree of protection.

Microsoft's methodology provides guidelines on the importance of risk communication with the reason that various people involved in the risk assessment process define risk differently. It advises to ensure consistency in definition of terms across all stages of an information risk management cycle, to agree upon single definition of risk at the beginning. It guides the user to determine the organization's risk management maturity level, how to define roles and responsibilities and to build the risk management team.

2.2.8.2 Evaluation

The advantage of the methodology is that it includes not only risk assessment but also risk management by conducting decision support, implementing controls, and measuring program effectiveness, however the pitfall of this approach is that it introduces much larger scope than the boundaries of an information risk assessment, decreasing the specifity characteristic. The methodology is strong in itirativeness, as the cycle of risk management is defined as an ongoing program, allowing the information risk assessment to be re-started at regular intervals to refresh the data in each stage. This period is

reported in Microsoft to be usually aligned periodically with an organization's fiscal accounting cycle to align budget requests for controls with normal business processes.

The methodology, having a wide-scope has the disadvantage of loosing its depth, as there are only a few worksheets that accompany the methodology. There is no automatic capability for collection of data or the reporting of data by graphical representations. The documentation provides a direction and a perspective to its user, in information risk management. While it is generic, it is more effective to implement in technology organizations like Microsoft itself as it embodies the expertise in IT companies like Microsoft.

As in all of the above methodologies discussed, there is no quantification on risk.

2.2.9 SARA

SARA [31] which stands for Simple to Apply Risk Analysis is reported as a detailed methodology for analyzing information risk in critical information systems, developed by ISF which stands for International Security Forum. It is examined and combined with another methodology; SPRINT [32] and updated into a new methodology; IRAM which we discussed earlier.

Sections of SARA include "IT Risk Management Process", "IT Risk Management Model", and "Risk Analysis in the Systems Development Life Cycle". Its application for different systems and it displays the dependencies between these systems. First, baseline controls and system specific controls are established. The control requirements and techniques are then selected. The main steps in the method are described as meeting with the system owner, meeting with the systems development manager, a workshop to assess business impact; and another workshop to assess vulnerability and control requirements.

SARA is focused on conducting risk analysis, specifically on application and system basis. In addition to an application, a system is specified to include a database and IT infrastructure to support the application. It is applied in the life cycle of the development of an application, as the risk analysis method prior to system implementation; recommended for planning and feasibility assessment, definition of system requirements, design and build. It is applied during live operation and prior to a major change as well.

SARA is designed to support the risk analysis for applications of all sizes from small PC based systems to large mainframe based applications in development. Its application varies according to the scale and complexity of the application. For large mainframe based applications, many workshops may be required to analyze the risks while separate workshops may be appropriate for confidentiality, integrity and availability.

2.2.10 MEHARI

MEHARI [22] is a product of CLUSIF which is a French organization oriented to information security. It replaces the MARION methodology and stands for "Harmonized Method to Analyze Information Risks". It is updated in 2004. When MARION methodology was no longer sponsored by CLUSIF it was replaced by MEHARI.

MEHARI provides a risk assessment model, as well as an approach to define countermeasures for risk reduction with respect to the objectives of the organization. It has quantitative elements in it and has an audit flavor, like MARION. The documentation and its accompanying tools being in French, its use is restricted to French speaking regions, including government organizations in Quebec, as well as the private sector.

The risk assessment model used by MEHARI is based on an evaluation of the potential impact of a risk scenario based on its potentiality and the strength of the measures in place

to mitigate the risk. Risk assessment is performed directly by scoring the impact for each scenario, within measures specified as "dissuasive", "preventive", "protective", "palliative", based on the evaluation of the vulnerability in different category of events.

MEHARI is reported to provide a risk assessment model in modular components and processes, while enhancing the ability to find out vulnerabilities through assessment, analyzing the risk situations out of the 171 risk scenarios situated in its knowledgebase. It includes formulas for threat identification and threat characterization, with optimal selection of corrective actions. It has strong quantitative attributes. While it is accompanied with Risi-Base software to facilitate the data collection and information risk assessment process, being available in French and not translated to English restricts its use beyond French speaking regions.

2.2.11 SPRINT

SPRINT [32] stands for Simplified Process for Risk Identification is used in assessing business impact and analyzing information risk in important information systems that are not critical. It is a complementary methodology that is designed to be used with SARA discussed earlier and is again developed by ISF which stands for International Security Forum.

SPRINT is reported as a method for analyzing the business risks associated with an information system and for the safeguards or controls. [32] The levels of risk associated with a system are determined to guide the user in selection of action items for keeping risks within acceptable predetermined limits. The vulnerabilities of existing systems and the safeguards are determined. The security requirements for systems under development and the controls needed to satisfy them can also be identified, by using SPRINT.

It has three main phases. In the first phase, the level of business risk associated with an information system is assessed, where the consequences and impact of a loss are determined with respect to the confidentiality, integrity or availability of information processed by the system. The second phase identifies the controls needed to keep risks within acceptable limits, by considering the threats and vulnerabilities which could lead to a loss of confidentiality, integrity or availability. The third phase produces an agreed plan of action for implementing required controls, by considering the priority of controls identified.

2.2.12 FIRM and the Survey

FIRM [36] stands for Fundamental Information Risk Management and is published by ISF; Information Security Forum. It provides an approach to control and monitor an organization's information risks. FIRM includes a guideline for communication, gaining support of stakeholders and implementation. An "Information Risk Scorecard" is a part of FIRM, used to collect information on a particular asset. The information collected on an asset includes its owner, its degree of criticality, the threats and level of threats to its security. Therefore, it can be used as an accompanying tool in information risk assessment.

2.2.13 Austrian IT Security Handbook

Austrian IT Security Handbook is originally developed by Austrian Federal Chancellery, for government organizations.[12] It includes a generic description of how risk assessment should be conducted.

The hand book has two parts where the first part provides a detailed description of the IT security management process, including development of security policies, risk analysis.

The second part concentrates on security measures, providing two hundred thirty baseline security measures with an implementation tool. The methodology is now used by businesses, while it has been developed originally for the government. The methodology is reported to be compliant with ISO / IEC IS 13335 and ISO / IEC IS 17799. Its last version is published in 2004.

2.2.14 MARION

MARION is a product of CLUSIF which is a French organization oriented to information security. MARION translates into "Methodology of Information Risk Analysis and Optimization by Level".

It is structured as an information security audit, including a security questionnaire. The method has quantitative elements in it, where the security level is estimated in six subject areas, with levels assigned a grade between zero and four based on their maturity. The risks are identified in light of the responses from the questionnaire while the process is followed by a detailed threat and vulnerability analysis.

MARION methodology is no longer sponsored by CLUSIF and is replaced by MEHARI which stands for "Harmonized Method to Analyze Information Risks".

2.2.15 SBA

SBA which stands for Swedish Information Processing Assessment is developed by Swedish Information Processing Society. SBA is reported as a flexible and simple to use qualitative method for classifying assets, identifying security weaknesses and recommending countermeasures. The SBA methodology consists of three phases. The first phase is the "analysis phase". The second phase is "executive phase" and the last phase is "wind-up phase".

2.2.16 OCTAVE-s

OCTAVE – s is developed by Carnegie Mellon University, Software Engineering Institute which stands for the Operationally Critical Threat, Asset and Vulnerability Evaluation. Like OCTAVE, it is a qualitative risk assessment methodology. Its last version is published in 2005. While OCTAVE is designed for organizations with more than 300 employees, OCTAVE-s is its modified version for smaller size organizations with less than 300 employees. OCTAVE-s is left out of our scope of evaluation, as it is not applicable for large scale organizations.

2.3 Electronic Tools

The following tools discussed are software packages in security, available at a license fee, from their vendors. They can be used for large scale organizations' information risk assessments. We have provided a brief description on them; however, left them out of scope of our assessment.

2.3.1 Risk PAC

Risk PAC is a software tool. It is developed with respect to a risk assessment methodology, integrated within the tool. The owner of the software tool is CSCI Inc. which is based in USA. Risk PAC is a software-based tool that is reported to be used to identify threats, to conduct analysis of the risks and to determine cost-effective counter-measures in order to mitigate risks. The Risk PAC methodology includes four phases. The first phase is composed of questions in security subject areas, including but not limited to information security. The second phase displays the risk profiles assessed in response to the questions. The third phase presents recommendations that propose solutions. The fourth phase maps tables that relate the results of questionnaire in the

second phase, based on the scoring of the recommendations in the third phase.

2.3.2 Countermeasures Risk Analysis Software

Countermeasures Risk Analysis Software is reported to provide reporting of both information and physical security, including critical infrastructure, port and school security, anti-terrorism force protection by Alion Science and Technology. As reported by the vendor, the phases are developed based on:

- data collection;
- analysis of threats;
- prioritizing risks iteratively;
- generating management level reports with graphs in threat vulnerability assessment;
- justification of funding by showing return on investment;
- managing the security data in a central database; and
- responses to issues and inquiries.

2.3.3 Riskwatch

Riskwatch software is focused towards physical and homeland security, identifying assets, determining values for assets, identifying infrastructure vulnerabilities, safeguards and determining a plan to implement the safeguards. It includes, but is not limited to the assessment of information risks. Its steps include "preparation phase" where scope of the risk assessment is set and parameters are selected, assets and their values are defined, threat data is evaluated to identify vulnerabilities, degree of loss and safeguard identification is done through a cost and benefit analysis.

2.3.4 BIA / LDRPS

BIA standing for Business Impact Analysis and LDRPS standing for Living Disaster Recovery Planning Software are both software products from Strohl Inc. that support information security. As they are flexible tools, they can be customized according to the specific needs of the organization, though neither can be classified as information risk assessment tool specifically.

The first tool BIA [51] is used to conduct business impact analysis, based on a similar approach like in the other methodologies in information risk assessment is the first phase of the IRAM methodology. LDRPS [52] is another software product used for business continuity planning and IT disaster recovery planning that form protection strategies that may be required as a countermeasure with respect to the findings from an information risk assessment. LDRPS is a flexible database tool and can be customized to be used for risk assessment.

2.4 Standards and Best Practices

2.4.1 ISO / IEC IS 13335 -2

ISO / IEC IS 13335 – 2 is an international standard, developed by ISO; International Standards Organization. Its last version is published in 2006. It includes guidelines to information risk analysis and describes the process of information security management. List of common threats and security controls are available within the standard documentation, for user selection.

2.4.2 ISO / IEC IS 17799

ISO / IEC IS 17799 [40] is an international standard, originally developed as a British standard and adapted to ISO. It is updated version is published in 2005. It includes

information security best practices that support information risk assessment, but does not provide a method on how to conduct a risk assessment.

2.4.3 ISO / IEC IS 27001

Reference ISO / IEC IS 27001 is used for certification and includes a set of information security controls that can be to be implemented upon conducting a formal risk assessment. Its last version is in 2005, as it is discussed in methodologies section, under "IT Grundschutz" [29].

2.4.4 AS / NZS 4360

Reference AS / NZS 4360: 2004 is Australian / New Zealand Standard in risk management. It is latest version is published in 2004. AS / NZS 4360 [11] is different from the international standards listed above, in the aspect that it is not specific to information security risks, but is a generic approach to risk assessment and risk management. It does not provide a framework on how to conduct information security risk analysis specifically. It provides guidelines for establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risk. The concepts in this standard are applicable and furthermore essential for any type of risk assessment, including information security risks. It refers to a risk management process that can be applied in a variety of sectors and a range of different subject areas.

2.4.5 The Standard of Good Practices for Information Security

The Standard of Good Practices for Information Security is first released in 1996, by ISF and is updated every two years. Its latest version is published in 2007 [31]. It sets the foundation to develop the information security survey questions that can be used as part of the information risk assessment, to measure the level of awareness of participants in

information security.

2.4.6 COBIT

COBIT stands for "Control Objectives for Information and Related Technology", published by IT Governance Institute, provides a set of guidance materials for IT governance, which are recognized internationally. The risk management ingredient in COBIT is embodied through the guidance it provides to management and information security professionals, in setting up the control framework that aligns IT with the mission and objectives of the business, to bring value to the business and manage IT risks appropriately, through best practices. COBIT control practices are available from the internet site of ISACA, free of charge to its members.

Chapter 3: Comparative Study

3.1 Introduction

This chapter is dedicated to compare the previously evaluated information risk assessment methodologies, with respect to the metrics identified. The objective is to identify the common points of the methodologies, the points essential in an information risk assessment, strengths of these methodologies, as well as their limitations. Our intent in the next chapter is to design a new information risk assessment process by leveraging the positive features while improving the weaknesses to manage the quality of the risk assessment process. The approach provides guidelines for both researchers and practitioners in information risk assessment to adopt the methodology in different conditions and organizations.

The framework for comparison focuses only on the selected methodologies in information risk assessment. The basis of our selection is more prominent methodologies in information risk assessment that are explained in a phase by phase structure, but are also accompanied with tools to guide the user step by step on how to conduct an information risk assessment for a large organization, where their documentation and tools are available in English language.

This section introduces a methodological approach designed to provide the ability to conduct a comprehensive comparative evaluation of different methodologies which drive the information risk assessment process. The proposed comparative approach stems primarily from conducting information risk analysis in various organizations. Such evaluation framework refers to a selected set of critical attributes that represent the requirements of the present information risk assessment methodologies. This framework also helps defining an integrated methodology, based on an analysis where the commonalities and differences of the existing methodologies are emphasized with their strengths and weaknesses.

3.2 Criteria

The resulting requirements and features are broadly classified into structural, identification, techniques, training, functionality, usability, consistency, tool support and organizational criteria. Some of the criteria listed apply to enterprise risk assessment process and security processes, besides information security, such as in cyber-forensic processes [15]:

- *Structure*: This criterion reveals the process actions on conducting a full information risk assessment in a given environment and organization. Structure provides a step by step approach and directs a user in a more structured way than guidelines, best practices and standards in security and risk. The structure, however, needs to be easily customized into the needs of the organization being assessed, for the security risk analyst or the analysis team to act correctly, according to organization's needs and requirements.
- *Identification*: This feature represents all specific procedures that an analysis team needs to follow to scope the assessment. Indeed, an organized and controlled method of

identification is required. Processes, information assets, threats, vulnerabilities, impacts, risks are the elements that need to be identified, throughout an information risk assessment, in order to select the critical ones. A catalogue of threats and a list of security practice areas are available within the methodology, for reference purposes.

- *Techniques*: An important feature regarding the information risk assessment methodology lies in the need to provide practitioners with appropriate, updated, and improved techniques to properly gather, analyze, and report the findings of an information risk assessment.

- *Training:* This is a vital requirement for information risk analysts and the participants of the information risk assessment process to focus on acquiring sufficient knowledge and basic skills to enable them to adequately perform the tasks regarding information risk assessment. One of the results achieved in conducting an information risk assessment in an organization is increased awareness of organization's members in their level of security understanding.

- *Functionality*: Information risk assessment processes and tasks are required to provide effective functionalities in the course of challenging activities performed in identification, information collection, analysis, validation, reporting and presentation of the results. The purpose of an information risk assessment methodology is to allow the analysis team to perform a variety of functions, in accordance with established requirements. In this respect, the core functions of an information risk assessment methodology can be clearly identified as:

  - *Data Collection*: Data collection or acquisition from a source is the most significant function of an information risk assessment process. While most of the

data is collected via interviews or work-sessions, historical organizational data is also valuable to the process.

– *Analysis*: Once the necessary data has been collected, the next step is examination and analysis. Analysis is an essential function through which the information risk specialist or the analysis team derives useful information. It refers to the process of interpreting the extracted data, through a set of activities.

– *Validation*: It refers to validation of the information gathered and results with the participants, to ensure accuracy of the information and results compiled.

– *Reporting*: It refers to the important phase where the tasks are completed and accurate reporting of the findings is required. In this respect, comprehensive documentation including findings in each phase and the final result on the overall risk profile of the organization, with suggested security protection strategy and mitigation actions.

– *Presentation*: Presentation of the results is an important factor in communication. While establishing an ongoing communication throughout the risk assessment project, the final results are presented to the executive sponsorship, participants, and the stakeholders of the information risk assessment.

- *Guidance - Organizational Factors:* This criterion reveals the guidance that the methodology provides to attain organizational support which is a crucial success factor, in conducting a full information risk analysis, in a given environment and organization. The information risk assessment methodology should provide guidance on the following organizational factors in order to attain a successful result:

– *Sponsorship*: This feature represents necessity of senior management to support the information risk assessment process. Absence of this support will most likely lead to stakeholders resisting to participate or to underestimate the efforts of the process. There are many reasons why required participants, including employees and upper management may fail to cooperate, of which two can be summarized as resistance to change and insufficient knowledge in information security. They may also not be aware of the benefits.

– *Stakeholders*: These are the members of an organization with a vested interest in the results of the security risk assessment. Stakeholder engagement to the process is critical in its success, and an engagement process must be included in the guidelines. Prior to start of the process in information risk assessment, stakeholders, including the analysis team and the sponsors need to be identified.

– *Maturity Level*: The organization's maturity in risk management culture makes it easier to implement the information risk assessment. If the organization does not have security risk management process in place, it involves significantly higher effort to conduct an information risk assessment and it involves too much change to implement an information security program.

– *Open Communication*: Projects usually operate on a need-to-know basis. This may lead to misunderstandings or gaps in communication. Open communication refers to sharing of the findings and information collected throughout the risk assessment process with the team and the stakeholders in a continuous and a planned manner.

- *Analysis Team*: The analysis team refers to the team who conducts the information risk assessment, analyzes the results from the information risk assessment process and prepares the results in a report format to be presented to appropriate management team. It is extremely important for the analysis team to foster a spirit of teamwork and be representative of the overall organization with members in different areas of expertise.

- *Authority*: Participants in the risk assessment process accept responsibility for identifying and taking actions to control the most critical security risks to the organization for which they require sufficient level of authority, from management.

- *Usability:* This criterion is the degree in ease of use of the methodology and how well the analysis team can use the methodology to perform information risk assessment tasks with effectiveness, efficiency and to required satisfaction levels.

  - *General:* This requirement stipulates the solutions accommodated in the methodology must support different organizations, operating in a variety of environments, in different industries, with the necessity of organizations to comply with different set of regulations.

  - *Descriptive:* The requirement stipulates that the methodology is to incorporate relevant and detailed guidelines, procedures which lead to the successful completion of each phase and overall information risk assessment process. These procedures should be documented.

- *Consistency:* This criterion refers to the consistency in application of the methodology by different team members. One factor effective in helping to attain consistency is setting the definition of the terms in information risk assessment.
- *Tool Support:* The methodology is much easier to use if supported by tools that implement the tasks to be performed and provide ease of customization according to the organization's needs.

3.3 Comparison

A common definition of the terms referred in the information risk assessment process is established to promote a common understanding. After the stand-alone analysis of the methodologies presented in Chapter 2, we compare the methodologies in information risk assessment for large organizations. These models have distinct characteristics and specific advantages and disadvantages, despite their similarities.

Comparing existing methodologies of information risk assessment is helpful in drafting an initial list of requirements for the new methodology, based on the criteria developed in Section 3.2, in addition to the initial criteria defined in the stand alone analysis of methodologies, in Chapter 2. Based on these requirements and characteristics, the table below provides a comparison of the activities, tasks, and processes corresponding to each methodology in information risk assessment.

Qualitative Measure of Criteria - Structure	
Level	*Units of measure: Methodology is structured*
High	*Methodology is divided in phases where each phase outputs are clearly defined to guide the user step by step.*
Medium	*Methodology is divided in phases where major activities in each phase are explained, however inputs and outputs of each phase is not clearly structured.*
Low	*Methodology is a series of guidelines.*

Table 3-1: Grading for Structure

Qualitative Measure of Criteria - Identification	
Level	*Units of measure: Identification.*
High	*Identification of essential parameters is executed throughout the process, as well as for scoping in the early stages of the assignment. A catalogue is used to choose the relevant ones (assets/ threats / vulnerabilities) for the organization.*
Medium	*Identification is done throughout the risk assessment in an iterative manner.*
Low	*Identification is a limited characteristic of the methodology.*

Table 3-2: Grading for Identification

Qualitative Measure of Criteria - Techniques	
Level	*Units of measure: Techniques used*
High	*Methodology is very rich in using specific techniques, to better gather, analyze, evaluate, report results. (eg. quantitative models to evaluate risks, graphical models to represent data)*
Medium	*Methodology makes use an adequate amount of techniques to gather, analyze, evaluate, report results.*
Low	*Methodology is limited in techniques to gather, analyze, evaluate, report results.*

Table 3-3: Grading for Techniques

Qualitative Measure of Criteria - Training	
Level	*Units of measure: Training*
High	*Methodology provides significant training and awareness capability to all of its stakeholders, participants and the analysis team, with a specific section on security training and awareness.*
Medium	*Methodology provides training and awareness capability to selected group of stakeholders, participants and the analysis team conducting the information risk assessment.*
Low	*Methodology provides general awareness and training capability.*

Table 3-4: Grading for Training

Qualitative Measure of Criteria - Functionality	
Level	*Units of measure: Functionality*
High	*Methodology provides strong attributes to perform the required functions: "Data Collection", "Analysis", "Validation", "Reporting", "Presentation", throughout the risk assessment process.*
Medium	*Methodology provides adequate functionality to perform the required functions.*
Low	*Methodology provides limited functionality to perform the required functions.*

Table 3-5: Grading for Functionality

Qualitative Measure of Criteria – Guidance in Organizational Factors	
Level	*Units of measure: Guidance*
High	*Methodology provides excellent guidance on organizational factors that impact the successful implementation of an information risk assessment. These include executive sponsorship, stakeholders, maturity level, open communication, formation of an analysis team, and authority.*
Medium	*Methodology provides organizational factors, with guidelines on their implementation in undertaking of information risk assessment. These guidelines are specific to the targeted industry group.*
Low	*Methodology provides guidance in organizational factors, with limited guidelines on how to implement them.*

Table 3-6: Grading for Guidance in Organizational Factors

Qualitative Measure of Criteria – Usability	
Level	*Units of measure: Usability*
High	*Methodology has detailed guidelines for each phase, yet it can be used in various industries with a small degree of customization.*
Medium	*Methodology has guidelines for activities on a generic level in each phase and can be used in various industries, if customized properly. Its use is regional.*
Low	*Methodology has guidelines in a descriptive manner, while its use stays limited.*

Table 3-7: Grading for Usability

Qualitative Measure of Criteria – Consistency	
Level	*Units of measure: Consistency*
High	*Methodology provides consistency within the approach in terms and definitions to guide users in the same direction.*
Medium	*Methodology provides a common understanding with no established glossary or reference of terms.*
Low	*Methodology may be interpreted differently by different audience, has limited elements to attain consistency.*

Table 3-8: Grading for Consistency

Qualitative Measure of Criteria – Tool Support	
Level	*Units of measure: Tool Support*
3	*Methodology is supported by an electronic tool, which provides templates for each activity, as well as reporting and graphical presentation capability.*
2	*Methodology is supported by an electronic tool, which provides templates for each activity.*
1	*Methodology is supported by templates only.*

Table 3-9: Grading for Tool Support

	OCTAVE	*IRAM*	*CRAMM*	*EBIOS*	*IT Grundschutz*	*CORAS*	*NIST SP800-30, SP800-53*	*Microsoft*
Structure	*Medium*	*Medium*	*Medium*	*High*	*Low*	*Medium*	*Low*	*High*
Identification	*High*	*Medium*	*High*	*Medium*	*High*	*Medium*	*High*	*Medium*
Techniques	*Medium*	*Medium*	*High*	*Medium*	*Low*	*Medium*	*Low*	*Low*
Training	*Medium*	*Low*	*Medium*	*Low*	*Medium*	*Medium*	*Low*	*Low*
Function-ality	*Medium*	*Medium*	*Medium*	*Low*	*Low*	*Medium*	*Low*	*Low*
Guidance	*Low*	*Medium*	*Medium*	*Medium*	*Medium*	*Low*	*Medium*	*Medium*
Usability	*Medium*	*Medium*	*Medium*	*Medium*	*Low*	*Low*	*Medium*	*Low*
Consistency	*High*	*Medium*	*High*	*High*	*High*	*High*	*Medium*	*Medium*
Tool Support	*Low*	*Medium*	*High*	*Medium*	*Low*	*Medium*	*Low*	*Low*

Table 3-10: Comparative Criteria

The above table depicts the overall criteria on which we compare the present methodologies. Based on the descriptions for each methodology in Chapter 2, we conclude that each methodology adopts and incorporates a set of phases, tasks, or processes, such as identification of information assets, threat and vulnerability assessment, risk analysis, risk prioritization, understanding the level of maturity in information security, security awareness and training, communications planning, project planning, in different levels.

These activities are commonly considered to greatly influence the successful outcomes of an information risk assessment. A common inherent feature characterizing these frameworks is the presence of basic functionalities that form the core of a risk assessment methodology, such as data collection, analysis, validation, reporting and presentation.

This derives a general trend towards building and implementing standardized frameworks of information risk assessment, designed to understand the information risks of the organization. Appropriate actions are performed at each step of the information risk assessment in pursuit of the final goal of determining a profile of the organization's information security risks.

Structure: Methodologies in information risk assessment provide - through phases consisting of several activities - the ability to perform several steps: asset identification, measuring organization's security understanding, threat and vulnerability assessment, impact assessment and risk assessment. While structure is critical to guide a user in implementation of information risk assessment, it also brings limitations in flexibility to customize the methodology which may be required to use the methodology across different industries.

The existing methodologies discussed are structured in phases and activities. The steps of each methodology are described in Chapter 2. NIST 800-30 and IT Grundschutz can also be presented as guidelines. The tasks executed in different phases remain the same, although their sequence may change from one methodology to the other. As a result of this, the phases can be viewed as misplaced. For example, the impact analysis is made in the first phase of the IRAM methodology, whereas it is placed in the third phase of the OCTAVE methodology. The structure of EBIOS is specific for defense industry and

French government, as its original development reason. Microsoft's structure is also very adaptable to IT companies like Microsoft, bringing an element of specificity to its structure.

Identification: The characteristics identified in each phase are different from one methodology to another, which impacts how they approach determining scope. Identification is critical in the initial scoping of the effort. OCTAVE scopes the effort iteratively in the first phase, while also bringing an element of validation. This is done trough identification of inputs (assets, the areas of concerns, and the security requirements of the organization) in the first three processes, starting with the senior management, continuing with the operational management and ending with the staff level. In IRAM, the scope is determined prior to the start of the first phase. The critical assets of the organization are identified prior to conducting business impact analysis. This activity is usually done during the first phase of the other methodologies. NIST SP 800-30, SP 800-53 and Microsoft also include a risk management, presenting a wider scope of analysis. The criticality determines the scope of the assessment. As the critical information assets and their dependencies are identified within the risk assessment, the scope is revised. Therefore, it is ideal to prepare a draft scope at the beginning of the project and revise as more information is gained during the assignment.

Techniques: Different techniques are employed in the methodologies and at different stages of the information risk assessment project. One commonality is that IRAM, IT Grundschutz, CRAMM, EBIOS, CORAS, NIST SP 800-30 propose a catalogue of threats to select the appropriate ones for the organization. Microsoft and OCTAVE do not include a threat catalogue. The list of threats is specific to each organization; however, a

starting list is useful for the organizations who are conducting the information risk assessment for the first time.

In terms of presentation, CRAMM includes techniques for better visibility and communication, such as the graphical representation of the results and reporting through its software, CORAS uses visual techniques, OCTAVE refers to the threat tree diagrams. The other methodologies provide templates, but do not include specific visual tools or graphical representation of results for easier management review.

None of the present information risk assessment methodologies involve quantitative risk assessment techniques. Risk evaluation is the one of the most critical steps in present methodologies. The present methodologies do not propose a model nor refer to quantitative approaches in evaluating information risks, although there are many software tools available for modeling and quantifying of risks in other areas outside of information security, which can be adapted to the information risk assessment methodologies.

Another pitfall is that risk evaluation depends on a set of criteria which is highly impacted by the subjectivity of the participants. Iteration, review and validation of the results decrease this ambiguity to a certain extent, while including the participants in the process helps them to own the implementation exercise of the security. Thus, open communication, knowledge transfer, change management are critical organizational factors in the process.

Training: Information risk assessment is the first step to help a given organization in reducing and successfully responding to information risks. A training program for the analysis team conducting the assessment, as well as a staff training and awareness program in information security is necessary to accompany the process in handling

information security risks. While information security is perceived as primarily information technology staff's responsibility, given the fact that most threats are internal to the organization, it requires everyone's contribution to reduce the risk. The majority of the methodologies include information security best practices, like ISO 17799 which provides internationally recognized best practices in information security and can be leveraged in a survey form. This survey is critical to measure the awareness of participants in information security risks and practices, but also is used as a tool to increase awareness. The organization's specific control environment is also a critical input to consider in preparation of the questions for a survey which measures participants' awareness in security.

The minority of the present methodologies have formal trainings organized by the source organizations to transfer the knowledge necessary to the analysis team of the organizations, like OCTAVE provided by Carnegie Mellon University. These training programs include exercises that practice the activities in each phase. A larger scale of training program is not available with the methodologies and is employed separately for information security by those organizations who realize its importance.

Functionality: "Data Collection", "Analysis", "Validation", "Reporting" and "Presentation" represent major activities in each methodology, while some of the methodologies consist of these attributes more than the others. CRAMM with its software improves the automated reporting capability. CORAS makes use of the visual tools that are helpful in presentation of the data. In OCTAVE, results from each phase are validated at the closure of the phase. EBIOS, NIST SP 800-30, IT Grundschutz and Microsoft methodologies provide guidelines.

One of the functionalities is the threat and vulnerability assessment phase that is mainly technical and is performed by information security specialists who are specifically trained in this area. "Analysis" differs from examination in that it refers to interpretation, by different members. It is recommended that the analysis team conduct a workshop to review the findings from the threat and vulnerability assessment once the results are established.

Guidance: The studied methodologies provide guidelines and a structure for the user to follow. They do not elaborate on project and change management requirements adequately that are critically required within the process of information risk assessment adequately. While the exercise seems to be primarily a technical challenge, it is indeed more of an art in obtaining the collaboration of the individuals within the organization and making the changes required with the controls established to be more resilient to overcome security incidents. The proposed methodologies are limited in addressing the issue of change required in the organization to establish a risk aware culture.

The methodologies are not detailed in providing tasks to demonstrate how to sustain sponsorship, keep the stakeholders engaged, foster a spirit of open communication and provide sufficient authority to the analysis team. Training and awareness is a critical element in risk recognition, not considered as a specific phase in the methodologies.

Usability: This characteristic refers to the degree in which an information risk assessment methodology is able to expand its usefulness. An information risk assessment methodology is mostly used in a certain region, with respect to its original language, industry standards, local best practices and regulatory environment. While the Microsoft and IRAM frameworks are unique in providing features tailored to support technology

organizations, EBIOS and NIST are developed specifically for defense organizations, OCTAVE primarily developed for defense organization can be properly described as general in its application. OCTAVE and NIST are widely used in North America; IRAM is mostly used in UK and Europe; EBIOS in France and French speaking regions; CORAS in Norway, Sweeden and in some areas of Europe; Microsoft methodology in technology companies in US; IT Grundschutz, in Germany, Austria and the rest of Europe. OCTAVE, EBIOS, NIST are originally developed for defense industry, but have expanded their use over the years, in terms of industry.

Consistency: Consistency in the definition and understanding of these concepts contribute significantly in eliminating confusion, with regards to selecting the appropriate methodology that is adaptable to the organization's needs. In seeking to identify common terms, it is useful to establish a common understanding of terms to enhance communication. The methodologies provide descriptions of the terms and some of them have a glossary.

Tool Support: It is appropriate to note that the information risk assessment frameworks presented herein give little consideration to important features such as modeling and quantification of risks which impact the results and the quality of the process. Another issue is that the frameworks provided have electronic tools, but no automatic reporting capability, except the excel sheets or the other templates provided within the tool. Thus, there is a considerable administrative part that goes along the process of recording, reporting and keeping track of the records. CRAMM decreases this burden with its software.

The challenge with a software product is the time spent to effectively and efficiently use it during the process. The licensing costs, training time required for the tool and the support time for maintenance needs also to be considered in the project cost and schedule management, specifically for organizations conducting information risk analyses, for the first time with an accompanying tool.

With respect to the set of shortcomings observed along the analysis in Chapter 2 and comparative study in Chapter 3, the new information risk assessment methodology should be seen from a perspective of improving project management and quality aspects with the major objective: present an integrated process in information risk evaluation. The other points can be considered as those common and essential in any information risk assessment process.

Chapter 4: Integrated Methodology

4.1 Introduction

In this chapter, the primary objective is to propose an integrated information risk assessment methodology developed with support of the literature review and comparative analysis presented in Chapters 2 and 3. The intent is to present a new methodology in information risk assessment designed to:

- Construct further on common practices related to the existing state of the art methodologies;
- Incorporate the strengths of the reviewed methodologies;
- Address the weaknesses of the reviewed methodologies; and
- Propose new ideas to improve the state of the art on information risk assessment methodology.

Most of the professionals in the information security field are focused in technical aspects in information security. This study brings a process centric approach that addresses the challenges in assessment of information security risks within the organization, through a structured methodology, based on principles defined. The research reported in this chapter is an effort to contribute to the state of the art information risk assessment methodologies.

It is not to create a comprehensive methodology designed to outperform the existing processes. In this respect, the characteristics of the information risk assessment methodology presented in this chapter are summarized first with its foundation named as principles and is followed with its phases. Phases are steps that the information risk analyst or the analysis team is required to take in a sequential manner. On the other hand, principles are a set of specific objectives that forms the foundation of the methodology, and that the information risk analyst or the analysis team is required to progressively achieve throughout the information risk assessment process. [15]

4.2 Principles

A principle represents a fundamental attribute or requirement of the information risk analysis that cannot be uniquely associated with a single phase. A principle is set and followed through the methodology, throughout its phases. Based on the following principles which we explain each in detail, we develop our methodology. Some of these principles apply to comparison frameworks of other security processes, such as in cyber-forensic processes [15]:

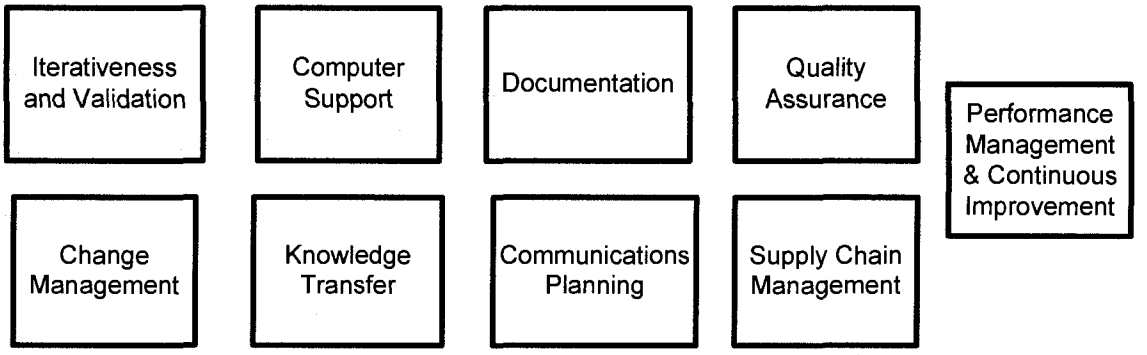

Figure 4-1: Principles of the Integrated Methodology

4.2.1 Iterativeness and Validation

The iterativeness and validation principle stipulates that for each phase of the information risk assessment, results from the previous phases are considered as inputs. The proposed methodology has a control structure that permits feedback from phases together with the iteration of some of the steps when required.

Validation is required throughout the process of risk assessment. In order to start a new phase in the risk assessment methodology validated results from the preceding process are required. Validation is also required for the sustainability of information risk assessments. It is necessary to introduce an ongoing program of validation to ensure that the security strategy and procedures set as a result of the information risk assessment are correctly followed and the results from the assessment are valid. Communication and knowledge transfer throughout the project also support validation mechanism.

4.2.2 Computer Support

An important feature of the proposed process is computer support for information risk assessment. It means that the process is implemented by using software or electronic worksheets or other tools. It is directed towards guiding the information risk analyst or the analysis team through the phases when conducting an information risk assessment. The methodology enables a database model to be established, with respect to the parameters and activities required in each phase. The model is to be user friendly and have automatic reporting capability to present data.

4.2.3 Documentation

The documentation principle stipulates that all activities executed within an information risk assessment must be fully documented. During the reporting and presentation phases,

documentation pertaining to the previous phases is assembled and compiled into a final report. It is important to maintain documentation regarding the review and results of the risk assessment as well as all approved preventive and corrective measures. All the documentation collected and created during the process is properly archived, in case of reference for future assessments. Documentation also serves as a tool for compliance with requirements of the regulatory bodies, as well as the third party auditors.

4.2.4 Quality Assurance

The quality assurance principle is integrated to ensure the consistent quality of all phases and tasks that are undertaken during an information risk assessment process. It is required to provide appropriate procedures and training in order to meet the requirements of control, accuracy, and reliability of the collected data during the information risk assessment. All phases require a quality assurance mechanism to monitor executed actions, control, and ensure their validity of the outputs.

4.2.5 Change Management

An important element in conducting an effective information risk assessment is change management plan. This principle is more relevant to risk management program, specifically in implementation of risk mitigation actions as countermeasures for identified risks. On the other hand, with respect to the fact that the assessment of information risks is the first step of the risk management program, it is important to consider the change vision in the first step. If the organization's culture incorporates information risk management within its daily operations, it is more likely to establish a successful risk management program. The vision for change provides direction on why the change initiative is being undertaken. Introducing new risks to the audience that they were

unaware requires managing the change effectively, throughout the risk assessment process. Thus, the objective is to design communication plan for change that ensures broad-based buy-in into information risk assessment project as a fundamental component.

A meeting with senior management and interviews with stakeholders occurs to analyze their positions on impact of change in establishing a change management program. This information is used to recommend appropriate responses in the scheme of the project, specifically in defining the security strategy and countermeasures to the threats identified. At the end of the risk assessment process, responsibilities are assigned for each mitigation activity to implement the change to secure information assets of the organization.

4.2.6 Communications Planning

This principle stipulates the need to plan the communication throughout the information risk assessment process. Usually, a gap in communication exists between IT and the business within an organization. IT security managers are generally not in the top management ranks within an organization, yet is the owner of IT security risk assessment. The business owners are perceived of having only limited knowledge in security, but could cause great threat potential due to their inadequate knowledge, by the majority of IT staff.

In order to address the communication issues and sustain commitment to the process and upper management support, the owner of the IT risk assessment project is selected from the business side of the organization, preferably a person with a full understanding of challenges of information security. Business needs to own the IT risk assessment project and thus, the risk management process that takes place once the assessment is completed. Any, or a combination, of the techniques can be used in gathering information relevant to

an information asset. One of them is to utilize questionnaires to collect relevant information on the present controls of the asset. The questionnaire can also be used during work-shops or interviews. Interviews conducted with business and IT staff also allows useful information to be gathered. Site visits allow identifying the physical vulnerabilities and possible threat scenarios. Review of policy documentation, system user guides, procedures system administrators must adhere are other ways of gathering information.

4.2.7 Supply Chain Management

Present methodologies focus directly to the critical information assets of the organization, while our process-centric methodology focuses on the critical processes of the organization. This helps to produce more viable results, because most of the organizations who undertake information security risk assessment have a series of processes interlinked and an infrastructure connecting the information required within these processes. Information flows between various departments within the organization as well as to and from the third party suppliers outside the organization. The interdependence between the partners and the organization increases with respect to effective relationships [41]. The success of the business relationships between these parties is achieved through mutual trust gained through open communication. The exchange of information of the different parties within the operating business environment brings additional risks that need to be considered in the information security risk assessment.

An effective conflict resolution mechanism is highly important to strengthen the supply chain relationship. The presence of flexibility, cooperation and trust are basis to the

relationship. Specifically, commitment of top management is crucial for the success. Good organizational arrangements are necessary for information sharing. Inadequate sharing of information breaks the supply chain partnerships. Communications and change management principles support the concepts in supply chain. The analysis team needs to understand how supply chain dynamics work within an organization which will directly impact the risk portfolio, as well as development of the protection strategy, risk mitigation plans and naturally success of the security program in the organization.

4.2.7 Knowledge Transfer

There is a need to manage knowledge transfer while conducting the information risk assessment. One of the objectives of the information risk assessment is to increase information security awareness within the organization. In order to measure the level of security understanding in the organization, a security survey can be conducted. The questionnaire, based on the best practices of an internationally recognized standard needs to be customized to integrate specific compliance requirements of the organization.

Transferring the knowledge in information security to participants during the process also ensures higher quality, sustainability and continuity of efforts, upon completion of the information risk assessment. The way to transfer knowledge throughout the risk assessment process is by working closely with the risk assessment participants during and after the risk assessment, involving them to ensure that all pertinent knowledge is transferred to relevant staff.

4.2.8 Performance Management and Continuous Improvement

Continuous improvement to attain best practices in information security is part of the new methodology. Breakthrough improvement referring to discontinuous change is not

preferred as we are looking for gradual, continuous improvement that does not require the organization to stretch to the point of functioning in a completely different way. What we are looking for is incremental improvement actions, applied throughout the risk assessment process as awareness of the participants increases and unknown risks are identified. Many organizations are familiar with the concept of continuous improvement through their quality management program. The challenge of the new methodology is to implement the similar way of thinking to the information security risk assessment process.

Continuous assurance and monitoring is done throughout the process. The priority is to monitor the high risk areas. Risk related activities that have high incidence of change need to be monitored. While the change can be sudden, gradual or persistent, gradual change is what we are targeting throughout the process. A potential failure of the change management program is when the changes are implemented or imposed without regard to the risks involved, and thus monitoring and validation is necessary in every step to ensure the change is gradual and could be sustained. Performance measurement is part of the validation mechanism. There are certain criteria that should be watched out for, concerning performance indicators, which we discuss in our case study.

4.3 Phases

Based on the principles covered above, we develop the methodology and display the activities or tasks that need to be executed during an information risk assessment process, phase by phase, in a sequential structure, as shown in the following diagram.

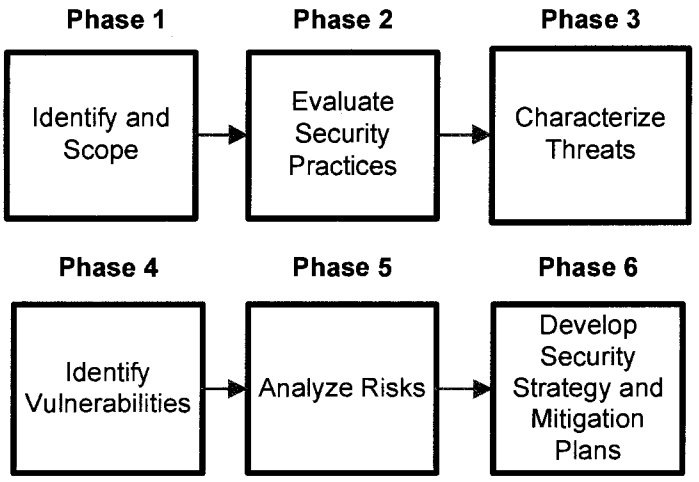

Figure 4-2: Phases of the Integrated Methodology

From hereon, at the beginning of each phase, we provide a description of that phase, emphasizing what it brings to the integrated methodology different from that of the existing methodologies. We state the objectives of the phase. A schematic diagram demonstrates the activities to be conducted step by step, in each phase. We explain each activity, in sequence. At the end of each phase, we summarize the inputs that are required and outputs that are produced.

4.3.1 Identify and Scope

Description: The first step in an information risk assessment undertaking is to clearly understand the business objectives of the organization defining the processes that are critical for the organization to achieve its objectives and the relationship of these processes to the information assets. Once the information assets are identified, we start collecting information on the threats that face the assets. This sets the scope of the information risk assessment. The highlights of the first phase that provide improved functionality, compared to the existing methodologies are:

- Process centric assessment based on supply chain principles; and

- Scoping with clear definition of time, budget and resource commitment; based on the project management practices;

Objectives: To obtain a general understanding of the business and to define what is important to the business and to set the scope. Prepare the project plan and have it approved.

Activities: The following activities, illustrated in the diagram, take place in Phase 1.

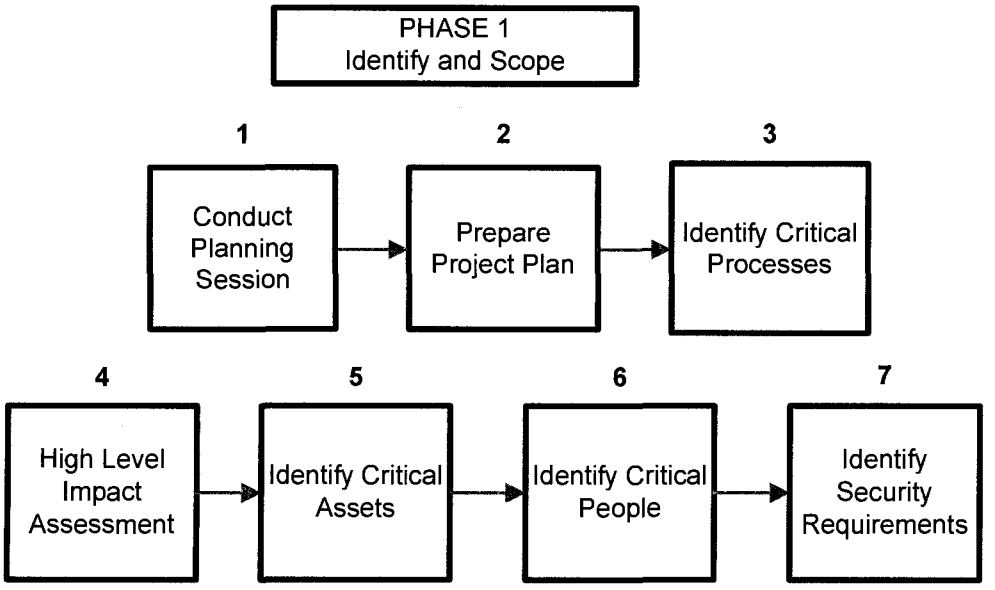

Figure 4-3: Phase 1 Activities

1. Conduct Planning Session: First, we organize a session with stakeholders who are at the upper levels of management. Sponsorship for the information risk assessment initiative is part of the agenda for the meeting. In the working session, we explain the needs and expected benefits to conduct an information risk assessment. We target to understand how much of uncertainty stakeholders are willing to expect as an input in our scoping. The risk tolerance for the organization is discussed, in consult with the upper

management. This is further enhanced by defining the perimeters of "high", "medium" and "low" risk areas in the risk portfolio diagram discussed in Phase 5.

We define the analysis team to undertake implementation of the methodology in the organization. The members of the team are selected experts in their own functions, both from business, and information technology side of the organization.

2. *Prepare Project Plan:* Once the management session is executed and the team is defined, we draft a project management plan. The project management plan consists of the activities step by step that are required to be conducted throughout the assessment. Activity durations are matched with the amount of time required from the resources, which is used to derive the budget of the project. The cost, schedule and resource plan of the project is presented for management approval. In preparation of the project plan, we suggest the user refer to the best practices established by Project Management Institute (PMI) which recognizes five basic process groups and nine knowledge areas typical of almost all projects. The basic concepts are applicable to projects and programs. The five basic process groups are initiation, planning, execution, control and closing which is presented as follows according to Project Management Institute, [45]:

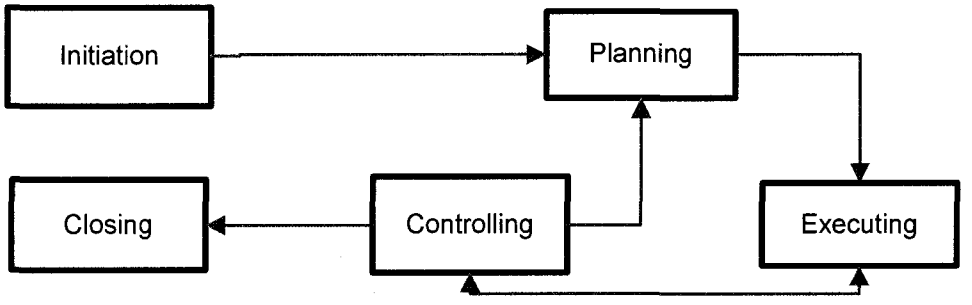

Figure 4-4: Process Groups, Project Management Institute

The nine knowledge areas are of PMI [45] are (1) Project Integration Management, (2) Project Scope Management, (3) Project Time Management, (4) Project Cost Management, (5) Project Quality Management, (6) Project Human Resource Management, (7) Project Communications Management, (8) Project Risk Management, and (9) Project Procurement Management.

Approved project plans include approved resource planning, activity planning, critical milestones, project schedule, project cost, project risk planning, project communications planning, change management. Upon presentation of the project plan with project schedule and budget, management now has the tools to make an informed decision to undertake information security risk assessment. At this point, we ask for commitment from the management and them to sign off on the project plan.

3. *Identify critical processes:* Once the budget is approved, we start the information risk assessment process, with the identification of business processes and assets. Organization charts help us to identify the departments and their relevant directors, managers and staff members. Process diagrams show the inputs and outputs of each process and their dependant processes. In selection of the critical processes, the analysis team needs to review the list of main business processes, in the organization. For each applicable main process, the inter-relations between other processes and assets are determined.

4. *High Level Impact Assessment*: For each main process, its criticality to the business is assessed in case an incident occurs. The magnitude of the impact on the organization needs to be determined if the processes are accessed or performed by unauthorized people, if the resources-assets are modified without authorization or lost, destroyed, cannot be performed due to an interruption impacting their availability.

An impact value from "High" to "Low" is assigned for each applicable scenario, qualifying the assessment with comments. Then, the most critical processes which have the highest impact, on the organization are selected.

5. *Identify critical assets:* Inputs, processing assets and outputs are defined for each critical process selected in order to select the top critical assets. Inputs are what people need or use to perform their jobs to start the process, processing assets are what people require to perform the process, and the outputs are the assets people produce as a result of conducting a process. The reason for selecting each critical resource-asset is documented.

6. *Identify critical people:* The knowledge and skills of the critical people required for each critical process is documented by considering the special skills or knowledge which would be difficult to replace and yet vital to the organization. For each critical information asset, users, the information owner and the information custodian must be determined, by determined.

The "information owner" is usually the manager of the department or the business unit, who is responsible for the creation of information. Information owners are also responsible to ensure information classification is in place and current, as well as the access rights to the information.

The "information custodian" is the authority assigned by the information owner who has the expertise to manage the technical aspects of the information includes back ups, recovery, implementation of access rights, control and monitoring.

7. *Identify the Security Requirements:* The security requirements for each critical resource-asset are determined from the categories of confidentiality, integrity, and availability. One asset may have more than one security requirement critical to protect.

Inputs of Phase 1:

- Expected benefits of information risk assessment to the organization;
- Presentation of the information risk assessment methodology;
- Specific security needs of the organization;
- Concerns and objectives of the upper management;
- List of business processes of the organization, process diagrams, procedures;
- List of resources – assets of the organization; and
- Organizational chart.

Outputs of Phase 1:

- Analysis team members are identified;
- Project plan is approved by management;
- Critical business processes are identified;
- Critical resources- assets of the processes are selected, specifying the reasons roles and responsibilities related to the asset; and
- Information security requirements of the critical resources – assets are identified.

4.3.2 Evaluate Security Practices

Description: This phase is dedicated to collecting relevant data from the organization in order to understand the control structure and the present security practices applied in the organization.

The highlights of the second phase are:

- Analysis of the control structure of the organization, from an audit perspective;
- Measuring the level of security in the organization, with specific questions relevant to the organization's security objectives.

Objectives: To understand business and security objectives. To determine the level of maturity in security within the organization and the level of compliance to the information security best practices.

Activities: The following activities, illustrated in the diagram take place in Phase 2.

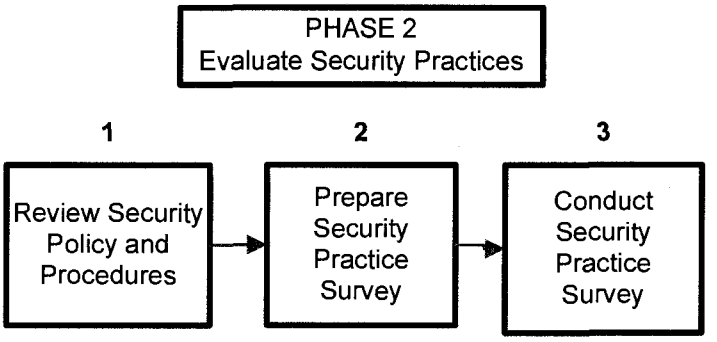

Figure 4-5: Phase 2 Activities

1. Review security policy and procedures: We obtain security policy and procedures, as well present controls. Security policy and related information security procedures help us to identify the objectives stated by the management and what staff members within the organization are required to respect. We then organize an information gathering session with the selected participants of the organization.

2. *Prepare Security Practice Survey:* A security practice survey enables an analysis team to evaluate the extent to which security practices are reflected in the way the business manages security. Best practices in information security are present in the existing methodologies presented in Chapter 3; OCTAVE, IRAM, IT Grundschutz, and the

international standard ISO 17799. The organization undertaking information risk assessment exercise must develop a proprietary information security survey building on the best practices in the industry, addressing specific security objectives and security requirements of the organization based on its own unique operating environment. The security practice areas must be categorized and specific questions pertaining to each security practice area must be created as part of the survey preparation.

One categorization could potentially be to divide security practices into strategic and operational, as done in OCTAVE. Strategic security practices are those that focus on organizational issues at the policy level. They include business-related issues as well as issues that require business-wide plans and participation can be summarized as [9]:

- Security Awareness and Training;
- Security Strategy;
- Security Management;
- Security Policies and Regulations;
- People;
- Collaborative Security Management; and
- Contingency Planning/Disaster Recovery.

Operational security practices are more technical and focused to the practice area of information technology staff. They focus on technology-related issues. They include issues related to how people use and protect technology in their daily operational environment. The operational security practices can be summarized in the following categories [9]:

- Physical Access Control;
- Monitoring and Auditing Physical Security;
- System and Network Management;
- Monitoring and Auditing IT Security;
- Authentication and Authorization;
- Vulnerability Management;
- Encryption;
- Security Architecture and Design; and
- Incident Management.

While the above categories present an example of how to classify best practices in information security; an internationally recognized standard, ISO 17799 [40] uses a similar list as best practices in information security. An organization uses best practices that are most relevant to its requirements as a starting point, and then tailors them according to the needs and prerequisites of the control environment it is operating in.

3. *Conduct Security Practice Survey*: The survey can be conducted within a working session with the participants or in one-to-one interviews, or can be distributed to the participants for them to respond individually. In completion of the survey, what the business currently doing well in a specific security area and not doing so well need to be considered. In response to their knowledge of a security practice area, the participants select between "Yes", "Yes, but not effective", "No" and "Do not know". According to the findings from the security survey analysis, the analysis team determines the status of each security practice area question, by one of the following choices:

- *Green* – The application of security practices in the organization is satisfactory;
- *Yellow* – The application of security practices in the organization needs some improvement; and
- *Red* – The application of security practices in the organization needs significant amount of improvement.

Inputs of Phase 2:

- Security policy and procedures;
- Present controls in the organization; and
- Security best practices survey questions.

Outputs of Phase 2:

- Level of maturity in security awareness in the organization;
- Degree of compliance to the best practices is determined; and
- Areas of weaknesses in security practices.

4.3.3 Characterize Threats

Description: At this phase, a team composed of participants from business and IT conduct a detailed information risk assessment. The team focuses on the critical processes and their related assets identified in the first phase. The team starts by identifying the threat sources that have a potential to produce such threats. The team also documents the history of threat occurrences. The highlight of the third phase is to characterize threats based on the potentiality, considering the likelihood, strength of the motive of an actor, as well as the past history of occurrence.

Objectives: To identify threats, actors and their motives. To document the history of the threat scenarios occurred in the past.

Activities: The following activities, illustrated in the diagram, take place in Phase 3.

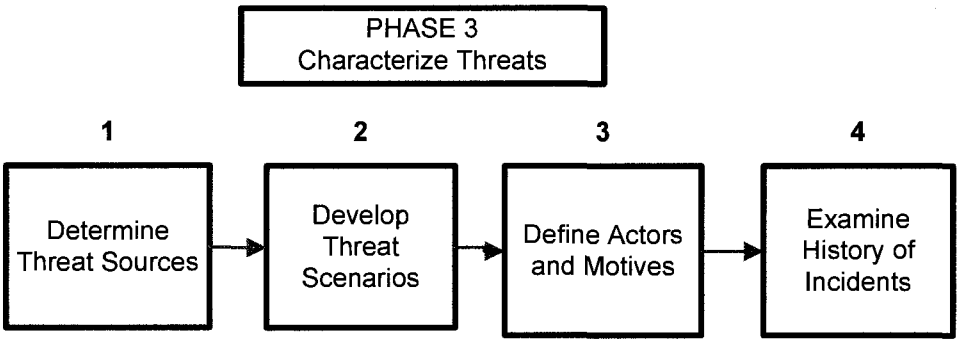

Figure 4-6: Phase 3 Activities

1. Determine Threat Sources: A threat profile is defined in OCTAVE as, a structured way of presenting a range of threats to a critical asset. Threats in the profile are grouped according to the source of the threat. Present methodologies often have a generic threat profile which is a catalog of threats containing a range of potential threats under consideration. IT Grundschutz [29] has a detailed catalog of threats which consists of possible threats that may be applicable to the organization. The generic threat profile is a starting point for creating a unique threat profile for each critical asset, according to their use in a specific organization.

Threat scenarios are characterized by their related asset, by the people who may violate the security, by the access method of the people and their motive. The outcome of the threat is the end result, causing disclosure, modification, destruction or interruption by violating one or more of the security requirements of an asset.

Each critical asset, whether it is an application, database, a system or information has a unique threat profile that needs to be addressed by the participants of the information risk

assessment. One of the following categories or a combination of more than one may be threat sources:

- People: The types of threats involving people require direct action by a person and can be performed deliberately or accidentally. A system interruption due to natural causes does not fit into this category.

- Network access: The threats in this category are network-based threats to the organization's critical assets.

- Physical access: The threats in this category are physical threats to the organization's critical assets.

- Natural Causes: The threats in this category are problems that do not directly involve human actors.

- Utility Causes: The threats in this category are problems related to the third party suppliers, like telephone companies or utilities, which ultimately impact the operation.

2. *Develop Threat Scenarios:* Threats are represented visually in a structure using the categories of threat sources above. Each critical asset has a different threat profile. All threat scenarios must be discussed during the assessment, regardless of their impact, probability or the present controls on them. This is extremely important as probability of event occurrences may change and impacts may vary, as well as control adequacy may not be accessed correctly.

3. *Define Actors and Motives:* In determining the actors, outsiders and insiders are considered in terms of threat sources, as insiders are the dominant cause of security

breaches. Their access methods to the valuable asset, either via network or via physical means needs to be considered. The actor's motive and the strengths of the motive are identified. The ranking of actor's motive became more of a concern, with respect to the increase in terrorism threats. In order to define the actor's motive, the options from "High" to "Low" must be considered:

- *High* – The actor has defined goals, specifically targeting the critical asset; and
- *Low*– The actor does not have specific goals, is targeting any asset that can be attacked easily.

4. Examine history of incidents: In reference to the threat scenarios developed, the incident history is reviewed, to identify if and how frequently the threat has occurred in the past. This can be done by reviewing any objective data available, such as documented incident data, system logs or by obtaining subjective data, based on interviews, from what people recall.

Inputs of Phase 3:

- Types of threats and sources; and
- Critical assets and their security requirements identified.

Outputs of Phase 3:

- Selected types of threats for each critical asset;
- Determination of actors and their motives for the relevant threat scenarios; and
- Frequency of occurrence for selected threats and accuracy of data.

4.3.4 Identify Vulnerabilities

Description: In this phase, for each critical asset identified the analysis team determines vulnerabilities. The highlight of Phase 4 that provides improved functionality, compared to the existing methodologies is assessing physical vulnerabilities in addition to electronic vulnerabilities.

Electronic vulnerability assessment focuses on the vulnerabilities exposed through the network access paths, which are the ways in which systems, devices, information, or services can be accessed via an organization's network. Physical vulnerability assessment focuses on the vulnerabilities exposed through the physical access paths where the critical information of the organization resides.

Objective: To examine access paths (electronic and physical) to critical components of the asset or system of interest.

Activities: The following activities, illustrated in the diagram, take place in Phase 4.

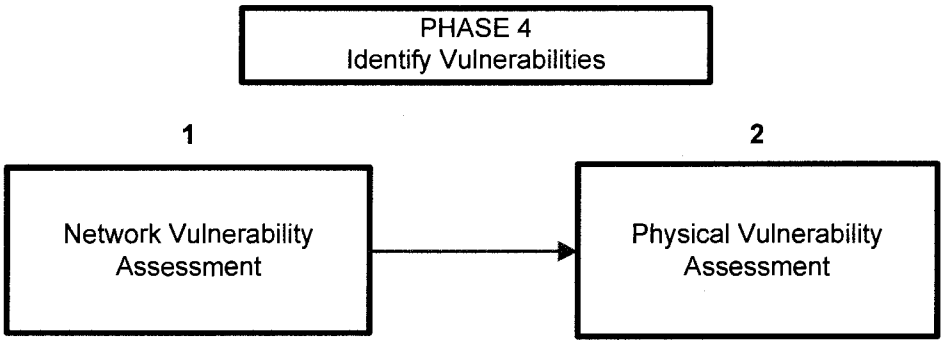

Figure 4.3 -7: Phase 4 Activities

1. *Network Vulnerability Assessment:* We start by examining the access paths, conducting a vulnerability assessment on the network. In terms of access paths, we first consider the interfaces for access used to transmit information and applications from the system of interest to people. We then determine if data storage locations are linked to

information on the system of interest. The access points and storage locations are analyzed. The analysis team determines which components people use to access the system of interest. The options include on-site workstations, laptops, or wireless components, home/external workstations and others.

We then compare the list of electronic components and access paths identified for the specific critical asset to other critical assets. The classes of components related to one or more critical assets are considered critical. Next, we identify the party responsible for maintaining and securing each class of components. The party responsible for maintaining and securing each class of electronic components must be identified.

We determine how well each class of components is currently protected. The extent of confidence is indicated, when maintaining each class of components in reference to the following scale:

- *Very much* –The objective data is available;
- *Somewhat* – A limited amount of objective data related to the estimate is available;
- *Not at all* – Little objective data related to the estimate is available; and
- *Don't Know* – There is not adequate expertise to make the estimate.

2. *Physical Vulnerability Assessment:* In this activity, we focus on the vulnerabilities exposed through the physical access paths where the critical information of the organization resides. The information usually resides in the main building of the organization, in the computer room and other defined locations. During physical vulnerability assessment, the electric power supply system, fire protection system, environmental control systems such as air conditioning, water protection, building entry surveillance are the areas in

scope of the review. Any potential weaknesses in these areas that may impact the security of the critical information in the organization are identified and documented.

Specific control measures are taken for the computer room. During the physical vulnerability assessment, the following measures are reviewed:

- If access to the computer room or the data centre is restricted to authorized personnel with a security access card;
- If security cameras are installed that helps to monitor traffic to and from the data centre;
- If the door alarms to selected restricted areas are functional;
- The operation of uninterrupted power supply (UPS) in the computer room;
- Sensors for temperature and humidity control;
- Smoke detectors and fire prevention equipment; and
- Visitors are authorized for restricted areas by the appropriate member of management and are accompanied by internal staff.

Inputs of Phase 4:

- Critical systems of interest; and
- List of components for storage of data from the system of interest;

Outputs of Phase 4:

- Selected key class components of critical systems of interest;
- Selected access paths;

- List of components for storage of data;
- Responsible for key class components;
- Extent of security protection for each key class component; and
- The existing physical controls for information security and vulnerabilities.

4.3.5 Analyze Risks

Description: This phase is to determine and analyze risks to the organization's information security. During this phase, the analysis team identifies risks to the organization's critical assets and develops the risk portfolio for the information security risks of the organization. The highlights of Phase 5 that provide improved techniques, compared to the existing methodologies are:

- Identification of residual risks, based on the controls established and the inherent risks through risk portfolio; and
- Impact rating, control grading, and risk tolerance defined based on the organization's goals and objectives.

Objectives: To identify risks based on the threats, impacts and likelihoods. To determine information risk profile for an organization, deriving the residual risk upon analysis of the inherent risks and the controls.

Activities: The following activities, illustrated in the diagram, take place in Phase 5.

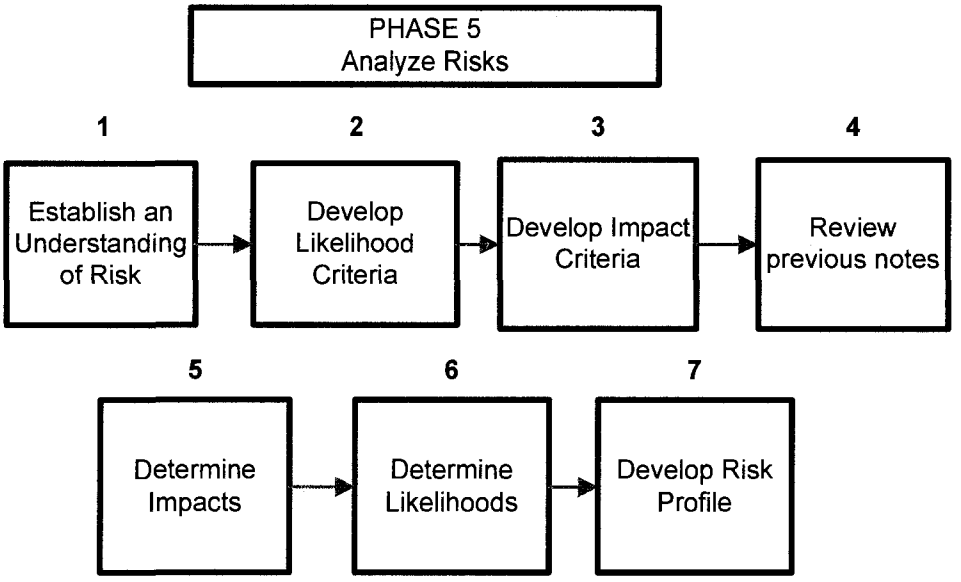

Figure 4-8: Phase 5 Activities

1. Establish an Understanding of Risk: In this step, we establish the understanding for risk, which is the possibility of suffering harm or loss, as defined in OCTAVE. NIST SP 800-30 [50] defines risk as "a function of the likelihood of a given threat source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization". In information security, the term risk refers to a situation an undesirable outcome violating the information security requirements of an organization's critical asset, resulting in a negative impact or consequence. An information risk is composed of:

- an incident
- uncertainty
- a consequence

In information security, the basic event is a security threat. Uncertainty is embodied in much of the information gathered during the evaluation. There is uncertainty surrounding whether a threat will occur and whether the organization is sufficiently protected against

the threat. Uncertainty is often represented using likelihood of occurrence, or probability. The consequence that ultimately matters in information security risk is the resulting impact on the organization due to a threat occurrence. Impact describes how an organization might be affected based on the threat outcomes.

2. Develop Likelihood Criteria: We first establish the criteria for the likelihood of an incident to occur, defined by a set of evaluation criteria that set definitions for likelihood values. These criteria are divided from high to low measures of threats' likelihood by considering a range of frequencies, such as daily, weekly, monthly, quarterly, semi-annually, once per year, once every two years, once every five years, once every ten years and above. The goal is to define probability measures based on how often threats are likely to occur:

- the types of threats to critical assets;
- how often each threat has occurred in the past (history);
- the vulnerabilities present in the system and infrastructure; and
- any additional relevant information recorded.

3. Develop Impact Criteria: Impact is directly linked to the organization's mission and business objectives. In creating impact evaluation criteria for the organization, types of impacts are considered, starting with those to the strategic goals of the organization, the customer confidence, health and safety, legal penalties and publicity. Tangible impacts, such as those to the organization's financial state, to the productivity and to other factors specific to the organization's operating environment are also considered.

We then establish the impact criteria via a facilitated discussion with management. When determining the impact severity levels relative to the organization, for the impact types described above, the impact severity is defined from high to low.

4. Review previous notes: Before conducting the rest of the activities for risk analysis, we review any notes and recommendations recorded during the previous processes. These notes and recommendations are important to the next activities conducted. The items in the scope of the review include threats to the critical assets, threat characteristics; such as threat actors, motive, incident history and the security requirements of the critical asset.

5. Determine Impacts: Each impact area is assigned an impact measure from "High" to "Low", based on the impact criteria set in the earlier step. When assigning the impact measures the factors defined in Phases 3 and 4 are considered. They are the motive for deliberate actions by human actors, the summary of network infrastructure vulnerabilities, physical infrastructure vulnerabilities and the contextual information about threat actors.

6. Determine Likelihoods: Similar to the likelihood criteria, the estimate of any threat occurrence must be adjusted in reference from "High" to "Low" for the likelihoods. In assigning likelihood estimates, the accuracy of historic data, the person's confidence in the estimate of motive strength, comprehensiveness of the evaluation of the network and physical infrastructure vulnerabilities are to be considered.

7. Develop Risk Profile: Risk is the product of its impact and likelihood. For known threats, the risk level is estimated and noted on the risk profile chart, based on its impact and likelihood. The chart is an easy to review visual product used to facilitate a discussion. The high risk areas composed of high impact severity and likelihood of occurrence are shown in "red". The medium risk areas are highlighted in "yellow" and the low risk areas

are highlighted in "green".

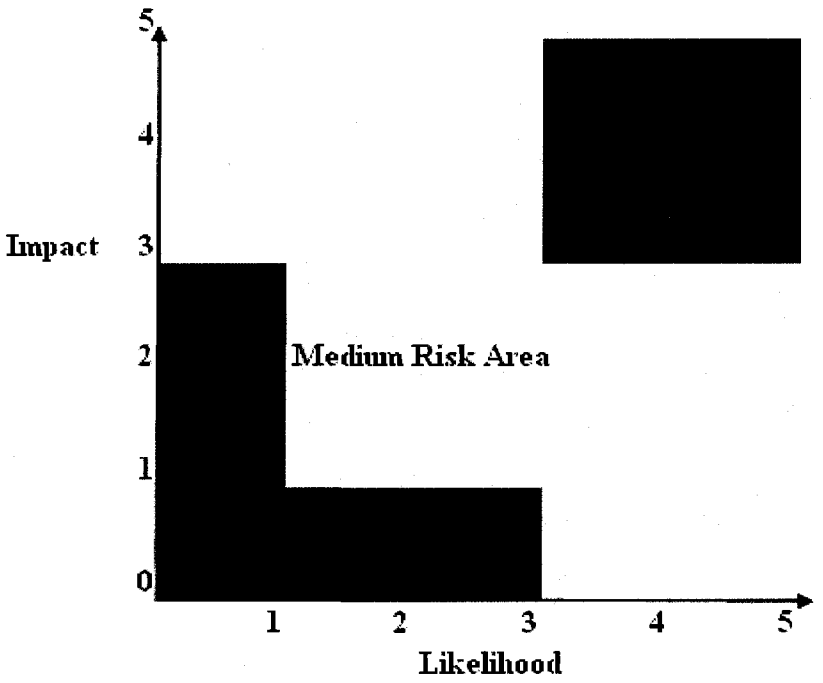

Figure 4.3 -9: Graphical Presentation of the Risks

Upon determining the organization's risk profile, organization's control structure is reviewed, based on the vulnerability analysis performed previously. If an identified risk shifts to a lower degree of severity, with respect to the present control, it must be identified. The remaining residual risk is discussed.

Inputs of Phase 5:

- Critical Assets;
- Threats identified for each asset in scope;
- Motive for actions by human actors;
- Summary of computing infrastructure vulnerabilities for network threats;
- Summary of physical infrastructure vulnerabilities for physical threats; and

- Contextual information about threat actors.

Outputs of Phase 5:

- Impact criteria for the organization defined;
- Impact measures are established;
- Probability measures are established;
- Each threat is assigned with a probability and impact;
- Prioritized risk portfolio of the organization; and
- Controls established and residual risks.

4.3.6 Develop Security Strategy and Mitigation Plans

Description: The success of the implementation of a risk treatment plan requires an effective management system that specifies actions and methods, assigns responsibilities and accountabilities for actions and monitors them against the specified performance criteria.

The highlights of this phase are the communication and change management discussed as principles. They must be present as an ongoing effort throughout the risk assessment to produce viable results, while they become more important in this phase, where plans to manage risks are developed to be implemented.

A method utilized is gap analysis in consult with security objectives is performed to define mitigation approaches to identified gaps in security.

Objectives: To determine and to select the risk treatment options for the information risks identified.

Activities: The following activities, illustrated in the diagram, take place in Phase 6.

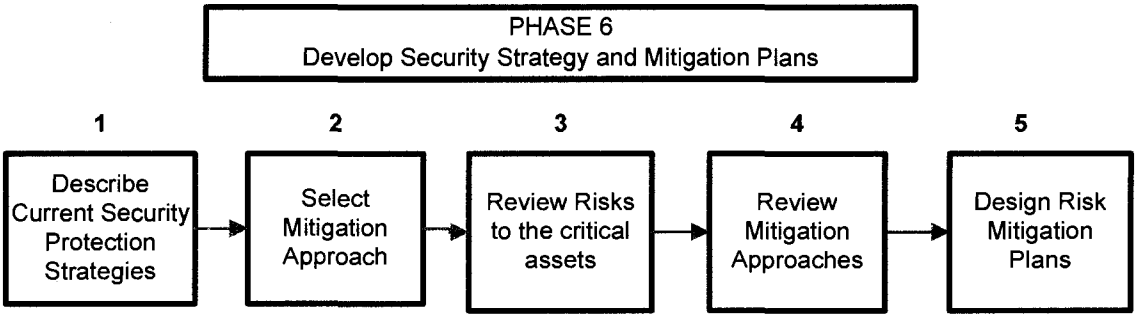

Figure 4.3-10: Phase 6 Activities

1. Describe Current Security Protection Strategies: Security best practices are available in each information risk assessment methodology, as explained in the earlier step "Evaluation of Security Practices". Each security practice area has multiple characteristics that must be addressed. The following diagram depicts the characteristics for "*Security Awareness and Training*", a strategic security practice area [9]:

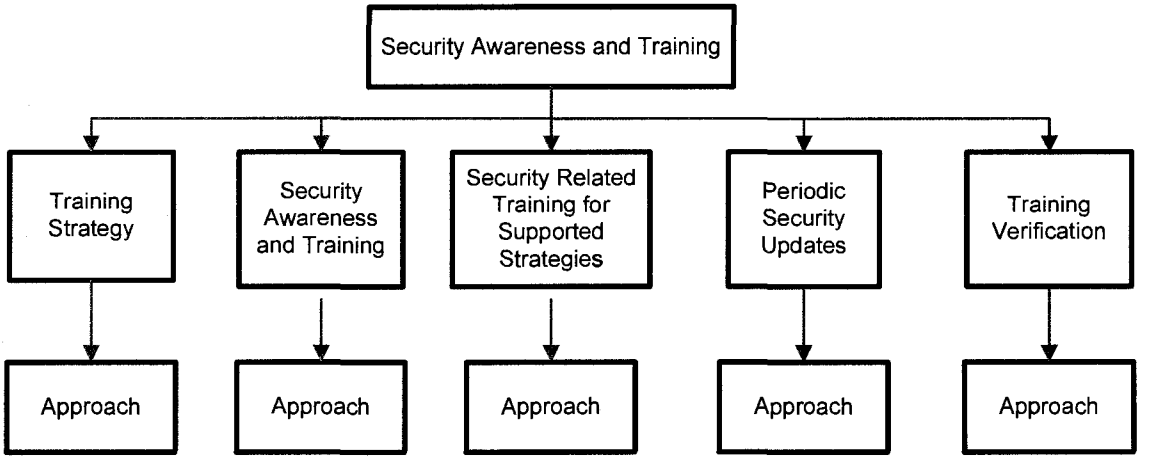

Figure 4.3-11: Example of a Security Practice

Each *strategic* security practice area has a unique set of characteristics. The protection strategy describes the processes used to perform activities in each security practice area, which is the target control strategy of the organization. The extent to which processes are formally defined is explored.

The status on the security practices survey indicates how well the analysis team believes its organization is performing in each area. An organization could be performing very well in an area, but have very informal processes. Likewise, an organization could have significant room for improvement despite having very formal policies and procedures. The organization also may be over controlling in some areas, and under controlling in the others. The gap analysis is conducted where each security practice area is assessed, taking into consideration the following factors, in a security practice.

- Responsibility: This characteristic depicts the responsible person for completing a set of specified tasks for the security practice area, to which accountability is assigned. This characteristic also defines whether accountability for each task rests with people in the organization, or with the third parties, or with a combination of people in the organization as well as third parties.

- Procedures: The *Procedures* are documented within description of the extent of which an operational security practice area is formally defined.

- Training: The *Training* characteristic defines the approach for building analysis team's skills and the participants' skills in a practice area.

- Verification: The *Verification* characteristic defines the degree to which each third party complies with the requirements for an operational security practice area.

For each security practice area, the respondent considers who is currently responsible for completing each task in this operational security practice area. If the responsibility resides with the people in the organization, a third party or a combination of people in the organization and one or more third parties.

2. Select Mitigation Approach: Mitigation approach is how an organization intends to address a risk. An organization has the following options for each risk: accept, mitigate, or defer which can be defined as follows:

- Accept – a decision made during risk analysis to take no action to address a risk and to accept the consequences should the risk occur. Risks that are accepted typically have a low impact on an organization.
- Mitigate – a decision made during risk analysis to address a risk by implementing activities designed to counter the underlying threat. Risks that are mitigated typically have a high impact on an organization.
- Defer – a situation where a risk is neither accepted nor mitigated. The impact on the organization due to a deferred risk is above a minimal threshold, but not so large as to be an immediate priority. Deferred risks are watched and re-evaluated at some point in the future.

The mitigation area is a security practice area that is designated to be improved in order to mitigate one or more of an organization's security risks. The decision to accept a risk, to mitigate it, or to defer the decision is based on a number of factors. Impact value is often the primary driver when making the decision. Likelihood is also used to determine which risks need to be mitigated first.

Unfortunately, there is no set decision-making process that applies in all circumstances. The information risk profile created for an organization is a decision support tool. It presents threats, impact values for multiple impact areas, likelihood values, and the statuses of the security practice areas, illustrating a picture of the risks affecting that critical asset. An analysis team uses the risk profile to support the mitigation decisions

that it makes. The approach to best suit the analysis team's preferences as well as the organization's accepted practices is selected, as there is no single approach for analyzing the information that is recorded throughout the evaluation.

All information recorded throughout the evaluation is reviewed and specific attention is paid to any recommendations that are made regarding potential mitigation activities. It must be ensured that the review of all recorded information during the evaluation is completed, before selecting mitigation approaches.

3. *Review risks to the critical assets*: In the work-session, the decision makers need to consider which risks need to be mitigated, accepted or deferred. Selecting too many areas will likely overwhelm the process of mitigation planning. Some risks will not be accepted nor mitigated, due to the potential impacts too low enough to accept, nor large enough to be designated as a current mitigation priority. These risks are deferred. Deferred risks are watched and re-evaluated at some point in the future. The relevant security practice areas are selected as mitigation areas. Any constraints in resources or funding are considered, when making the selections.

4. *Design Risk Mitigation Plans:* Risk mitigation plans are often linked to the organization's survivability. They are generally designed to reduce the risks could prevent an organization from achieving its mission by addressing the underlying threats. A mitigation activity can address threats in one or more of the following ways:

- Recognize threats as they occur;
- Resist threats to prevent them from occurring; and
- Recover from threats after they occur.

Risk mitigation plans comprise the following elements:

- *mitigation activity* – defines the activities to be implemented in a security practice area;
- *responsibility* – identifies who must be involved in implementing each activity; and
- *requirements* – any support that will be needed when implementing each mitigation activity.

Risk mitigation plans can trigger a change in the organization's protection strategy, while other activities do not create a major change, but only improve how the current protection strategy is implemented. It is identified if the mitigation activity causes a change in the organization's present protection strategy, which characteristics in the security practice area would be affected, and which factors is the change driven by.

The activities that will produce the protection strategy are identified and documented in the mitigation plan for the appropriate security practice area. For each of the action items, one must specify a description of the action, responsibility for completing the action, and a term or a date for completing the action.

Inputs of Phase 6:

- Prioritized Risk Portfolio of the organization;
- Countermeasures against risks.

Outputs of Phase 6:

- Gap Analysis;
- Security Protection Strategy;

- Mitigated Risks; and
- Deferred Risks.

This concludes our information risk assessment process. Periodic reviews are required in order to monitor and control the improvement in information security maturity of the organization. The control and monitoring phases are considered as part of risk management.

4.4 Conclusions

The proposed methodology provides improved usability by its phase approach, where each activity is mapped. These activities are also demonstrated in the next section through the case study to provide a better understanding to the user, decreasing the need for specialized training.

Phase 1 provides improved functionality and guidance, in consult with project management principles. The process is time and cost bounded providing decision making criteria for the management prior to committing to the process. Schedule, resource and budget planning helps to achieve improved scoping.

The methodology is process centric, compared to system focus of the existing methodologies. We start by identification of the critical business processes for the organization in Phase1. Based on the inputs and processing assets required for these processes, the critical information assets of the organization are defined. The dependencies of processes and their related information are taken into consideration with respect to the supply chain principle.

Phase 2 assesses the organization's information security maturity level, analyzing the present control structure from an audit perspective. The development of a security survey questionnaire that is specific to the organization improves the knowledge in security of the participants. The specialized training need is less, while an understanding of risk is promoted at every level within the organization that lead to more viable results.

In characterization of the threats in Phase 3, the potentiality of a threat and strength of the motive are considered as well as the past history.

Physical vulnerability analysis is provided displaying physical methods to access the critical information assets, as well as the electronic vulnerability assessment, in Phase 4.

Phase 5 introduces improved techniques by presentation of risk portfolio, deriving residual risks, based on the analysis of the inherent risks and the present controls. Impact types, severities and control scale are determined with respect to the organization's operating environment.

By employing change management principles, in Phase 6 more viable security strategies and risk mitigation plans are initiated and sustained.

The secondary findings of the methodology can be summarized as follows:

Communications planning, performance management and continuous improvement principles improve the management and the quality of the information risk assessment process and help to produce more viable results for the organization.

Results from a phase are validated through multiple team members by the analysis team prior to the start of a new phase, enabling control, accuracy and reliability of the collected data, helping to ensure quality.

Documented results support for internal verification as well as external third party audits and compliance to the regulatory bodies.

Quality assurance principles foster an environment of continuous improvement and performance management of the project, while the viable results are sustained through knowledge transfer, communications and change management principles.

Chapter 5: Case Study

5.1 Introduction

Based on the proposed methodology presented in Chapter 4, this section is dedicated to case study. The tools and methods that relate to each of the principles in developing the proposed methodology are embodied within the case study. Phases and activities described in the previous chapter are followed, step by step, adapted to the operating environment of the organization.

5.2 Case Study

From here on, we present our case study in information risk assessment, phase by phase, in accordance to the steps of the proposed methodology explained in Chapter 4. The case study is a virtual one, because the results of the information risk assessment exercise is highly confidential for an organization and shall be distributed with restriction and not be shared in public under any circumstances. In order to demonstrate how the phases of the methodology are implemented, we used samples of processes and their associated information assets, created sample threat scenarios, a sample risk profile, presented results of gap analysis and provided recommendations based on the findings from the information risk assessment.

The methodology is customized according to the requirements of a large organization, operating in the service industry leading to slight variations in steps, between the methodology and case study. This is a general practice as each organization's operating environment is unique.

5.2.1 Identify and Scope

In the first phase, we scope the information risk assessment, by understanding what is critical to the organization's information security well being. A planning session with upper management is first conducted. A brief explanation on the methodology is made explaining the scope and objectives. We obtain management's commitment to the project. Before they select the analysis team members for the project, we provide training, by a walkthrough of the process, through a schematic diagram. This gives them an understanding of our methodology and what an information risk assessment involves. We conduct Phase 1, based on the steps of the methodology and Phase 2 within a 3 hours period, with the management team.

We draft a project schedule plan showing the time and duration of activities for each phase.

Stage	Task Name	Start	Finish	Duration	Week Starting: Mar 31	Apr 7	Apr 14	Apr 21	Apr 28	Jun 9
1 Project Planning	Plan Project and Conduct Management Session	Mar 31	Mar 31	1 d						
2 Risk Assessment	Identify and Scope	Apr 1	Apr 24	18 d						
	- Conduct Work-shops	Apr 22	Apr 29	6 d						
	- Interview selected staff	Apr 22	Apr 29	6 d						
	Evaluate Security Practices	Apr 22	Apr 29	6 d						
	Characterize Threats	Apr 22	Apr 29	6 d						
	Identify Vulnerabilities	Apr 22	Apr 29	6 d						
	Identify and Analyze Risks	Apr 22	Apr 29	6 d						
	Develop Security Strategy and Mitigation Plans	Apr 22	Apr 29	6 d						
3 Report Findings	Final Write-Up	May 20	May 30	9 d						
	Feedback and Updates	Jun 2	Jun 13	10 d						

Figure 5.2 -1: Project Timeline

The project start date is set as the 31st of March within duration of six weeks, as shown on the project schedule, with the dates of completion for each phase. The project milestones, like conducting the project launch meeting, completion of security strategy and mitigation plans are noted on the project schedule. Resource plans are prepared, based on the project schedule; in our case study for an analysis team of five. The total project budget for the process is also estimated, according to the hourly rates of the staff. The cost, schedule and resource plan of the project are presented for management approval. At this point, we ask for commitment from management. The project plan is signed off. Once the budget is approved, we start with the information risk assessment process by identifying the business processes and assets.

From a review of the processes in the organization, the two critical processes are identified as "the execution of projects" and "bid preparation", in which the "Design Department" and "Project Department" are actively involved. In the example below,

participants from these departments determine the critical information assets. Each asset is provided with a description as to the purpose of its use, its owner, user group and the custodian.

Asset Name	*Application Description*	*Asset Owner*	*User Group*	*Asset Custodian*
Risk Watch	*Tool for Risk Analysis*	*Project Department Manager*	*Project Department*	*IT Department*
MS Project	*Software for Project Scheduling*			
Cost Software	*Cost Estimation software*			
AutoCAD	*Modeling application*	*Design Department Manager*	*Design Department*	
Auto Desk License	*Auto Cad License*			
Design Software	*Process engineering software*			

Table 5-1: Asset Identification

The critical assets are distinguished whether they are "inputs", "processing assets" or "outputs". Their impact severities are defined from "High" to "Low" for the following threat scenarios which all violate one or more security requirements of the asset.

- "access by unauthorized people";
- "modification without authorization"; and
- "loss and destruction" and "interruption".

Assets	*Magnitude of the Impact in case of the following outcomes*			
	Access by unauthorized people	*Modification without authorization*	*Loss or Destruction*	*Interruption*
Inputs				
Resume Bank (Purpose of use: in proposal responses to bid for projects)	*Medium*	*Low*	*High*	*High*
References – client references from previous projects (Purpose of use: in proposal)	*Medium*	*Low*	*High*	*High*

Table 5-2: High Level Impact Table for Inputs

Assets	*Magnitude of the Impact in case of*			
	Access by unauthorized people	*Modification without authorization*	*Loss or Destruction*	*Interruption*
Processing Assets				
Cost Estimation Software	*Medium*	*Low*	*High*	*High*
Design Calculations	*Low*	*Medium*	*High*	*High*
Design Drawings	*Low*	*Medium*	*High*	*High*
Outputs				
Technical Package – Response to Proposal	*High*	*High*	*High*	*High*
Pricing Package – Response to Proposal	*High*	*High*	*High*	*High*

Table 5-3: High Level Impact Table – for Processing Assets and Outputs

From the table above, we conclude that for the majority of asset availability is the most critical security requirement. This is due to the nature of the business in proposal preparation, where the team works against a tight deadline. It is unlikely to submit the proposal response on time, in case of asset and resource unavailability. The modification of the data can cause deviations in the technical package, as well as in the pricing package, such as errors in design and cost estimates. A security breach is access of unauthorized people to the "Resume Bank" leading to the disclosure of the asset, which has a negative impact on the competitive advantage of the company and may cause privacy issues, leading to legal consequences. Once the impact severity levels are defined for the organization, the information owners determine the severity of the impact for each threat scenario, in the next steps of the information risk assessment process.

Assets	*Employee roles (those who have a special skill or knowledge that is difficult to replace, yet critical for the organization)*	*List special skills or knowledge*
Design Drawings	*Design Department Chief*	*Specific designs developed for special customers – large accounts*
Cost Estimation Software / Pricing Package	*Cost Estimation Expert*	*Accuracy in project cost estimation and leverage of contingency, based on vast previous project experience*

Table 5-4: Resources and Skills

Regardless of their type and use, all assets including those systems under development are in scope of the assessment. This is a recommended practice in the system development life-cycle. The security requirements of organization's critical information assets are distinguished between confidentiality, integrity or availability of an asset. The following tables present the security requirements of the assets discussed earlier:

Input Assets	*Confidentiality*	*Integrity*	*Availability*
Resume Bank	*Secondary Security Requirement*	*Third Important Security Requirement*	*Primary Security Requirement*
References – client references from previous projects	*Secondary Security Requirement*	*Third Important Security Requirement*	*Primary Security Requirement*

Table 5-5: Security Requirements for Inputs

Processing Assets	*Confidentiality*	*Integrity*	*Availability*
Cost Estimation Software	*Secondary Security Requirement*	*Third Important Security Requirement*	*Primary Security Requirement*
Design Calculations	*Third Important Security Requirement*	*Secondary Security Requirement*	*Primary Security Requirement*
Design Drawings	*Third Important Security Requirement*	*Secondary Security Requirement*	*Primary Security Requirement*

Table 5-6: Security Requirements for Processing Assets

Output Assets	*Confidentiality*	*Integrity*	*Availability*
Technical Package – Response to Proposal	*All Security Requirements are equally important.*	*All Security Requirements are equally important*	*All Security Requirements are equally important*
Pricing Package – Response to Proposal	*All Security Requirements are equally important*	*All Security Requirements are equally important*	*All Security Requirements are equally important*

Table 5-7: Security Requirements for Outputs

5.2.2 Evaluate Security Practices

The identification of the critical information assets in the organization, performed in the first stage helps to scope the information risk assessment. We also want to understand the level of awareness in information security in the organization at this stage. In order to identify management knowledge and the operational level staff's knowledge, a good cross-section from each level is selected within the organization, for a workshop session facilitated by the information risk analysis team or simply a security survey is completed. The security practices survey is developed based on the best practices, standards, and structured methodologies, presented in Chapter 2. Best practices in information security

are updated on a periodic basis, with respect to the developments in the security practice area. The analysis team members are expected to prepare questions, by selecting the most appropriate security practices from the best practices that apply to the organization undergoing information risk assessment.

The responses to the survey questions are used to assess the security knowledge of the members in the organization. In the next steps of the risk assessment, these findings are used as basis to recommend actions to reach the desired state of security for the organization. In the example below, samples from survey results are shown on the first set of questions in strategic security practice: "Security Awareness". The participants demonstrate their knowledge and awareness in implementing the security practice in the organization. The percentages are cumulative from 14 participants from the Design Department, 12 participants in Project Department, 5 participants from Finance Department, and 7 participants from IT Department. Full set of survey questions can be customized from the methodologies, best practices and guidelines, modified according to the organization's requirements.

Security Practice Area Question	*Cumulative Results from Respondents*
Staff members understand their roles and responsibilities, regarding protection of assets. The roles and responsibilities are documented and verified.[9]	*37.5% - Yes; 37. 5 % - Yes, but not effective; 25% - No; 0% – Don't know*
There is expertise for all responsibilities of data custodian, within the organization, including their secure operation. This is documented and verified.[9]	*37.5% - Yes, 25.0% - Yes, but not effective, 12.5% - No, 25.0% – Don't know*

Table 5-8: Sample of Security Survey Results

According to the cumulative responses from the participants, we determine the status for each security practice area amongst the levels presented in the methodology.

Security Practice Area Question	*Status*
Staff members understand their security roles and responsibilities. This is documented and verified.	*Yellow – The organization is performing the security practices to some extent; there is room for improvement.*
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	*Yellow – The organization is performing the security practices to some extent; there is room for improvement.*

Table 5-9: Sample of Security Survey Results [6]

5.2.3 Characterize Threats

In this phase, the analysis team focuses on establishing the threat profile for each asset at risk. The threat and vulnerability analysis starts by consolidation of data collected on asset profiles. When consolidating data, it is important to represent the data as it was originally recorded. Information is grouped, conflicts are resolved, the information collected is validated with the respondents and the missing information is defined prior to characterize the threats.

Prior to seeking out threats from the participants, it is important to explain them the threat factors, so that they can define the threats to their information, by reflecting on these factors. Each threat comprises specific properties, as explained in Chapter 4. All of these properties may not be characteristics of one threat. Depending on the threat scenario, only a subset may be applicable. The first factor to form a threat is the asset. Once the asset which is at risk is identified, the threat is described, by the actor, his or her motive, and access method. The outcome, leading to an asset's disclosure, modification, destruction, loss or interruption is identified.

In the example, one of the critical assets of the Project Department; Resume Bank is taken into consideration, and analyzed against its pertaining threat scenarios. Human actors both inside the organization and outside the organization are considered to be a threat source. These actors can disturb the security of the asset, both by electronic access and by physical means. The motive of the actor can be assigned a value from "High" to "Low". High corresponds to "5" and the "Low" corresponds to "1". The same exercise is repeated for all selected critical assets to have the complete list of threats.

Department Name: Project Department *Asset Name: Resume Bank*				
Access Method *Actor* *Motive / Motive Strength*			*Outcome / Security Requirement Impacted*	*Threat Description*
People inside the organization via physical access, acting accidentally (3)			*Disclosure / Confidentiality*	*Insiders disclosing resumes to third parties without authorization.*
People inside the organization via physical access, acting accidentally (2)			*Modification / Integrity*	*Insiders acting accidentally: Typing errors impacts accuracy of resumes.*
People outside the organization via physical access, acting deliberately (2)			*Disclosure / Confidentiality*	*Outsiders acting intentionally to access Resume Database, without authorization.*
People outside the organization via electronic access, acting deliberately (2)			*Disclosure / Confidentiality*	*Outsiders acting intentionally to access Resume Database, provided to others by the third parties, without authorization.*
People outside the organization via electronic access, acting deliberately (2)			*Disclosure / Confidentiality*	*Contractors being provided with access Resume Database.*
Source	*Type*	*Severity*	*Outcome / Security Requirement*	*Threat Description*
Natural	*Fire*	*5*	*Loss / Destruction / Availability*	*Resume Database not being available for an undetermined time, as a result of fire.*
Natural	*Snow Storm*	*3*	*Interruption / Availability*	*Resume Database not being available due to snow storm, during proposal preparation.*
Utility	*Electricity*	*3*	*Interruption / Availability*	*Resume Database not being available due to an electricity interruption, during proposal preparation.*

Table 5-10: Threat Characterization

Based on the threat scenarios developed above, we review the incident history to understand if the listed threats have occurred and their frequency of occurrence.

Incident History	*Threat Descriptions*
Twice in the past 10 years	*Insiders disclosing resumes to third parties without authorization.*
Five times during the past year	*Insiders acting accidentally: Typing error, using the wrong version of the resumes in response to proposals.*
None	*Outsiders acting accidentally access Resume Database, without authorization.*
None	*Outsiders acting intentionally to access Resume Database, providing information to the third parties, without authorization.*
None	*Contractors being provided with access to Resume Database.*
None	*Resume Database not being available for an undetermined period of time, as a result of fire.*
Once in the past three years	*Resume Database not being available due to an electricity interruption, during proposal preparation.*

Table 5-11: Incident History

5.2.4 Identify Vulnerabilities

In this phase, the IT analysis team first determines network vulnerabilities for each critical asset identified. Following the network vulnerabilities, the physical threat and vulnerability assessment is conducted by assessing the current physical controls and areas of possible threat exposures.

First we analyze, the infrastructure dependencies of each critical asset, such as:

- servers in which the application and database reside;
- their associated networking components, such as routers, switches, and modems;
- their security components, like firewalls, desktop workstations, home computers of users, portable PC s, storage devices; and
- wireless components, such as mobile phones where the information is communicated and stored.

Topology or other types of network maps may be used to review where critical assets reside and how they are accessed. Qualified and trained IT staff in the organization makes the analysis. The results are discussed with the business participants. We use the same example, "Resume Database" that is used in the previous phase, to examine its systems of interest, intermediate access points, systems accessed to reach to "Resume Database", and data storage locations.

Systems of Interest	*File and Print Servers Resume Database resides on, Internal Networks, On-site workstations*
Intermediate Access Points	*Internal Networks, Company website, External Networks*
Systems Accessed	*On-site workstations, laptops, wireless devices, mobile phones, home computers, other external stations like client site computers*
Data Storage Locations	*Storage Devices, Back up tapes, alternative site*

Table 5-12: Dependencies of the Critical Asset

Upon review of the other critical assets and their dependencies, we conclude that "Resume Database" is dependent on the key systems and are shared by other critical assets. Then, we determine who is responsible for the selected components to manage the change required, to manage their security and how well each class of component is currently being protected. This is done by determining the extent security when configuring and maintaining each class of components. When the responsibilities are assigned to IT administrators, it should be noted that the ultimate responsibility resides with the IT Department Head.

Component Classes	*Responsibility*	*Very Much*	*Somewhat*	*Not at All*	*Don't Know*
Systems of Interest	*Network Administrator*	*X*			
Intermediate Access Points	*Telecommunications Agent*		*X*		
Systems Accessed	*Network Administrator*		*X*		
Data Storage Locations	*Network Administrator*		*X*		

Table 5-13: Review of Infrastructure

Vulnerability analysis is performed similar to the threat analysis. Vulnerabilities are classified into categories, as in the threat analysis. Categories of vulnerabilities could be similar to that of the security practices, established for the organization in Chapter 3. Additional vulnerability information can also be acquired upon an environmental analysis, a system analysis or a technical analysis. A technical evaluation for vulnerability analysis is run for the selected infrastructure components. If these tools are not owned by the organization, the service can be contracted. The initial summary of the results are produced by those who conduct the analysis and discussed with the other participants.

In the example below, part of the network vulnerabilities are displayed with their description into categories. The key components they impact technically are listed, with the critical assets that are impacted.

Risk Category	*Electronic Vulnerability Description*	*Key component Category*
Inadequate access control	*Users do not ask authorization from the right individual, when they are requesting access to the Resume Database. Some users ask access for themselves.*	*File and Print Server*
Inadequate access control	*Within the same department, all users have access to the Resume Database*	*File and Print Server*
Inadequate implementation of procedures	*Each department has different ways of delegating access to Resume Database, there is no single procedure followed.*	*File and Print Server*
Inadequate access control / Physical and environment security	*Information saved on local drives is easily accessible. Laptops are lost or stolen.*	*Workstations*
Archiving Process and Procedures	*Historic data in Resume Bank makes up 70% of the data on the file & print servers, taking up too much space.*	*File and Print Server*
Information Classification	*Resume Data is available in multiple locations and not specifically protected.*	*File and Print Server*

Table 5-14: Network Vulnerability Analysis

The results from the vulnerability analysis are analyzed within an organized workshop and summaries for each critical asset are built. The results are then discussed and the vulnerabilities that require to be fixed are determined.

Assess Physical Controls and Determine Physical Vulnerabilities: We have reviewed the control measures taken for physical security in the building, specifically in the computer room where the servers reside. We have identified and recorded the issues in the application of the controls, which may be potential vulnerabilities that can be exploited by the threats.

Risk Category	*Physical Vulnerability Description*	*Key component Category*
Inadequate access control to the Computer Room, Inadequate implementation of procedures	*Entrance to the computer room is controlled by access card, however there is accompanying personnel without the access card who enters to the Computer Room, on an add-hoc basis.*	*Servers – Key Components as dependents of critical assets*
Inadequate access control to Computer Room	*There is a camera for surveillance of entry to Computer room, yet there is no security staff assigned to watch it.*	*Servers – Key Components as dependents of critical assets*
Inadequate access control / Physical and environment security	*Door alarms are functional in case of access without authorization, although this alarm is mixed with the false alarm when the door is left open for an exceeding amount of time. No attention is paid even if the door alarm signals.*	*Hard copy documents that are critical information assets residing in the office, Laptops.*
Inadequate access control / Physical and environment security	*Unauthorized personnel can enter to the building. Laptops were lost and stolen.*	*Laptops*
Physical and environment security	*One of the UPS in the Computer Room is in service interruption, waiting for the technicians to be fixed.*	*Servers – Key Components as dependents of critical assets*
Physical and environment security	*A/C in the computer room has low capacity to supply adequately, as there are fluctuations in the temperature. Due to an unexpected capacity increase in the infrastructure and the number of servers, an A/C system upgrade is required.*	*Servers – Key Components as dependents of critical assets*
Inadequate access control	*There are visitors in the building without a visitor badge or another indication that they are visitors and are not always accompanied by authorized personnel.*	*Hard copy documents that are critical information assets residing in the office, laptops.*

Table 5-15: Physical Vulnerability Analysis

5.2.5 Analyze Risks

In this phase, we determine and analyze the risks to the organization's information security. Risks are classified into categories and a risk matrix is used to present the risk portfolio, based on a scale of likelihood versus the impact of the risks to determine the

magnitude of the risk. With this view, high risk areas can be seen easily with respect to the medium and low risk areas.

We first determine the likelihood and then the impact criteria for the organization. For each identified risk, two factors, its likelihood and impact are determined, in order to prioritize the information security risks. Likelihood rating of each risk is determined, based on to the following criteria established for the organization, by the participants and the analysis team.

Likelihood Rating				
Assessment	*Rating*	*Description*	*Indicators*	*Occurrence Probability*
Very Likely	*5*	*Almost Certain*	*Likely to occur in a monthly time period*	*Above %95*
Likely	*4*	*Probable*	*Likely to occur in a quarterly time period*	*50 - 95%*
Moderate	*3*	*Possible*	*Likely to occur in a one year time period*	*30 - 49%*
Unlikely	*2*	*Possible*	*Likely to occur in a five year time period*	*5 – 29%*
Rare	*1*	*Remote*	*Not likely to occur in a ten year time period*	*< 5%*

Table 5-16: Likelihood Rating

Upon determination of likelihood criteria, we focus on determining impact criteria for the organization. Then, statements of actual impact to the organization are defined for each threat outcome. The impact criteria defined for the organization must be uniform, throughout the information risk assessment. Thus, it is necessary to select the impact criteria either with the upper management or confirm it with them.

Once impact criteria are established, they are used to assess all risks identified throughout the information risk assessment. This provides consistency. The impact severities are determined by the participants. The impact types can be tangible or intangible. The types are financial, strategic, operational and marketing impacts that impact the goals of

the organization. The following impact criteria set is considered as the basis in determining impacts of threats to the organization's critical assets.

Quantitative Measure of Risk Impact (Financial)	
Level	*Units of measure: Dollars*
5. Catastrophic	*Loss to the organization exceeds $50m*
4. High	*Loss to the organization is between $20m and $50m*
3. Medium	*Loss to the organization is between $5m and $20m*
2. Low	*Loss to the organization is between $1m and 5m*
1. Immaterial	*Loss is less than $1m*

Table 5-17: Quantitative Measure of Financial Impact

Qualitative Measure of Risk Impact (Strategic)		
Level	*Units of measure: Strategic objectives met*	*Units of measure: Publicity*
5. Catastrophic	*An inability to deliver most strategic objectives*	*Government or other investigative business initiates a high-profile, in-depth investigation into business practices, accompanied with high criticism in the media*
4. High	*A major failing in the delivery of some strategic objectives*	*Sustained criticism over three or four months in the media*
3. Medium	*A failing in one or two strategic objectives*	*Government requests information, some national public or media criticism lasting a week*
2. Low	*An inability to deliver some department objective*	*A sideline in the local press*
1. Immaterial	*No impact on organizational strategic objectives*	*A low level of interest in a particular activity*

Table 5-18: Qualitative Measure of Strategic, Legal, Publicity Impacts

Qualitative Measure of Risk Impact (Marketing)		
Level	*Units of measure: Product delivery*	*Units of measure: Customer Service*
5. Catastrophic	*Inability to deliver key products for more than three months*	*Delay in delivery costs above 5 % of the total revenue*
4. High	*Inability to deliver key products for more than three weeks*	*Delay in delivery costs above 3 % of the total revenue*
3. Medium	*Inability to deliver key products more than three days*	*Delay in delivery costs 1 % of the total revenue*
2. Low	*Delivery of key products delayed for more than a day or less*	*Delay in delivery costs less than 1% of the total revenue*
1. Immaterial	*Minor issues with regard to relationships with suppliers*	*Delay in delivery causes less than 0.1% of the total revenue*

Table 5-19: Qualitative Measure of Impact to the Customer

Qualitative Measure of Risk Impact (Health and Safety & Production)		
Level	*Units of measure: Health, safety and environmental incidents*	*Units of measure: Production hours lost*
5. Catastrophic	*Multiple major reportable events or a single catastrophic event*	*Substantial loss of production capability – more than three days of production hours*
4. High	*Major reportable event*	*Significant loss of production – up to one day of production hours*
3. Medium	*Several reportable incidents*	*Effect between 5% and 20% of day's production hours*
2. Low	*One or two reportable incidents*	*Effect less than 5% of day's production hours*
1. Immaterial	*No reportable incidents*	*Minimal loss of production hours*

Table 5-20: Qualitative Measure of Health and Safety & Production Impacts

Once likelihood and impact criteria are set, we analyze the risks that impact critical assets identified. In the example below, risks pertaining to the top three critical assets of the

organization are listed. The information is collected in a work-session from the workshop participants responsible for project execution, as well as proposal preparation.

Asset 1	*Risks*
Proposal Information	*Acrobat files must be adjusted prior to distribution of final pricing and technical package in bid response. Security of acrobat files is not considered, staff is not educated on the security features of acrobat reader files. (PI 1)*
	Proposal preparations are done with minimum budget involve junior staff, which causes errors in various steps, including design calculation. (PI 2)
	During the proposal preparation stage, competitors try gaining access to the response information by their personal contacts. (PI 3)
	Proposal drafts are accessible to many staff members, during the preparation stage, which violates confidentiality. (PI 4)
	A significant number of staff from different departments is involved in preparation of proposals. (PI 5)

Table 5-21: Asset 1 versus Risks

Asset 2	*Risks*
Design Drawings	*The applications used daily, for design not being available in a timely manner. (DD 6)*
	Design drawings information is erased or lost. (DD 7)
	Archived designs are not available when required documentation must be created from scratch. (DD 8)
	Fire destroying hard copies of archived design drawings. (DD 9)
	Modification of drawings without authorization.(DD 10)
	Design inputs entered incorrectly or modified. (DD 11)
	Color codes on drawings being misinterpreted in acrobat reader copies.(DD 12)

Table 5-22: Asset 2 versus Risks

Asset 3	*Risks*
Project Information	*Employees, contractors leaving work premises with paper or electronic copies of project information. (PP 13)*
	Physical access to the main office not being adequately controlled. (PP 14)
	Procedures are present to protect access rights to project information, but they are not implemented and practices fully, although management assumes they are in practice. (PP 15)
	Project costs being disclosed to unauthorized parties, deliberately or accidentally. (PP 16)
	Archive project information being classified only at one location, which is vulnerable to physical threats. (PP 17)
	Information on project site not being available, timely when required. (PP 18)
	Confidential reports being disclosed to unauthorized third parties. (PP 19)

	Not being able to access project information during life cycle of a project, due to inadequate classification organization. (PP 20)
	Design errors impacting project execution (PP 21)
	Documents easily accessible desks of personnel, offices, cabinets not locked clean desk policy not practiced. (PP 22)
	Individuals accumulating a lot of unnecessary information, filling up the space in the project directories. (PP 23)
	Inadequate procedures for physical access control. (PP 24)
	Project information not being available, due to interruptions. (PP 25)
	Unauthorized parties entering to restricted areas. (PP 26)
	Temporary accesses to clients, partners, contractors not being controlled. (PP 27)
	Contracts not being accessible when required for legal purposes. (PP 28)
	Clients disclosing project confidential information to third parties. (PP 29)
	Project costs being modified, by unauthorized access. (PP 30)

Table 5-23: Asset 3 versus Risks

We then define the impact criteria into five levels, similar to the likelihood grading, and we develop a risk matrix for the organization. We determine inherent risks by multiplying the likelihood with impact rating. Then, we determine if there are any established controls to minimize the risk. The control grading scale is as follows, according to effectiveness of the control.

Controls Rating		
Assessment	*Rating*	*Description*
Very effective	*5*	*Risk response is adequate to the threat*
Effective	*4*	*Risk response is appropriate for the foreseeable results of the threat*
Moderate	*3*	*Risk response is appropriate for the threat but gaps have been identified that could result in unwelcome surprises / outcomes*
Limited	*2*	*Risk response is inadequate and could readily lead to unwelcome surprises / outcomes under normal operating conditions*
None	*1*	*Risk response does not reduce inherent risk rating. Risk before the control and after the control is the same.*

Table 5-24: Controls Rating

The risks to the three assets are evaluated according to their likelihood and impact. Once the controls that are countermeasures are established, the risks are re-evaluated. These

are called inherent risks. The inherent risks are determined based on the level of impact and likelihood of the residual risk that remains upon implementation of the controls.

Asset Name	*Risk No*	*Impact*	*Likeli-hood*	*Risk*	*Control*	*Residual Impact*	*Residual Likelihood*	*Residual Risk*
Proposal Information	*1*	*5*	*5*	*25*	*1*	*5*	*5*	*25*
	2	*5*	*5*	*25*	*3*	*3*	*3*	*15*
	3	*5*	*5*	*25*	*1*	*5*	*5*	*25*
	4	*5*	*4*	*20*	*1*	*5*	*4*	*20*
	5	*4*	*5*	*20*	*2*	*4*	*5*	*20*
Design Information	*6*	*4*	*5*	*20*	*3*	*4*	*5*	*20*
	7	*4*	*4*	*16*	*1*	*4*	*4*	*16*
	8	*5*	*5*	*25*	*3*	*4*	*4*	*16*
	9	*5*	*4*	*20*	*2*	*5*	*3*	*15*
	10	*3*	*5*	*15*	*1*	*3*	*5*	*15*
	11	*3*	*5*	*15*	*1*	*3*	*5*	*15*
	12	*3*	*5*	*15*	*1*	*3*	*5*	*15*
Project Information	*13*	*3*	*5*	*15*	*2*	*3*	*5*	*15*
	14	*5*	*5*	*25*	*3*	*5*	*3*	*15*
	15	*3*	*3*	*9*	*1*	*3*	*3*	*9*
	16	*3*	*5*	*15*	*1*	*3*	*5*	*15*
	17	*3*	*5*	*15*	*1*	*3*	*5*	*15*
	18	*4*	*5*	*20*	*2*	*4*	*5*	*20*
	19	*4*	*5*	*20*	*3*	*4*	*5*	*20*
	20	*4*	*4*	*16*	*1*	*4*	*4*	*16*
	21	*5*	*5*	*25*	*3*	*4*	*4*	*16*
	22	*5*	*4*	*20*	*2*	*5*	*3*	*15*
	23	*3*	*5*	*15*	*1*	*3*	*5*	*15*
	24	*3*	*5*	*15*	*1*	*3*	*5*	*15*
	25	*3*	*5*	*15*	*1*	*3*	*5*	*15*
	26	*4*	*5*	*20*	*3*	*4*	*5*	*20*
	27	*4*	*4*	*16*	*1*	*4*	*4*	*16*
	28	*5*	*5*	*25*	*3*	*4*	*4*	*16*
	29	*5*	*4*	*20*	*2*	*5*	*3*	*15*
	30	*4*	*4*	*16*	*1*	*4*	*4*	*16*

Table 5-25: Risk Profile

Results are validated through discussion with management. The results may be different than the perception prior to conducting the risk assessment. It is required to improve the awareness of staff and management in security for the results to be accepted and the

action plan to be implemented. Change management and communication planning concepts are essential. In the management session, a graphical tool is used to understand the priorities of the above risks as a visual aid and a communication tool. The likelihood of a risk is recorded on the X and the impact on the Y axis. From their product, the risk is calculated. The high risk areas are shown in dark grey color, towards to the upper right hand of the graph. The colors change to lighter grey, as the risk levels decrease. The scale of five is used to measure and record the impact severity and likelihood of occurrence, based on the criteria defined in five levels previously.

According to their likelihood and impacts noted in the above table, the residual risks listed are shown on a graph. In the graph, the high risks are demonstrated towards the top right corner of the graph, whereas the low risk areas are demonstrated towards the bottom left corner. All risks have to be reviewed in the management session, as it is possible that a risk could be rated higher or lower than what it is supposed to be. For example, a low risk may have been misjudged and actually it can be a medium to high risk, where countermeasure is required, instead of its deferral.

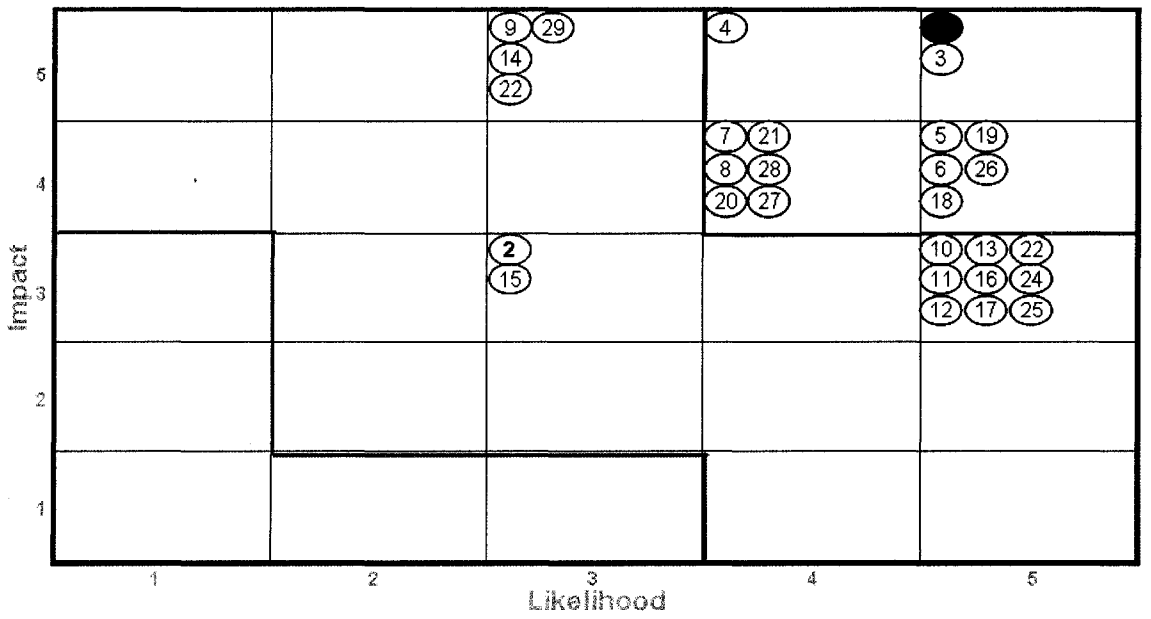

Figure 5.2-2: Risk Profile

5.3.6 Develop Security Strategy and Mitigation Plans

The protection strategy defines the strategies that an organization uses to enable, initiate, implement and maintain its internal security. It is a long-term commitment and is organization-wide. The security protection strategy must include strategic and operational controls. Prior to establishing the security strategy, the analysis team reviews risks from the graphical presentation and the results from the previous steps, specifically those pertaining to the security practices survey conducted, in Phase 2.

We conduct a gap analysis between the current security state and the target security state of the organization. The purpose of the gap analysis is to understand the magnitude of change to move from the current state of security within the organization to the desired future state; where the management wants to be at, within a given period of time in maturity of security. The magnitude of change (i.e. the gap between the current and future) drives the change management strategy for implementation stage of security practices and controls, in management of information security risks. The gap between

the two states requires a series of activity planning, projects to take the countermeasures necessary to bridge the gap and achieve the future state.

In our study, the gap analysis is performed by comparing the present state of security to the information security best practices and guidelines established in ISO 17799 [40] as the basis of our security strategy and mitigation planning development. According to ISO 17799, security practices could be summarized in the areas of:

- Security Policy;
- Organizational Security Practice;
- Asset Classification and Control;
- Personnel Security;
- Physical Environment Security;
- Communications and Operations Management;
- Access Control;
- Systems Development and Maintenance;
- Information Security Incidents;
- Business Continuity Management; and
- Compliance.

Security policy covers policy definition and structure, maintenance of policy documentation. Organizational security practice area covers management support, information security roles and responsibilities, confidentiality agreements, external parties. Asset classification and control covers areas in responsibility for assets, information classification. Personnel security covers prior to the employment stage,

during employment and upon termination or leave. Physical environmental security looks into secure areas and equipment security. Communications and operations management covers areas in operational procedures and responsibilities, third party service delivery management, protection against malicious and mobile code, systems planning and acceptance, back-up, network security management, media handling, exchange of information, e-commerce services, monitoring. Access control covers business requirements for access control, user access management, user responsibilities, network access control, operating system access control, application and information access control, mobile computing tele-working. System development and maintenance covers security in development and support processes, correct processing in applications, technical vulnerability management, security requirements of information systems, cryptographic controls, security of system files. Information security incident management covers areas in reporting information security events and weaknesses, management of information security incidents and improvements. Business continuity management covers areas in information security aspects of business continuity management and disaster recovery planning. Compliance includes compliance with legal requirements, compliance with security policies and standards, information systems audit considerations.

We provided recommendations on how to improve the present situation in security, based on the findings by giving priorities to the action items, categorized into short term actions; up to six months, mid term actions; between six months to a year, and long term security planning for the strategy; from one year to two years.

In the table below, only the "Security Policy" area is taken into consideration for review.

With respect to the nature of the security practice, accountability resides with the IT Department Manager. Security policy and procedures must be followed by all personnel in the organization. Training and awareness sessions must be organized for the staff to learn more about the practices and implement them regularly. Collaborative issues must also be taken into account, as the organization works with third parties, contractors and clients during projects. Third parties must adhere to the security policy. This must be verified, by assigned security staff from the organization.

With respect to the nature of the organization, the work environment necessitates working with clients and contractors during project life-cycles. In this case, the responsibility to adhere with the security policy is a combined responsibility that includes internal and external staff.

Upon completing the protection strategy, through gap analysis, the analysis team presents the proposed protection strategy to the senior managers in the organization. The senior management then reviews and revises the strategy. The risk mitigation plans are developed for the risks identified, on an asset basis in Phase 5. The protection strategy developed with respect to each practice area defines the long, medium, or short-term actions. Risk mitigation plans need to be consistent with the protection strategy. While defining the action items, the responsible person, the expected completion date and management responsibility are defined, as part of the risk management process.

No.	Security Practice Area	Vulnerability	Mitigation Strategy	Timeline
CLAUSE – SECURITY POLICY [40]				
Policy definition and structure:				
1.1	The Information Security policy is defined.	Currently only partial elements of the overall Information Security policy exists in the organization. Management is in the process of defining additional Information Security policies.	Create and implement the remaining components of the Information Security policy clearly establishing: • Application (the intended audience). • Authority and Process (roles and responsibilities). • Information (key internal and external contacts). • Brief process description. • Revision history. • Related policies.	Short Term
1.2	Management approves and supports the Information Security policy.			
1.3	The organization has established a formal process for developing Policies and Procedures.	Elements of the Information Security policy have been established through an informal process at the enterprise level. Each group within the organization is responsible for creation of its own policies.	Establish a Steering Committee that defines policy guidelines at the enterprise level and ensures all business units implement them consistently. Through the Steering Committee, design and implement a formal process of developing necessary policies and procedures within the organization. Engage the Steering Committee to regularly review existing policies and ensure a comprehensive coverage of the organization's needs.	Short Term

No.	Security Practice Area	Vulnerability	Mitigation Strategy	Timeline
Maintenance of policy documentation:				
1.4	*The policy has an identified owner.*	*Current policies in effect in the organization clearly establish an identified owner.*	*Through the identified owner, conduct regular revision of policies to ensure their accuracy and availability to the target audience.*	*Long Term*
1.5	*A regular policy review process takes place in the organization.*	*The organization does not currently have a formal policy review mechanism in place.*	*Through the policy committee, develop and implement a formalized policy review process which captures:* • *Feedback from all relevant parties.* • *Frequency of reviews (at least annual or after significant organizational/technical changes).* • *Management approval of changes to existing policies.* • *Policy revision history.*	*Mid Term*
1.6	*The organization has established formal performance metrics to monitor policy implementation.*	*Performance metrics are in the process of being redesigned as part of the current Management re-organization initiative taking place at the organization.*	*When designing policies, construct and implement performance metrics that encourage measurement of policy "success." For example, in checking how many employees successfully adhere to a clean desk policy implemented by Management, a performance metric that can be used is the number of compliant desks after random sweeps on a quarterly basis.* *Performance metrics should also provide feedback for policy improvement,*	*Mid Term*

No.	Security Practice Area	Vulnerability	Mitigation Strategy	Timeline
			effectiveness, and application of appropriate levels of internal controls.	

Table 5-26: Sample Gap Analysis & Recommendations

	Risk Number	Residual Risk	Mitigation Approach	Security Practice Area	Responsibility
Proposal Information	1	25	Mitigate	Organizational Security Practice	Marketing Lead
	2	15	Defer		
	3	25	Mitigate	Access Control	Department Head
	4	20	Mitigate	Access Control	Department Head
	5	20	Mitigate	Access Control	Department Head
Design Information	6	20	Mitigate	Business Continuity Management	Department Head
	7	16	Defer		
	8	16	Defer		
	9	15	Defer		
	10	15	Defer		
	11	15	Defer		
	12	15	Defer		
Project Information	13	15	Defer		
	14	15	Defer		
	15	9	Accept		
	16	15	Defer		
	17	15	Defer		
	18	20	Mitigate	Business Continuity Management	Department Head
	19	20	Mitigate	Access Control	Department Head
	20	16	Defer		
	21	16	Defer		
	22	15	Defer		
	23	15	Defer		
	24	15	Defer		
	25	15	Defer		
	26	20	Mitigate	Access Control	Department Head
	27	16	Defer		
	28	16	Defer		
	29	15	Defer		
	30	16	Defer		

Table 5-27 : Risk Mitigation Plans

As a result, the following summary of mitigation planning activities is required, with respect to the security practice areas in scope.

Security Practice Areas	*Mitigation Activity*
Security Policy	
Organizational Security Practice	12%
Asset Classification and Control	
Personnel Security	
Physical Environment Security	
Communications and Operations Management	
Access Control	63%
Systems Development and Maintenance	
Information Security Incidents	
Business Continuity Management	25%
Compliance	

Table 5-28: Risk Mitigation Plans

A graphical representation is provided, by a bar chart to show the percentage of effort required for each security practice area where mitigation plan is required for the countermeasures against information security risks.

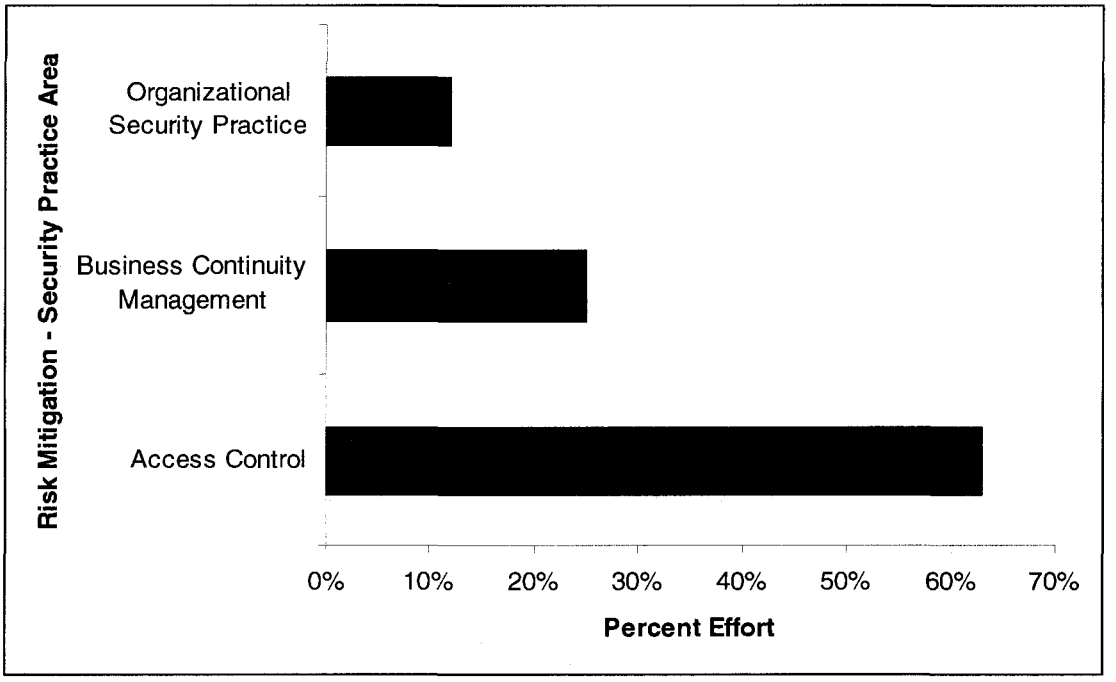

Figure 5.2-3: Graphical Representation of Mitigation Activities

5.3 Conclusions

In the case study presented, we demonstrated how an information risk assessment is conducted, following the principles and activities of the methodology proposed in Chapter 4. While all the present information risk assessment methodologies provide guidelines and worksheets, we have accompanied our methodology with a case study to validate the proposed methodology and to help the user better understand the process and ease the implementation efforts, which can be used for training purposes for the analysis team as well as for participants. Besides the demonstration of the activities in each phase, the principles emphasized in the methodology are used as building blocks in the case study. Information risk assessment sets the foundation of good information security management and is not a stand alone effort, therefore

organizational factors and its related principles are put in practice if a successful and effective information security program is desired.

Chapter 6: Conclusion

Information security is emerging as one of the most important challenges both in private and public sectors and in academic research. Individuals, corporations and organizations are exposed to various security incidents that lead to consequences ranging from small interruption to the business to shut down of the business for a long period of time. Availability, integrity and confidentiality of the critical information to the organization must be secured at all times.

Methodologies to manage information security risks are developing and ad-hoc information risk assessments are no longer adequate for the organizations. In this context, information risk assessment plays a major role by providing a structured methodology in detecting and effectively managing information security risks. Although, information risk assessment is considered a technical threat and vulnerability assessment in many organizations, it is extremely pertinent as a security tool now-a-days more than ever, that serves to organization's strategic, operational goals and regulatory compliance.

Accordingly, there is a need to understand what information risk assessment involves, how it is structured, which one is more suitable for an organization and how it can be customized according to the organization's need undertaking the assessment so that it can be implemented effectively. A methodology incorporates dedicated processes, methodologies and techniques to assess information risks to the organization. Such a framework will help the organization and the analysis team who undertakes the task of conducting the information risk assessment.

The contribution to this thesis is relative to the information risk assessment methodologies. In this respect, this thesis presents a detailed study of the state of the art processes. It also focuses on a comparative study of the existing information risk assessment methodologies. With a deep understanding of the potentials, and pitfalls in implementation, a proposal is provided for a new methodology that may leverage the major features of existing methodologies and may fix their identified shortcomings. In addition, the information risk assessment process provides new features which can be summarized as follows in principles:

- Iterativeness and Validation;
- Computer Support;
- Documentation;
- Quality Assurance;
- Change Management;
- Communications Planning;
- Supply Chain Management;

- Knowledge Transfer; and
- Performance Management and Continuous Improvement.

According to these principles, following phases which propose a set of activities are created to guide the user in implementation of the methodology:

- Identify and Scope;
- Evaluate Security Practices;
- Characterize Threats;
- Identify Vulnerabilities;
- Analyze Risks; and
- Develop Security Strategy and Mitigation Plans.

The implementation of the proposed methodology is demonstrated in a case study with customization according to the organization's needs, as part of a basic requirement in an implementation of a risk assessment. This exercise follows the steps developed in the proposed methodology with practical insights and useful abstractions that may help those undertaking information risk assessment, its research, development and organizational implementation.

As future work, multiple case studies can be conducted in the same industry. This serves as common knowledge base for a certain industry and helps to define the typical types of threats, historical data on threats, common risks for that industry and effective security strategies and countermeasures that are applied in that industry.

Bibliography

[1] C. J. Alberts, A. J. Dorofee, "Octave Method Implementation Guide: Volume 1: Introduction", Carnegie Mellon Software Engineering Institute, version 2.0, June 2001.

[2] C. J. Alberts, A. J. Dorofee, "Octave Method Implementation Guide: Volume 3: Process 1- Identify Senior Management Knowledge", Carnegie Mellon Software Engineering Institute, version 2.0., June 2001.

[3] C. J. Alberts, A. J. Dorofee, "Octave Method Implementation Guide: Volume 4: Process 2- Identify Operational Area Management Knowledge", Carnegie Mellon Software Engineering Institute, version 2.0, June 2001.

[4] C. J. Alberts, A. J. Dorofee, "Octave Method Implementation Guide: Volume 5: Process 3- Identify Staff Knowledge", Carnegie Mellon Software Engineering Institute, version 2.0, June 2001.

[5] C. J. Alberts, A. J. Dorofee, "Octave Method Implementation Guide: Volume 6: Process 4- Create Threat Profile", Carnegie Mellon Software Engineering Institute, version 2.0, June 2001.

[6] C. J. Alberts, A. J. Dorofee, "Octave Method Implementation Guide: Volume 9: Process 7-Conduct Risk Analysis", Carnegie Mellon Software Engineering Institute, version 2.0, June 2001.

[7] C. J. Alberts, A. J. Dorofee, "Octave Method Implementation Guide: Volume 12: Asset Profile Workbook", Carnegie Mellon Software Engineering Institute, version 2.0, June 2001.

[8] C. J. Alberts, A. J. Dorofee, "Octave Method Implementation Guide: Volume 16 Appendix B – Octave Data Flow", Carnegie Mellon Software Engineering Institute, version 2.0, June 2001.

[9] C. J. Alberts, A. J. Dorofee, "Managing Information Security Risks, The Octave Approach", SEI Series, CERT (Computer Emergency Response Team), 2003.

[10] C. Anderson, K. Barker, Y. Haimes, " Assessing and Prioritizing Critical Assets for the United States Army with a Modified RFRM Methodology", in Journal of Homeland Security and Emergency Management, volume5, issue 1, 2008.

[11] AS/NZ 4360, Australia / New Zealand Standard for Risk Management: Standards Australia / Standards New Zealand, 2004.

[12] Austrian Federal Chancellery, "Austrian IT Security Handbook", 2004.

[13] Bank for International Settlements, "Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework", 2005.

[14] Barnoff, Harrington, Niehaus, "Risk Assessment", 1st Edition, 2005.

[15] D. Benredjem, Concordia University, The Department of Electronic and Computer Engineering, "Contributions to Forensics: Processes and Analysis", p. 5, pp. 58-63, 2007.

[16] F den Braber, I Hogganvik, M S Lund, K Stolen and F Vraalsen, "Model-based security analysis in seven steps – a guided tour to the CORAS method", BT Journal, Vol 25 No 1, 2007.

[17] W.G. Bornman; L. Labuschagne. "A Comparative Framework for Evaluating Information Security Risk Management Methods". RAU Standard Bank Academy for Information Technology, Rand Afrikaans University, 2004.

[18] P. Bowen, J. Hash, M. Wilson, "NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems", National Institute of Standards and Technology, December 2007.

[19] CERT Institute and US Secret Service, "E-Crime 2005 Survey", 2005.

[20] Sunil Chopra, Peter Meindl, "Supply Chain Management, Strategy, Planning & Operation", Third Edition, pp. 483-495, 2007.

[21] COBIT, "Control Objectives for Information and Related Technology", IT Governance Institute, 1992.

[22] CLUSIF, "Mehari V3- Guide de l'Analysis des Risques", 2004.

[23] DCSSI Advisory Office, "Best Practices for ISS Risk Management, Using Results of EBIOS Method to Study an Existing System", 2004.

[24] DCSSI Advisory Office, "EBIOS – Section 1: Introduction", 2004.

[25] DCSSI Advisory Office, "EBIOS – Section 2: Approach", 2004.

[26] DCSSI Advisory Office, "EBIOS – Section 3: Techniques", 2004.

[27] ENISA: European Network and Information Security Agency ad hoc Working Group on Risk Assessment and Risk Management. "Inventory of Risk Assessment and Risk Management Methodologies", 2006.

[28] Evans and Lindsay, "An Introduction to Six Sigma and Process Improvement", 2005.

[29] Federal Office for Information Security, Germany, "IT-Grundschutz Catalogues", 2005.

[30] Insight Consulting, "Managing Risk in Your Organization, Achieving True Corporate Governance through the Management of Risk", 2005.

[31] Information Security Forum. "SARA: Simple to Apply Risk Analysis for Information Systems", version 1.0. Reprint, May 1993.

[32] Information Security Forum, "SPRINT: Risk Analysis for Information Systems User Guide" version 1.0, January 1997.

[33] ISF: Information Security Forum, "The Standard of Good Practice for Information Security", January 2005.

[34] ISF: Information Security Forum. "IRAM: Information Risk Analysis Methodologies Project Control Selection", January 2006.

[35] ISF: Information Security Forum. "IRAM: Information Risk Analysis Methodologies Project. Threat and Vulnerability Assessment", June 2005.

[36] ISF: Information Security Forum. "The Revised FIRM Information Risk Scorecard", August 2005.

[37] ISF: Information Security Forum. "IRAM: Information Risk Analysis Methodologies project. Understanding and Using the ISF's information risk management tools", October 2003.

[38] Information Security Forum, "Information Security Status Survey", 2003.

[39] Insight Consulting, "CRAMM v5.1 Security ToolKit", 2003.

[40] ISO IEC/17799: 2005, "Code of Practice for Information Security Management", 2005.

[41] N. Kumar, "The Power of Trust in Manufacturer- Retailer Relationships", Harvard Business Review, pp. 92-106, November - December 1996.

[42] Microsoft Solutions for Security and Security Center of Excellence, "SRMG Tool 1 Data Gathering", 2004.

[43] Microsoft Solutions for Security and Security Center of Excellence, "SRMG Tool 2 Summary Risk Level", 2004.

[44] Microsoft Solutions for Security and Security Center of Excellence. "The Security Risk Management Guide" Version 1.1, 2004.

[45] PMBOK, Project Management Institute, 2005.

[46] P. E. Tarlow, PhD, "Event Risk Management and Safety", The Wiley Event Management Series, 2002, p.122.

[47] G. Stoneburner, A. Gogueni, A. Ferignan, "Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30", 2002.

[48] K. Stolen, "Security Analysis: An Introduction to CORAS", Sintef & University of Oslo, 2007.

[49] K. Stolen, "Security Analysis: CORAS in Seven Steps", Sintef & University of Oslo, 2007.

[50] G. Stoneburner, A. Goguen, A. Feringa, "NIST Special Publication 800-30: The Security Self-Assessment Guide for Information Technology Systems", National Institute of Standards and Technology, July 2002.

[51] Strohl, "BIA User Guide", 2004.

[52] Strohl, "LDRSP User Guide", 2004.

[53] UK Financial Reporting Council, Internal Control, "Revised Guidance for Directors on the Combined Code", November 2005.

[54] US 107th Congress, Public Law 107-204, "The Sarbanes-Oxley Act of 2002 - Public Company Accounting Reform and Investor Protection Act of 2002", Sections 301, 302, 801, 802, 803, 804, 805, 2002

[55] S. Vidalis. "A Critical Discussion of Risk and Threat Analysis Methods and Methodologies", School of Computing and Technical Report CS-04-03. School of Computing, University of Glamorgan, 2004

[56] C. Woody, J. Coleman, M. Fancher, C. Myers, L. Young "Applying Octave: Practitioners Report, Network Systems Survivability" CMU/SEI-2006-TN-010, Carnegie Mellon University, Software Engineering Institute, May 2006

[57] M. N. Yusuff. "Contemporary Approaches to Project Risk Management: Assessment & Recommendations"