ISRAM Method Comparison

Comparative framework study for risk assessment methods

Mahmoud Berrady

MASTER THESIS(60 CREDITS) - SPRING 2021

The Faculty of Mathematics and Natural Sciences
Departement of Inoformatics
University of Oslo

Acknowledgement

Working on this Master project was different due to the current covid situation. This new predicament made us adapt to a new lifestyle and appreciate what we had before and took for granted. However, finishing this project in these conditions made the results more rewarding and worth the effort. I want to take this opportunity to thank UIO for welcoming me and my family for all the support they've been sending me all the way from Morocco. I want to thank my supervisor Audun Jøsang for his guidance and support, and of course my fellow students for their help and company.

Abstract

ISRM plays an important part in the information security field, it structures the concept of security in an organization and allows it to have an overview of its security posture. It also reveals its weaknesses and provides a basis to fix it in a bearable way. Risk assessment being the significant part of it, makes choosing a specific methodology a hard task, especially with the relatively large number of existing models for risk assessment. For an organization to choose a method for the process, the organization undertake a study, taking into consideration the organization's objectives and the method's nature. This study aims to shed a light on the topic of risk assessment, by comparing the four methodologies, CORAS, OCTAVE, ISRAM and FRAP based on specific criteria. These criteria would usually be part of a study to assess risk assessment models. A brief description about ISRM is given highlighting some of its challenges and information security challenges in general. A thorough description is given also to each of the models supported by some existing comparing work done on other methodologies. Each of these criteria was applied on each of the methods, and the results were used for the comparison and the final conclusion.

Table of Contents

List of Figures

1 Introduction

1.1 Motivation

The reason for this paper is to contribute to the information security field in general and information security risk management in particular. Information security has gained a lot of attention lately, because of the new technology challenges and the increasing number of cyber attacks, but most likely because of the new regulations, such as GDPR in Europe. The fines related to the security breaches, and unauthorized information disclosure is so significant that it made the board of management of any organization aware of the necessity of security and made risk management a suitable solution for it. Risk management in general and risk assessment in particular is the bridge that links all the security theories and principles with the real world scenarios. Risk assessment process allows you to put all the security skills you have to the test, while considering real threats on real assets in real scenarios. The research in this topic will allow me to study a number of risk assessment methodologies, and be familiar with the process of identifying key elements in information security it will also introduce me the discipline that orchestrate security in the corporate world, and to have a real look on how security is being applied in the real world rather than just in hypothetical environment.

1.2 The topic of this study

The topic of this study Information security Risk management is the backbone of security in an organization. keeping track of the status of security in a system or an organization can not be done randomly or in unplanned matters. Security is much more than just a firewall or an antivirus installed in a machine, security includes software, hardware, human factor, policies, regulations, compliances, etc..., it is linked to every aspect of the organization. Information security risk management is the discipline that regulates and structures the relation between the organization and security risks. Starting from establishing context all the way to accepting or rejecting a risk.

Risk assessment is part of risk management and it is considered to be the most important and most time consuming element, the reason that made a lot of third party organizations and private researchers to create methods to conduct risk assessment. Each of the methods is unique and was created to fulfill specific needs. The absence of a standardized method that can be safely used by all organizations or a certified comparing framework makes it a hard task to choose one. In order for an organization to decide on a method for conducting risk assessment, a study is required that takes in consideration a lot of aspects from the organization side and the method side. This process, if done in a good manner, can take a lot of time and consume a lot of resources.

The idea behind this thesis paper is to study a number of risk assessment methods that are available in the market, these methods have different structure, different approaches and different characteristics, some are considered big projects, and some are from independent researchers and finally try to compare them using a number of criteria that an organization would rely on to decide on the appropriate method.

1.2.1 The research questions of this study

- what are the purposes risk management /risk assessment?
- What criteria are important for an organization to use in choosing between methods?
- What is the difference between these methods ?
- What method is convenient to what type of organization?
- Why methods are different ?

1.3 Information

The Evolution of technology that the world has witnessed in the last thirty years is astonishing. Everyday we hear about new inventions and new technologies that make our life a lot easier, and a lot of the tasks that seemed in the past impossible or hard to do, are now possible or a button away from executing. All the technology and digitalisation revolve around a very important component, which is information. Information in the digital world is considered a currency. It has a value and it's value depends on its sensitivity and availability. Like anything with a value, information needs protection, this is where the term information security comes to mind. Information can be found everywhere and has different shapes and forms, however, the damage related to information is more serious when we discuss systems and organizations. The basic definition of information security is the practice of protecting the confidentiality, integrity and availability of the information. When it comes to complex IT systems and large IT organizations, this practice can be overwhelming. Best practice would be not to just stop an attack while it is happening but more of customising the IT system based on its environment to be resistant to these threats and to reduce the potential damage to the company. Doing so requires knowledge of the potential threats and the impacts of the different attacks on the business. That is precisely the focus of Information Security Risk Management (ISRM).

2 Background

2.1 Information security risk management

ISRM is the act of identifying, assessing and treating risks within an organization. While the risk can vary depending on the scope of assets, when it comes to IT systems, the risk we focus on, is about confidentiality, integrity and availability of the organization's information assets. The main goal of the risk management process is to identify potential threats and attacks that can endanger the IT system, and the process of identifying, reviewing, treating and monitoring risks to achieve an acceptable level of risk. Risk management is not new or exclusive to the IT industry. In fact, risk management is extensively used e.g. in finance and economics. In these sectors, there are well established and effective risk management models. It is also interesting to note that information security risk management is significantly different from financial risk management, whether in its nature, approach or purpose.

2.2 Risk management challenges

Siponen claims that traditional information security Risk Management methods disregard the human role within security, meaning that the ISRM method focuses on the technical part rather than the human factor (users of the system) which makes it hard to identify and treat the threats that are based on human errors and performance [40].

Elkelhart claims that the absence of adequate terminology used to define the different elements used in ISRM leads to confusion between the experts and the staff of the organization. The context of information security is very broad, with different elements and stakeholders. This can cause confusion in the interpretation of terms whether used by the users of the system or the experts applying ISRM and in the communication between them [13].

The organization must have a unified terminology when it comes to the terms used within the concept of ISRM, especially the risk scale. Different ISRM methods can be used within the same organization,(e.g. by different departments) depending on the nature of the organization, but the risk scale should preferably be unified throughout the whole organization.

Most of the information and the research about the ISRM is based on opinion or experience, not on well documented statistical qualitative studies. This can explain the lack of empirical research and valid data in ISRM. The lack of published studies is maybe due to the sensitivity of the information, meaning that the data that will be processed and published is critical to the organization. Simply the act of disclosing such data can be a threat itself.

Blakley and McDermott claim that the lack of validation and testing, i.e the absence of independent assessment of IS controls, makes it difficult to know the effectiveness of the controls. In addition, tests made by the vendors are rarely published. Most practitioners of ISRM tend to have a biased scope when applying ISRM disciplines, focusing more on applications, malware and hacking, and not including other elements, such as human error. After all, the human factor is the first line of defence [12].

Harris and Maymi also point out that many practitioners do not fully understand the risk management process and often are unable to estimate risks and apply ISRM as part of the business model of the organization. The confusion around information security risk management leads practitioners to miss important parts and the purpose of information security risk management [15].

Many practitioners think that risk management is risk identification, and often ignore important parts such as quantification and valuation of risk. They also consider security as the product rather than a process that should be followed by multiple steps that need to be implemented in order to achieve the objective. In order to get the most value out of the risk management process, it must be done correctly. Unless ISRM is being applied respectfully and based on a specific methodology, ISRM can have negative effects on the organization, for example it can give a false impression of having security risks under control, or consuming the company's resources without any added value.

2.3 Existing information security challenges

2.3.1 Mixing the professional life and personal life

As part of the daily routine, people typically interact with personal contacts and applications during work, whether it is to check personal emails on the company's machine or to use the company email for personal purposes. In addition people might use company-issued machines such as laptops or phones for games or illegal downloads . All these scenarios can be a security hazard to the company and the individual staff members.

2.3.2 Inconsistent enforcement of policies

When it comes to security policy in the organization, it is necessary to make the policy known and available for everyone. It must be updated, as the IT environment changes, whether it is the IT system, the components of the system, the assets of the organization or the users of the system and their roles. The documentation and the security policy must be up-to-date with any changes of this nature.

2.3.3 The IT department does not own and control all devices

In the case where the users of the system use their personal devices to store customer's data such as in sales. The legal aspect of the use of data, how it is stored and the access to it can be complicated, which require legal assessment and must be included in the risk assessment model.

2.3.4 Defining the exact perimeter of the network

It can be difficult to determine the precise perimeter of the organization's network. There can be multiple locations and multiple cloud solutions which create a network of networks for a single organisation, especially with options like remote

access for employees with VPNs, third party hosting services, cloud applications, extranets etc. This makes it hard to draw the line and say, this is where the network starts, and this where it ends.

2.3.5 The evolution of the attacks

In the past, attacks were more obvious and had a more immediate impact. However with time the objectives of the attackers have changed. For example, now we can see that the attacker's goal is to stay undetected and just remain in the system and exploit it as much as possible for a period of time, e.g for stealing data without being noticed or for using computing power after having installed rootkits and back-doors.

2.3.6 Changing attack scenarios

The different security threats that the IT system is confronted with are often similar, however the attack techniques the attacker will use to execute the threats change and evolve with time. Hence, for a risk management expert, it is important to stay updated and aware of the new technologies, the vulnerabilities and the novelties in the information security field. Nevertheless, engaging in such activities can be time consuming and drain a lot of a company's resources. Most of the new methods of attacks are just old ones wrapped in new lines of code but the algorithm is still the same, trying to exploit the same vulnerabilities and tweaked in a way that it may seem as a new exploit. The point here is that it is necessary to filter out the noise when it comes to pursuing all the attempted attacks and only focus on the ones that are actually new to the risk management model and can be a real threat to the system.

2.4 Benefits of risk management

The structure of an organization and the relationship between the different elements whether internally and externally is very complicated, and keeping track of everything that's going on can be an overwhelming process. In order to keep an organization secure and capable of maintaining operation in different situations, recurrent tasks should be conducted. And doing that in a random or in a non persistent way will lead to overlooking multiple scenarios and events that can have a very serious impact on the organization [45].

ISRM is a structured discipline, it provides an organized approach to not just deal with risks but also how to approach the different aspects of security. When an organization conducts Risk management, it's not just to identify risks and mitigate them, the process includes assets, threats, vulnerabilities, security controls, costs, losses, policies, mitigation plans ,recovery plans, and much more. By the end of the process, the rapport that is been generated or the results that been documented, allow the stakeholders to have database of information about the status of the organization, how the personnel perceive security, and internal/external policies, how information is being handled within, and much more information that wouldn't surface without this process.

Risk management gives the organization the opportunity to acknowledge the threat in its environment, to identify the risks and manage them. Information security is an investment that not all management is ready to make, especially when it's a profit driven mentality. it is a primitive solution, meaning that in case of an incident, it's already too late.

Information security Risk management gives the organization a chance to identify it's potential risks and implement the appropriate security controls that would guarantee the survival of the system in case of an incident.Security beaches can be very costly, they can even lead to bankruptcy, and the fines alone are a reason to consider security in every action.

3 Research method

The topic of this research paper is risk assessment, which is a part of the risk management process. Risk assessment is considered to be the step of risk management that requires the most effort and resources. Risk assessment combines three steps, risk identification, risk estimation and risk evaluation. Since this process takes a big share of time from the overall process and can be a bit confusing in terms of organization and expected outputs, many experts have proposed methodologies that facilitate this task and make it more manageable and worth the effort. For an organization to decide which method to apply for risk assessment, a study takes place to choose which one more suitable for the project, and this study takes a lot of aspects in consideration, for example, how big is the organization, how big is the scope, which part of the system the risk management process will apply to or is it the whole system, who will contribute in the tasks, what set of skills will be required to conduct the assessment, etc. This study focuses on proposing a framework that would minimize this task for the organization, and be a tool that can be used to choose the appropriate method suitable for the use case based on specific criteria. Many methods are being used in the market, each method comes with documentation which is used as a manual, this manual describes the method and its characteristics and proposes a set of steps to follow, some of them requires external expertise while other can be conducted by the organization's personnel, some take more time than others and thus the output also differs from one method to another. To be able to understand the methods and compare their characteristics, a literature study was conducted on the different the documentations they provide. The study focuses on the following methodologies: CORAS, OCTAVE, FRAP and ISRAM.

3.1 CORAS

In January 2001 the CORAS project was launched and in September 2003 the first version of the framework result saw the light. CORAS has the purpose of integrating security into system development and works on the concept of a framework that simplifies the risk management process, the CORAS framework includes three main classes, an experience library from previous projects, the methodology used in risk assessment and the terminology used in the project .

CORAS is a method for conducting risk analysis, the framework consists of : Risk analysis methodology: a step-by-step description of the security analysis process, with a guideline for creating the CORAS diagrams. Risk modeling language: includes both the graphical syntax of the CORAS diagrams and textual syntax and semantics. CORAS tool (to simplify the documentation,maintenance and reporting of the analysis process).

The CORAS method has a structured and systematic process. It is asset driven, meaning that the assets to be considered and protected are identified in the very early phases of the process, and all the following tasks such as risk identification and risk treatment are bound by these assets, to ensure that the focus of the analysis is always on the same area that the risk analysis is trying to protect. The method is also defensive meaning that the risk analysis is focusing on protecting existing assets rather than balancing potential gain against risk of investment loss like in the case of gambling or stock trading.

The CORAS method is also model driven using the UML language in terms of using graphical models throughout the whole process of the risk analysis and since some of the steps in the CORAS methodology use the result from the previous steps, the UML presentation is also used to support the various analysis tasks and also used for result documentation [1].

The basic CORAS method uses five diagrams throughout the eight-step process, namely asset diagrams, threat diagrams, risk diagrams, treatment diagrams, and treatment overview diagrams. In addition to these five basic diagrams, the CORAS method also provides additional modeling and analysis support provided by three extensions, namely high-level CORAS, dependent CORAS and legal CORAS [41].

- High- level CORAS is for hierarchical modeling at different levels of abstraction, and is a means for providing a comprehensible overview of large risk models.

- Dependent CORAS is designed to support the explicit documentation of analysis assumptions and analysis dependencies, and to support modular reasoning.

- Legal CORAS supports the identification and documentation of legal aspects that may affect risks, as well as the level of impact of legal aspects on risk.

The different diagrams used in the basic CORAS are consistent of the following concepts, which are part of the terminology that all the actors that are going to be part of the process must agree on in order to conduct risk analysis in a correct way and the results to be coherent:

- **Asset**: Something to which a party assigns value and hence for which the party requires protection.

- **Consequence**: The impact of an unwanted incident on an asset in terms of harm or reduced asset value.

- **Likelihood**: The frequency or probability of something to occur

- **Party**: An organization, company, person, group or other body on whose behalf a risk analysis is conducted.

- **Risk**: The likelihood of an unwanted incident and its consequence for a specific asset

- **Risk level**: The level or value of a risk as derived from its likelihood and consequence

- **Threat**: A potential cause of an unwanted incident.

- **Treatment**: An appropriate measure to reduce risk level.

- **Unwanted incident**: An event that harms or reduces the value of an asset.

- **vulnerability**: A weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset.

Since most of the organizations based their architecture and internal policies on international standards or follow specific techniques, the CORAS method is also based on international standards so that it would be compatible with different environments and easy to implement. The following standards were valid in 2001, but they have been replaced or withdrawn For example in risk management, the CORAS method takes into consideration the Australian/New Zealand Standard for Risk Management, AS/NZS 4360:2004 which has been replaced by ISO/IEC 27005 and the ISO/IEC 17799 which also has been replaced by ISO/IEC 27002 Code of practice for Information Security Management. The ISO/IEC 13335 Guidelines for the management of IT-Security which has been withdrawn.

In terms of system documentation, the CORAS method presents them in the form of the Reference Model for Open Distributed Processing. For security analysis techniques the CORAS method is based on the structured brainstorming technique HazOp, fault tree analysis (FTA) and the failure mode and effects analysis (FMEA) [14].

As mentioned earlier, the CORAS project consists of three areas, the CORAS terminology, the CORAS methodology and the CORAS library plus the integrated tool. But in this paper we will be interested in the methodology in particular. The CORAS methodology revolves around seven steps conducted by different agents from the subject organization, below is a brief description of each step with the anticipated output.

3.1.1 Step 1: Preparations for the Analysis

The first step of the process is the initial preparation for the risk assessment. The goal behind this step is to get an idea about the target and what would be the size of the analysis, maybe do some research on the analyst's part about the nature of the client company and its environment [19].

3.1.2 Step 2: Customer Presentation of the Target

the second step is more of an introductory meeting between the company representatives and the analysts that will carry the long process of the assessment, with the main goal to determine the target and the size of this analysis, So that the analysts team can do the necessary preparations based on the client's presentation and discussion such as gathering information for the actual analysis tasks [20].

3.1.3 Step 3: Refining the Target Description Using Asset Diagrams

The third step can also be considered a second introductory meeting between the analysts and the company representatives, where this time the analysts and the client representatives will present and agree on their understanding of the context and the targeted assets, based on the first meeting and the documentations provided by the client, this meeting also provides a high level security analysis, where the first threats, vulnerabilities, threat scenarios and unwanted incidents are identified and will be used for the upcoming steps [21].

3.1.4 Step 4: Approval of the Target Description

In the step 4 meeting, both the analysts and the client representatives focus on providing the necessary documentation for the rest of the analysis, including the focus, the target and the scope that they both understood and agreed on, this step focuses on presenting a more defined description of the target that will be analysed including assumptions and preconditions being made, the step 4 is considered to be finished, when the client approves the documentation [22].

3.1.5 Step 5: Risk Identification Using Threat Diagrams

This step is the risk identification step,the CORAS method uses the brainstorming method HazOP , through a workshop led by the analysts. The structured brainstorming session takes advantage of the different backgrounds, interests and competences of the participants to have suggestions from different perspectives, compared to a more homogeneous group or from the same department within the company. The risk identification process consists of identifying threats, unwanted incidents, threat scenarios and vulnerabilities, always in respect of the identified assets that both parties agreed on. The activities are supported by the CORAS language, the results are documented in the form of threat diagrams using UML language [23].

3.1.6 Step 6: Risk Estimation Using Threat Diagrams

The sixth step aims to determine the risk level of each risk identified in the previous step, this step also uses the brainstorming technique with the client company personnel from different backgrounds in order to determine the likelihood and the consequences of the unwanted incidents. The combination of these values give the risk level for each identified risk, the CORAS threat diagrams support the estimation of the likelihood for threats and threat scenarios to cause the unwanted incidents [24].

3.1.7 Step 7: Risk Evaluation Using Risk Diagrams

The seventh step focuses on risk evaluation using risk diagrams. It consists of deciding which risks are acceptable to the client and which are not and needing evaluation for possible treatment or reduction. This risk evaluation is done using the already defined risk evaluation criteria and the results of the risk estimation. Step seven involves more estimation and evaluation of risks always in respect of the agreed upon assets [25].

3.1.8 Step 8: Risk Treatment Using Treatment Diagrams

The eighth step is dedicated to identify and analyse risk treatments using treatment diagrams; the threats that have been identified and categorized as unacceptable are evaluated to find ways to reduce them (apply security controls) in regards to their cost-benefit before the final plan is made [26].

3.2 The Facilitated Risk Analysis Process (FRAP)

The FRAP method was designed to make sure that the risks related to the business operations in a given organisation are being considered and documented. The method focuses on a system, application or a segment of business operation at a time and as for the actors involved in the process, there are the business managers who are familiar with the business characteristics and technical staff who are familiar with the system and have deep understanding of the potential vulnerabilities and existing security controls .

The first sessions consist of brainstorming discussion to point threats, vulnerabilities and the impact on the CIA (Confidentiality, Integrity and Accountability) of information, the other sessions will consist of analysing the effects of such impacts on business operations and categorizing the risks according to their priority level. The team goal is not to determine the ALE (annualized loss expectancy) and threat likelihood unless the data is available and will not take a lot of resources to be obtained.

The team will rely on the experience of its members and their knowledge about threats and vulnerabilities that can be obtained from literature or incidence response centers. So based on this, the FRAP method can be considered a paper based qualitative method. The next step for the team is to identify the security controls that could be implemented to reduce the risk. The team will choose 26 most cost effective controls and it is up to the business managers to decide which controls to implement by taking in consideration the type of the information asset and how it affects the business operations and of course the cost of the controls. The final result of the risk analysis would be, the risks that the organization is facing, their priority and the controls needed, this will be documented and sent to the project lead and the business manager to finalize the action plan [35].

The business manager role is to decide which controls to implement, after every risk has been assigned a control or chosen to be accepted, the senior business manager alongside the technical expert signs the final document.

In theory each risk analysis with FRAP consists of four stages:

- The pre-FRAP meeting takes about an hour and has the business manager,

project lead, and facilitator.

- The FRAP session takes approximately four hours and includes 7 to 15 people, through sessions with as many as 50 and as few as four people have occurred.

- FRAP analysis and report generation usually takes 4 to 6 days and is completed by the facilitator and scribe.

- Post-FRAP session takes about an hour and has the same attendees as the pre-FRAP meeting.

3.2.1 The pre-FRAP meeting

This is the first meeting In the process, it can be considered as an introductory meeting. The meeting members are preferably the business manager (our representative), the project development lead, and the facilitator. The meeting takes about an hour and it discusses the following topics:

- Scope statement — the project lead and business manager establish a scope statement where they agree on the scope of the analysis, what is going to be the object of the analysis and document it to be used in the upcoming sessions

- Visual — creating a visual representation of the process to be reviewed, a diagram model will do, and this model will be used during the FRAP session to help the team understand the flow of the process that's being analysed

- Establish the FRAP team — the business manager and project lead are responsible of of selecting the FRAP team members, the ideal number of participants is between 7 and 15, depending on the scope of the analysis and the nature of the system, it's not obligatory to have the following members in the team but it's recommended to have representatives from the following areas in the FRAP process.

  - Functional owner

- System user
- System administrator
- Systems analysis
- Systems programming
- Applications programming
- Database administration
- Information security
- Physical security
- Telecommunications
- Network administration
- Service provider
- Auditing (if appropriate)
- Legal (if appropriate)
- Human resources (if appropriate)
- Labor relations (if appropriate)

There are no specific rules on who should and should not participate in the meetings, but to have accurate results and data, it will be necessary for the functional business owner and system users to be part of the FRAP, since it is their business process that is being reviewed and it would be practical for them to be part of the process.

The system group is considered an important part of the FRAP team. The

system administrator exists in the user department, and usually has some training in the new application or system that is subject to the analysis and system administrator also in direct contact with the user in case of a problem.

The system analysis group can make sure that all parties during the FRAP session are on the same page, since they are familiar with both languages, business and information systems. The systems programming group are the ones in charge of supporting the platforms and in charge of keeping the operating environment working and properly configured.

Application programming: are the individuals that are in charge of creating new applications or customizing existing applications or third party software to meet the owner's needs. Database administrators are the technical individuals that are familiar with the database structure and maintain its security mechanisms.

Information security: usually the FRAP is facilitated by someone from the information security department, but that does not mean that the team should not have a representative from the information security department, since the FRAP facilitator maintains a neutral position.

Physical security: a member from the facility engineering can have added value to the FRAP meeting by having a point of view from the physical operations perspective. Network administration: if the scope includes networks or telecommunication devices or systems, which is usually the case, having a representative from the network administration is necessary.

The rest of the group is classified as appropriate. The audit group will probably use the results of the analysis when conducting an audit for the ressource, the legal team would be recommended in case the resources in question have a huge impact on the organization, the same goes for the human resources, if the resources have impact on the employes, a representative from HR would be recommended to be part of FRAP. This list is not fixed and FRAP doesn't require all the members that have been mentioned above to conduct, the idea is that in order for a FRAP analysis to be fruitful, it must have representatives from a wide spectrum of employee groups.

- Agreement on definitions — since risk analysis topic can be new to some of the members of the FRAP, the terminology can be confusing the participants, therefore to avoid misconception, some of the key terms that will be used during the process should be defined and agreed upon such as:

- Risk
- Control
- Impact
- Venerability
- Confidentiality
- Integrity
- Availability

In the pre-FRAP meeting it's recommended also to decide which method will be used to prioritize threats. There are two ways to do so. First would be to have the FRAP team review all the existing threats as if no security controls are in place, this would result in the ideal logical control set. The second way would be to assess threats in consideration of the existing threats, which can be done through three phases:

1. Threat analysis : to review the existing environment, identify threats, prioritizes the threats and recommend safeguards.

2. Safeguard implementation : determine which safeguards are suitable to the business in regards of the costs

3. Security assessment : review the safeguards (controls) and determine their effectiveness.

3.2.2 The FRAP facilitator

The frap facilitator is a very important element during FRAP, in order for the FRAP sessions to be fruitful and interesting, the frap facilitator has to prepare himself and obtain a few skills such as:

- *Listen* — having the ability to be responsive to verbal and non-verbal behaviors of the attendees. Being able to paraphrase responses to the subject under review and to be able to clarify the responses.

- *Lead* — getting the FRAP session started and encouraging discussion while keeping the team focused on the topic at hand.

- *Reflect* — repeating ideas in fresh words or for emphasis.

- *Summarize* — being able to pull themes and ideas together.

- *Confront* — being able to feed back opinions, reacting honestly to input from the team and being able to take harsh comments and turn hem into positive statements

- *Support* — creating a climate of trust and acceptance.

- *Crisis intervention* — helping to expand a person's vision of options or alternatives and to reinforce action points that can help resolve any conflict or crisis.

- *Center* — helping the team to accept others' views and build confidence for all to respond and participate

- *Solve problems* — gathering relevant information about the issues at hand and help the team establish an effective control objective.

- *Change behavior* — look for those that appear not to be part of the process and bring them into active participation.

During the FRAP session a few regulations should be agreed upon by the partic-

ipants and preferably kept in the location where the FRAP meetings are taking place during the whole process such as:

- Everyone participates
- Stay within identified roles
- Stick to the agenda/current focus
- All ideas have equal values
- Listen to other points of view
- No ”plops”...all issues are recorded
- Deferred issues will be recorded
- Post the idea before discussing it
- Help scribe ensure all issues are recorded —One conversation at a time
- One angry person at a time
- Apply the 3-minute rule
- Be: Prompt,Fair,Nice and Creative

3.2.3 The FRAP session

The FRAP session normally lasts for four hours, but depending on the size of the organization and the context of the analysis. A typical FRAP session consists of three sections:

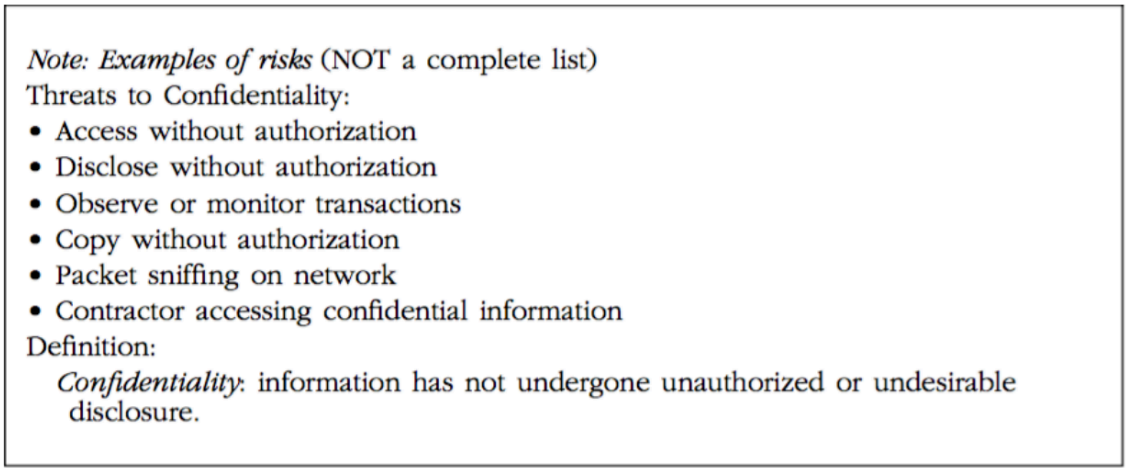
first section:
the first section is considered as an introduction to what is going to follow, during

this phase the FRAP team will be introduced and will be giving a name, title, department and phone number, which will be documented by the Facilitator/Scribe and most important, assigning roles and discuss it. The roles that are being suggested are:

- The Owner
- The Project Lead
- The Facilitator
- The Scribe
- The Team Members.

Also in this initial phase, the FRAP team will be introduced to the process of the method and the scope statement.it's important for the participants to understand the process, so one member of the technical team should give a 5 min presentation of the process using the visual model that was mentioned in the pre-FRAP section. Finally a copy of the definitions should be given after reviewing. *second section:* The second section is about brainstorming, where the team will focus on each of the review elements (integrity, confidentiality, and availability), and try to highlight risks, threats, and issues for each element, figure 3.1 is an example of some of the threats on confidentiality

Figure 3.1: Example of the list of threats on confidentiality [28]


Note: Examples of risks (NOT a complete list)
Threats to Confidentiality:
- Access without authorization
- Disclose without authorization
- Observe or monitor transactions
- Copy without authorization
- Packet sniffing on network
- Contractor accessing confidential information

Definition:
Confidentiality: information has not undergone unauthorized or undesirable disclosure.

The process for this step consists of the facilitator displaying definitions and some examples of risks, and the teams are given a few minutes (3 minutes) to note the risks that they think it's concerning. The facilitator then will go around and collect the risks, each person can provide one risk, so that everyone has a chance to contribute, this process goes for the rest of the elements until all the risks are documented. After a short break, the team will continue by reviewing and editing the risks (taking off duplicates) collected. Next, the team will prioritize each of the risks in terms of how vulnerable the organization is to the risk and the business impact in case of occurrence. The scale used is part of the definitions that have been agreed on during the pre-FRAP phase.

Some of the terms used are:

- *High* vulnerability: very substantial weakness exists in the systems or the operational routine, and where the business impact potential is severe or significant, the control must be improved.

- *Medium* vulnerability: some weaknesses exist and where the business impact potential is severe or significant, the controls can and should be improved.

- *Low* vulnerability: the system is already well constructed and operated correctly. No additional controls are needed to reduce vulnerability.

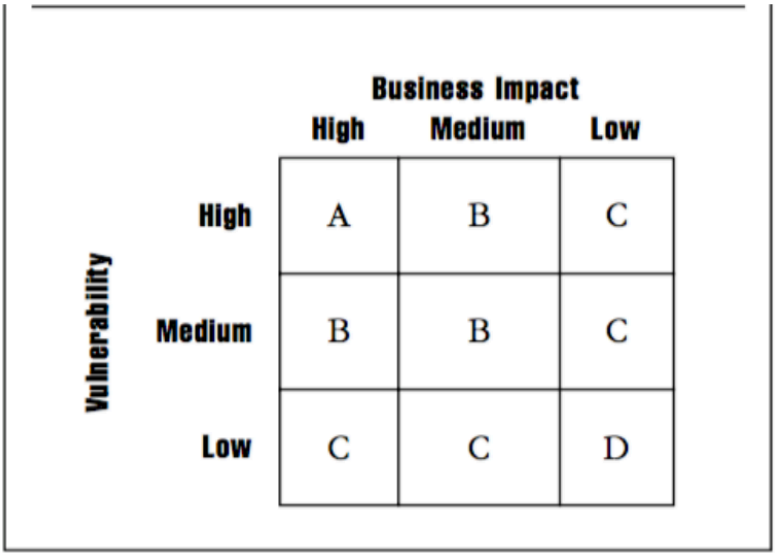
- *Severe* impact (High): likely to put us out of business or severely damage our business prospects and development.

- *Significant* impact (Medium): will cause us significant damage and cost, but we shall survive.

- *Minor* impact (Low): the type of operational impact we expect to have to manage as part of ordinary business life.

The team is given the matrix on figure 3.2 to assign each risk to a letter

Figure 3.2: Risk matrix [29]



Each risk should be assigned one of the following letters based on the nature of the risk and its impact on the organization:

- A — corrective action must be implemented
- B — corrective action should be implemented
- C — requires monitoring
- D — No action required

There are multiple ways to assign the priorities to the risks, one of which is the facilitator goes over each risk one by one and the team discusses each risk and then reaches consensus. figure 3.3 is an example of the results of this task

Figure 3.3: Example of risks given value and appropriate controls [30]

Risk #	Risk	Type	Priority	Controls
1	Information accessed by personnel not intended to have access	INT	B	3, 5, 6, 11, 12, 16
2	Unclear or nonexistent versioning of the information	INT	B	9, 13, 26
3	Database could be corrupted by hardware failure, incorrect, bad software	INT	D	
4	Data could be corrupted by an incomplete transaction	INT	C	
5	Ability to change data in transit and then changing it back in order to cover the activity	INT	C	
6	A failure to report integrity issues	INT	A	7, 11, 12, 13, 20, 21
7	Incompletely run process or failure to run a process that could corrupt the data	INT	B	1, 2, 12, 13, 14, 15, 18, 20, 21, 25
8	Lack of internal processes to create and control, manage data across functions	INT	A	7, 13, 17, 20, 23, 25
9	No notification of integrity problems	INT	A	7, 13, 26
10	Information being used in the wrong context	INT	B	11, 12, 19
11	Third-party information may have integrity issues	INT	B	7, 13, 26
12	Third-party access to information	INT	A	3, 4, 5

- *Risk* = actual risk voiced by FRAP team member
- *Type* = Integrity, Confidentiality, or Availability risk
- *Priority* = Priority level A, B, C, or D
- *Controls* = controls identified to help mitigate the risk

The controls used in the last example were provided by the business manager to the team members to use during the FRAP session, it's part of the FRAP supporting documents and it consists of a list of 26 controls developed by various FRAP facilitators, the document is used as a starting point, but it's subject to change if needed by the team. The output of the FRAP session is three deliverables:

- The risks identified
- The prioritization of each risk
- The suggested controls for high and major risks

The last step of the FRAP session is to identify controls for the concerning risks. To do so, one way is the facilitator going through each high priority risk and the team can suggest what control number they think can help reduce the risk. The controls that have been assigned to each risk by the team in the FRAP session were a suggestion, it does not mean that all of these controls will be implemented, the business manager, project lead and the facilitator will work together in the post-FRAP meeting on which of the controls are applicable. the control list is shown in figure 3.4

The FRAP session is considered complete, when the three deliverables are finished:

- Risks identified
- Risks prioritized
- Controls identified

Figure 3.4: List of security controls [31]

Control Number	Class	Control Description
14	Backup	Operations controls: training for a backup to the system administrator will be provided and duties rotated between them to ensure the adequacy of the training program.
15	Training	Operations controls: application developers will provide documentation, guidance, and support to the operations staff (service provider) in implementing mechanisms to ensure that the transfer of information between applications is secure.
16	Access control	Operations controls: mechanisms to protect the database against unauthorized access, and modifications made from outside the application, will be determined and implemented.
17	Interface dependencies	Operations controls: systems that feed information will be identified and communicated to the service provider to stress the impact to the functionality if these feeder applications are unavailable.
18	Maintenance	Operations controls: time requirements for technical maintenance will be tracked and a request for adjustment will be communicated to management if experience warrants.
19	Training	User controls: implement user programs (user performance evaluations) designed to encourage compliance with policies and procedures in place to ensure the appropriate utilization of the application.
20	Service level agreement	Acquire service level agreements to establish level of customer expectations and assurances from supporting operations.
21	Maintenance	Acquire maintenance and/or supplier agreements to facilitate the continued operational status of the application.
22	Physical security	In consultation with facilities management, facilitate the implementation of physical security controls designed to protect the information, software, and hardware required of the system.
23	Management support	Request management support to ensure the cooperation and coordination of various business units, to facilitate a smooth transition to the application.
24	Proprietary	Proprietary controls
25	Corrective strategies	The development team will develop corrective strategies such as: reworked processes, revised application logic, etc.
26	Change management	Production migration controls such as search and remove processes to ensure data stores are clean.

3.2.4 Post-FRAP meeting

The Post-FRAP meeting is supposed to have as a result, five deliverables:

- The Cross Reference Sheet
- Identification of existing controls
- Consulting with Owner on open risks
- Identification of controls for open risks
- Final Report

The most time consuming part of the post-FRAP meeting is considered to be the cross reference sheet, since the facilitator/scribe has to present each control and identify all the risks that can be affected by this control. Using the previous example of the FRAP session deliverable, on row 2 where the team identified 3 controls (9,13,26) for risk number 2, the cross reference sheet for control number 9 would be like the figure 3.5

Figure 3.5: Example of a cross reference sheet [32]

Control Number	Control Description	Risk #	Risk	Type	Priority
9	Adhere to a change management process designed to facilitate a structured approach to modifications, to ensure appropriate steps and precautions are followed. "Emergency" modifications should be included in this process.	2	Unclear or nonexistent versioning of the information	INT	B
		16	Impact to business by using information that is incorrect	INT	B
		23	Not responding to requests in a timely manner	INT	A
		25	E-business integrity policies conflict with existing corporate policies	INT	A
		29	Wrong document or data is published	INT	A
		35	Incorrect use of the modification process in the application development process (change code without testing)	INT	B
		40	Personal information for staff might be posted on the Internet without authorization	CON	A
		44	New technologies leading to breaches of confidentiality	CON	A
		47	Loss of sales and increased costs due to release of competitive advantage information without company knowledge	CON	B
		50	Electronic eavesdropping of company sites	CON	B
		9	Incorrectly made hardware or software changes	AVA	B

The cross reference sheet depicts the number of risks that can be mitigated by each control, which allows the business manager to decide which control is worth applying. Usually the facilitator is given a couple of days to finish the cross reference sheets. When the task is done, the action plan and the cross reference sheets are sent to the business manager. Using the action plan and the cross reference sheets, the facilitator and the project lead discuss and determine which controls already exist. When this task is done, the facilitator and the project lead meet with the business manager to go through the deliverables and recommend which controls are suitable for the remaining risks as shown in figure 3.6.

Figure 3.6: Selected controls [33]

Owner Action	By Who	When	Additional Comments
ACF2 has been implemented and the access control list will be reviewed to identify authorized users	Owner & IP	7/15/00	
Change management procedures already in place	Operations	complete	
Employee training sessions scheduled	HR	8/15/00	
Backup SLA to be reviewed with operations.	Owner & Operations	7/31/00	
SLA with service provider to be implemented.	Owner	8/20/00	
SLA with service provider to be implemented.	Owner	8/20/00	

The facilitator, project lead and the business manager get together also to determine which controls will be most effective and determine who will implement them and by what date. In case the controls will be implemented by a third party, a further discussion should take place to determine the completion date. After all the risks are either assigned a control or being accepted by the risk owner, The final document that should be delivered is the final report as shown in figure 3.7 [36].

Figure 3.7: Final report[34]

Date: (enter date)

To: Mr. Owner
IS Security Center of Excellence (SCoE) Manager
Owner/Owner's Representative

From: Ms. Facilitator
IS Information Management Center of Excellence (IMCoE) Manager

Subject: *Facilitated Risk Analysis*

The Information Protection group facilitated a Risk Analysis session on the functionality named below. The Risk Analysis attendees identified the risks and controls shown on the attached Action Plan. The attendees included you, or your representative, to ensure that the concerns of your organization were properly addressed.

The Action Plan shows which of the controls identified during the Risk Analysis have been, or will be implemented. You should have made the decisions as to if and when the controls will be implemented.

FRAP Date: 6/8/00
System/Application: IS E-commerce Functionality
Owner: Mr. Owner
Facilitator: Ms. Facilitator

Please read the Statement of Understanding below, sign it, and return it to me.

STATEMENT OF UNDERSTANDING: I, the Owner, understand that the risks identified on the attached Risk Analysis Action Plan could cause the integrity, confidentiality, and/or availability of this system/application's information to be negatively impacted. I have decided to implement the controls according to the schedule on the attached Risk Analysis Action Plan. I understand that any risks that are not controlled could adversely affect corporate information and company business.

I am aware that a copy of the Risk Analysis Action Plan will be forwarded to the Audit organization.

Owner/Owner's Representative
IS Security Center of Excellence (SCoE) Manager — Date

IS Information Management Center of Excellence (IMCoE) Manager — Date

3.3 ISRAM

ISRAM is an information security risk analysis method that was designed by Bilge Karabacak and Ibrahim Sogukpinar and was introduced to the public in 2004. The method was designed to combine both risk assessment methods, quantitative and qualitative. The core of the risk model used in the ISRAMM method is based on the following formula, which is the fundamental risk formula: Risk=Probability of occurrence of security breach * Consequence of occurrence of security breach. These are the two factors that the method focuses on during the whole analysis. The risk model of ISRAM which is based on the previous formula is demonstrated in figure 3.8, which presents the quantitative part in the method [17].

Figure 3.8: Formula used to calculate risk in ISRAM [16]

$$\text{Risk} = \left(\frac{\sum_{m} \left[T_1 \left(\sum_{i} w_i p_i \right) \right]}{m} \right) \left(\frac{\sum_{n} \left[T_2 \left(\sum_{j} w_j p_j \right) \right]}{n} \right)$$

- i: the number of questions for the survey of probability of occurrence, determined at Step 2.
- j: the number of questions for the survey of consequences of occurrence, determined at Step 2.
- m: the number of participants who participated in the survey of probability of occurrence, becomes definite at Step-5.
- n: the number of participants who participated in the survey of consequences of occurrence, becomes definite at Step 5.
- wi, wj: weight of the question “i” (“j”), determined at Step 2.
- pi, pj: numerical value of the selected answer choice for question “i” (“j”), determined at Step 3.

- T1: risk table for the survey of probability of occurrence, constructed at Step 4

- T2: risk table for the survey of consequences of occurrence, constructed at Step 4.

- Risk: single numeric value for representing the risk. Obtained at Step 6.

The ISRAM method is considered to be a survey based process that uses public opinion , where a designated team from the organization prepares and conducts surveys that contains questions concerning the information security problem for the rest of the personnel and system users that are subject to the security analysis, the participants can be managers engineers or common users of the system. The goal behind the survey is to understand and comprehend the effect of the security problem on the system or the organization. There are two surveys that are being conducted separately and independently during the process, one for each factor from the formula presented above (“Probability of occurrence of security breach” and “Consequence of occurrence of security breach”). The preparation and the conduction of the surveys are defined in the following steps. The ISRAM method is based on seven steps, for preparing and conducting the surveys, creating the risk tables, calculating risk and assessing the results.

3.3.1 The first step

Represents the awareness of the problem or the acknowledgement of the need for risk assessment. when the organization , or the management decides on conducting a risk assessment for a certain security problem, that means that the first step was achieved.

3.3.2 The second step

Consists of two main parts, first listing all the factors that affect the probability and the consequences of occurrence of a security breach, second part is assigning weight values to the factors, one factor can have more effect on the probability than consequence, that is why weight values are designated separately, it is more for the question than the factor, this step is considered very important to obtain accurate and objective results, to succeed in this step, employees who are familiar with the information system and have a security perspective and enough security awareness on the security problem, what would cause it and its consequences and also familiar with the information system that is affected by the security problem should participate.

3.3.3 The third step

Focuses on converting the factors into survey questions and appending each question with its appropriate answer choices. Each question may have a different number of answers, the number of choices for each question should be decided by the risk analyst depending on the question and the security problem in question. After determining the answer choices, each answer is given a numerical number. The answer choices and their numerical values must be selected carefully because the answers and their values selected by the survey participants are the main component of the risk calculations.

3.3.4 The fourth step

It is dedicated to creating risk tables for both factors, probability and consequences, the utility of the risk tables is to convert the bulk results of the surveys into quantitative and scaled values. The content of the tables change based on the survey conducted, the risk table is considered the link between the survey results and the quantitative value of the risk parameter under consideration.

3.3.5 The fifth step

Comes after establishing the survey questions and their answer options along with the weight values and of course the risk tables. The questions can be distributed to the participants via hard copies or electronically via email, the questions can be placed as two separate surveys, one for each risk factor. The survey questions are a valuable asset to the risk analysis process, but the main target of ISRAM is to convert these answers into numeric values.

3.3.6 The sixth step

Consists of applying the formula mentioned earlier to get a single quantitative result from the answers of the conducted surveys

3.3.7 The seventh step

It is the assessment step not only for the numerical results of the survey, but also for the answers given by the participants. The result of the ISRAM method is a report, where the survey results are displayed and assessed with the security risk mitigation suggested [18].

3.4 OCTAVE

OCTAVE is a framework for identifying and managing information security risks. OCTAVE was developed in 2001 at Carnegie Mellon University (CMU), for the United States Department of Defense. The framework has gone through several evolutionary phases since that time, but the basic principles and goals have remained the same. Two versions exist: OCTAVE-S, a simplified methodology for smaller organizations that have flat hierarchical structures, and OCTAVE Allegro, a more comprehensive version for large organizations or those with multilevel structures

The octave method uses a three phase approach to break down the main elements of the organization that will be used in the risk analysis process and also to identify its information security needs. Each phase contains a number of processes, to be specific four in phase one, two in phase two and two in phase three.

The Octave method consists of a series of workshops that require interaction from its participants. These workshops are divided into two types, the first type of workshops involve various members of the organisation from different backgrounds and departments and the second is between the analysis team members that they conduct on their own.

Both workshops have a leader and a scribe, where the leader is responsible for guiding all workshops and making sure that all activities are being conducted correctly and completely, the leader is also responsible for making sure that all members understand their roles and that all the members are participating actively. The scribe is a person responsible for documenting the process of the workshops electronically or on paper. The octave method is based on the self-directing concept, meaning that the analysis team is part of the organization and all of the participants are members of the organization. No external expertise is used during the process. The analysis team members belong to both the business units and the IT department, since information security covers both business and IT related issues. The team members coming from the business unit background can relate to what information is needed to complete their tasks and how to access it, while the IT department members understand the infrastructure of the IT system and how to keep the information flow running. The octave method is asset oriented, meaning that the analysis focuses on the organization's assets and it's evaluation

is asset driven .

The first step in the octave method is preparation. One of the main success factors of the risk evaluation is to have the senior management support, when the management sponsors the event, it reflects positively on the performance of the participants and their interaction during the workshops. The second factor is choosing the analysis team, having a team with sufficient skills and experience is very important, since these members will be in charge of managing the process and analysing the information. In order for the whole process to be successful and fruitful, the scope must be established and agreed on in the beginning to avoid any confusion or unnecessary waste of resources. Selecting participants for the workshop is also part of the preparation phase, it's not supposed to be based on availability but more on the skills and the knowledge of the individuals, and what is appropriate for the workshop. After the completion of the preparation for the OCTAVE method, the organization is ready to start the evaluation with phase 1. Phase 1 consists of 4 processes while both phase 2 and phase 3 consist of 2 processes [6].

3.4.1 Process 1 to 3 (phase 1)

Processes 1 to 3 focus on gathering necessary information on the organization to understand what is actually going on in it, what are the critical assets and how are they being protected by the organization. To do so, process 1 to 3 introduces a series of workshops held by the analysis team. This way you collect information through employees from different levels of the organization as well as from those with business and information technology expertise.

The workshops usually take around 3 to 4 hours depending on the facilitators and how they manage it. Each knowledge elicitation workshop is dedicated to a specific group of participants from an organizational level and the format of these workshops are the same through the three processes, the only difference is the audience. For example, for the first process the participants are senior managers, the second process is dedicated to operational area managers and the third process is for general staff and information technology staff. For the third process, it's preferable to conduct two separate workshops, one for the general staff members and one for the information technology staff members. The two separate

workshops give the opportunity for the information technology staff to focus on more technical issues. Depending on the size of the organization and the scope of the evaluation, you can end up with multiple workshops in each level. figure 3.9 demonstrates the tasks required in the workshops in each process.

Figure 3.9: Activities in process 1-3 [2]

Activity	Description
Identify assets and relative priorities	The participants identify the assets used by the organization. They then select the assets most important to the organization and discuss their rationale for selecting those assets.
Identify areas of concern	The participants identify scenarios that threaten their most important assets based on typical sources and outcomes of threats. They also discuss the potential impact of their scenarios on the organization.
Identify security requirements for most important assets	The participants identify the security requirements for their most important assets. In addition, they examine trade-offs among the requirements and select the most important requirement.
Capture knowledge of current security practices and organizational vulnerabilities	Participants complete surveys in which they indicate which practices are currently followed by the organization's personnel and which are not. After completing the survey, they discuss specific issues from the survey in more detail.

The last step or task of each of the three processes can be considered as the most important. As stated in the table above each of the participants is required to complete a number of surveys depending on the scope and the organization in which they indicate the practices that are currently followed by the organization's personnel and which are not. The surveys are based on a catalog of practices and each survey is specific to an organizational level .

3.4.2 Process 4 (Phase 1)

This process consists of two main tasks, the first task is to consolidate the information gathered from the previous processes 1 to 3, this action allows the analysis

team to fix any inconsistencies and gaps from the workshop participants. The figure 3.10 elaborates the procedure.

Figure 3.10: Activities in process 4 [3]

Activity	Description
Group assets by organizational level	The assets that were identified during processes 1 to 3 are grouped by organizational level to easily identify common assets and viewpoints.
Group security requirements by organizational level and asset	Security requirements that were identified during processes 1 to 3 are grouped by asset and organizational level to easily identify commonalities and conflicts.
Group areas of concern and impacts by organizational level and asset	Areas of concern that were identified during processes 1 to 3 are grouped by asset and organizational level to easily identify common concerns and gaps in perception at different levels.

The second task is examining the information based on the individual perspectives and deciding which assets are critical to the organization and how they are threatened. This process is considered vital to the rest of the evaluation. The critical assets are used in phase 2 to focus the infrastructure evaluation in phase 2 and the threat profiles are the basis for the risk analysis in phase 3. After filtering and grouping the information gathered in process 1 to 3 comes the second part of the process and it consists of 3 main tasks:

- Identifying critical assets
- Refine security requirements for critical assets
- Identify risks for critical assets

Usually 5 critical assets are enough to create a mitigation plan, but depending on the size of the organization and the scope of the evaluation, it could be more or less.

Defining security requirements for the critical assets can be a bit difficult since the data collected from the previous processes might have some contradictions depending on the participants point of view, for example senior managers might consider confidentiality as the most important security requirement, while staff members can choose availability as the most important. The task here is to choose the appropriate requirement from the organization perspective.

The last step of the fourth process is to identify the potential threats toward the organization's critical assets in order to create a threat profile for each one of them. To do so the Octave method provides the generic threat profile that the analysis team can use to perform this task.

Before creating the threat profile, the analysis team must start with mapping the areas of concern to the generic threat profile, first the team must select which category of threats the area of concern is targeting (e.g., human actors using network access), then you map the threat properties to the corresponding asset-based threat tree. The extent of threats to be considered amid the evaluation can be represented in three structures; there's one tree structure for each category of threat. The set of the tree structures is called the generic threat profile. figures 3.11 figures 3.12 figures 3.13 figures 3.14 represent the generic threat profile as provided by the Octave method.

Figure 3.11: Human actors using network access [3]

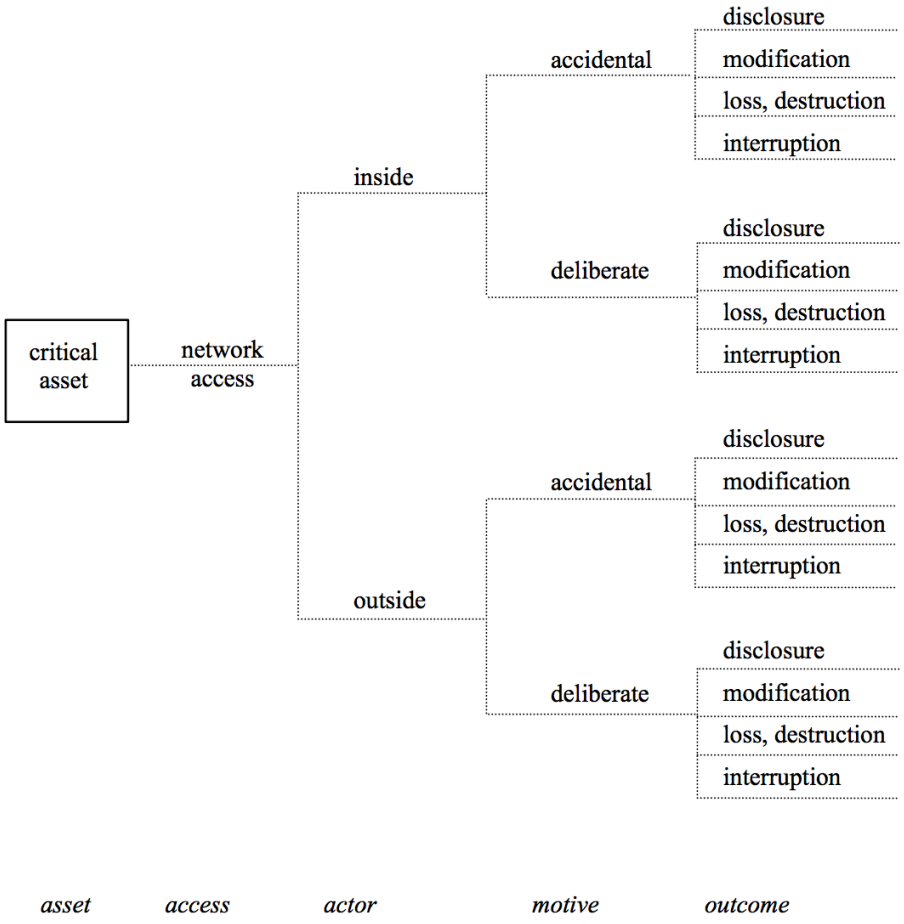


Figure 3.12: Human actors using physical access [3]

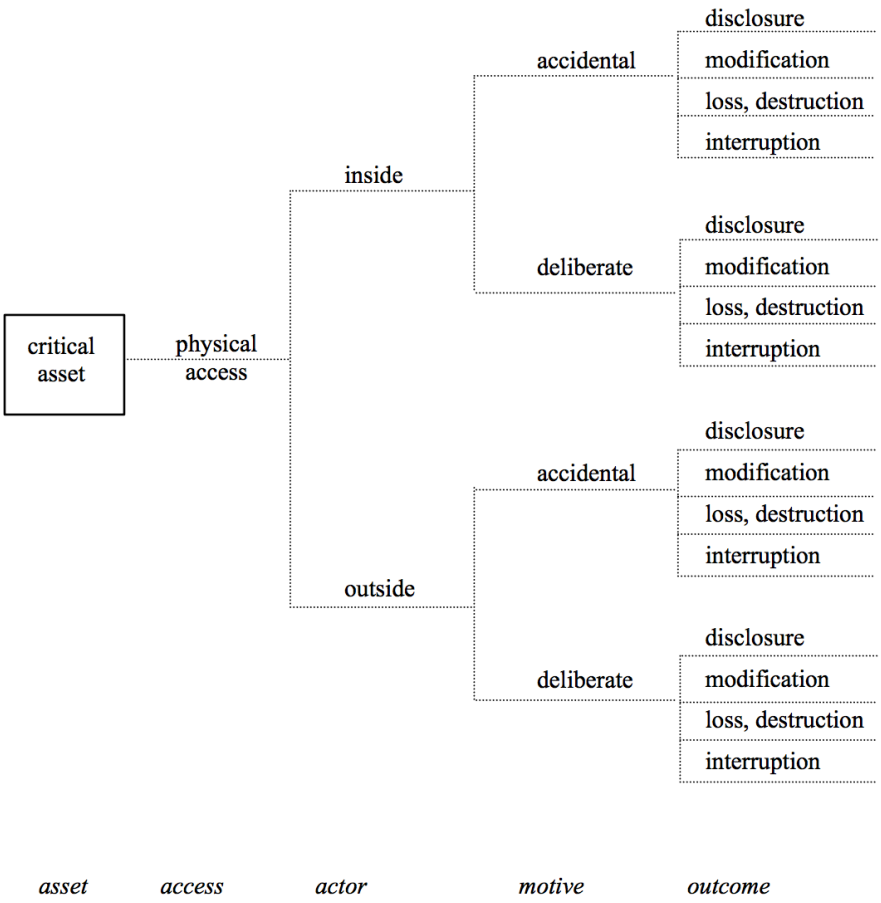
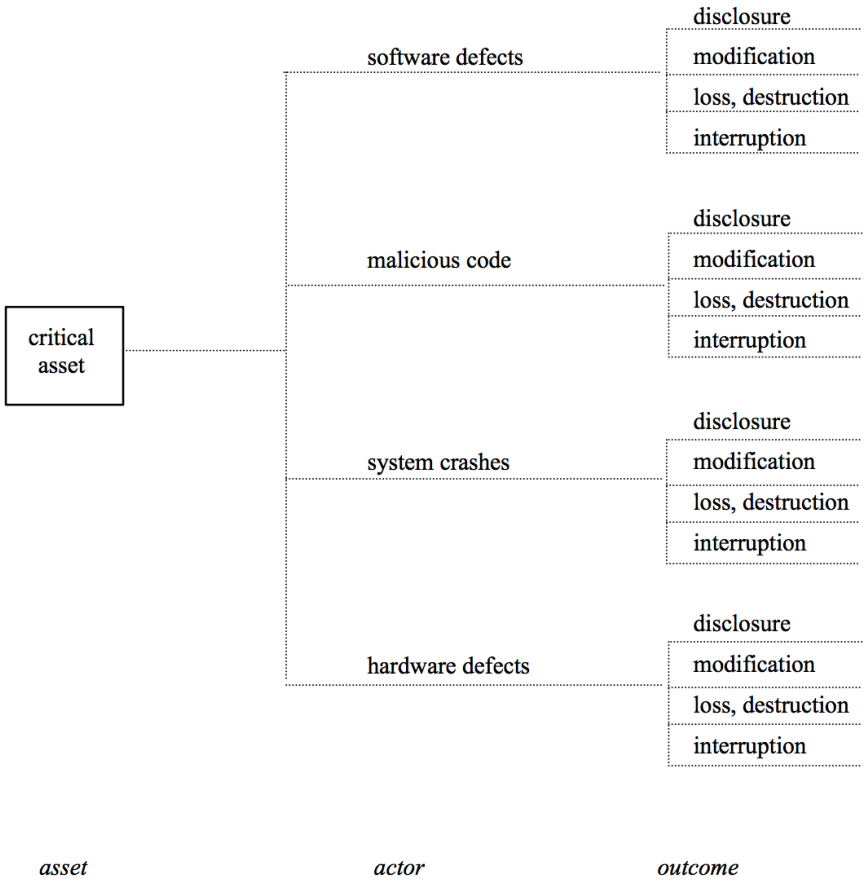


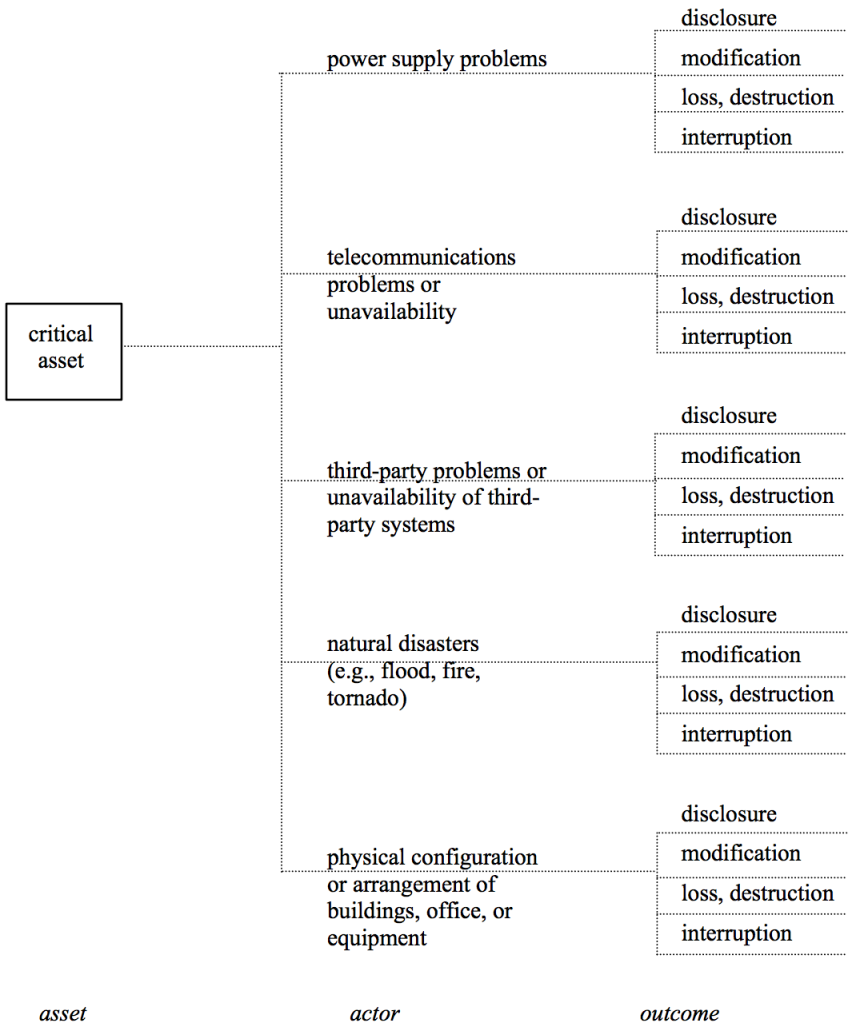
Figure 3.13: System problems [3]



The result of the first step would be a threat tree that is based on the area of concern which is the information obtained during the knowledge elicitation workshops. The next step would be performing a gap analysis, the reason behind this is to determine whether there are any other threats that endanger the critical assets of the organization that haven't been mentioned in the previous workshops. The last step of this part is checking threat profiles for consistency and completeness. After creating the threat tree for each critical asset, the analysis team must Compare the outcomes with the security requirements to check for consistency and completeness. When comparing the threat trees and the security requirements, must understand the relation between the outcomes and the security requirement such as confidentiality with disclosure, integrity with modification and availability with loss, destruction and interruption [7].

For example, if you have a security requirement for confidentiality but no threats with disclosure as an outcome, you need to interpret the meaning of this situation.

Figure 3.14: Other problems [3]



Consider the following possibilities:

- Confidentiality is not really a security requirement. You might have missed threats that result in disclosure of the critical asset.

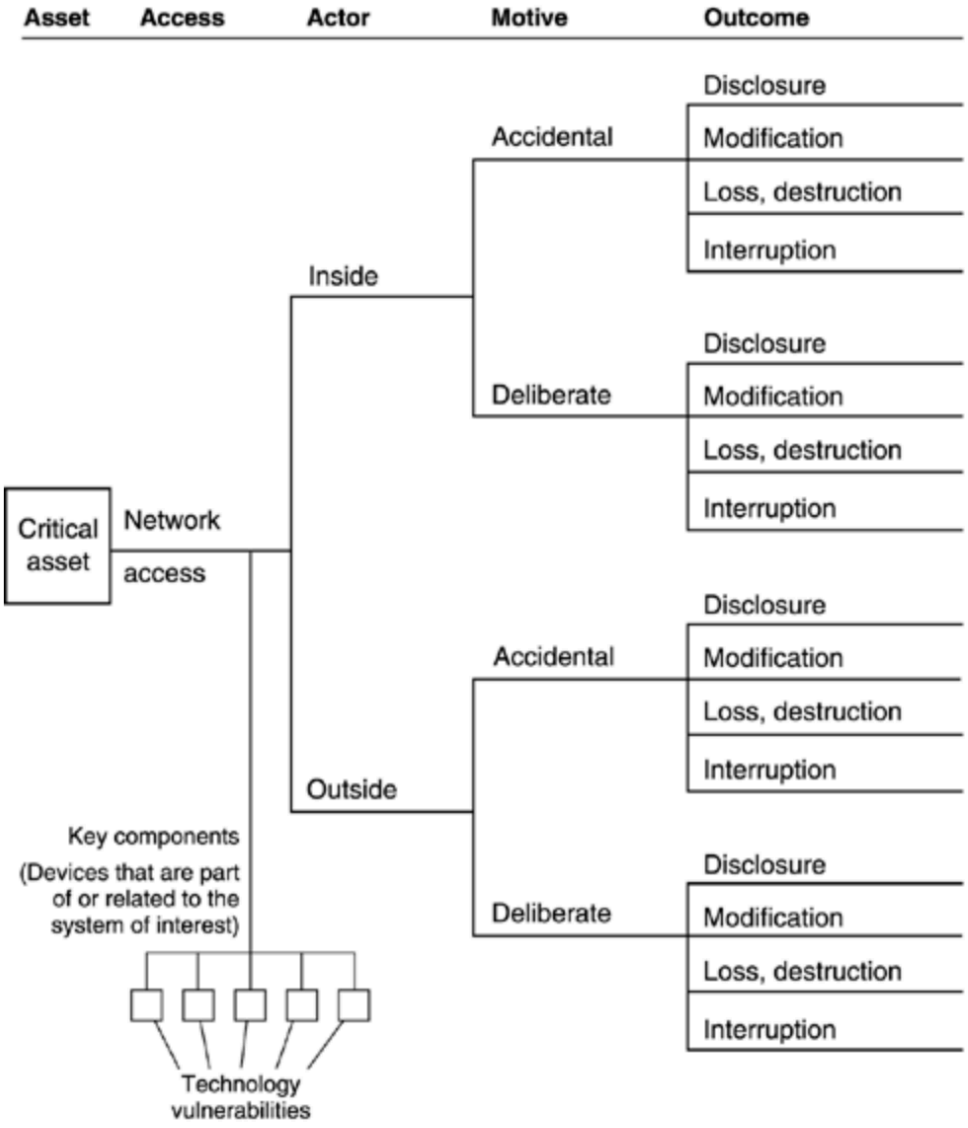
- There is no possibility or only a negligible possibility, of threats resulting in disclosure of the critical asset.

- The security requirement might be driven by law or regulation rather than by an existing threat.

3.4.3 Process 5 (phase 2)

Process 5 represents phase two, and the goal behind this process is first to identify key classes of components, and second, to identify infrastructure components to examine. In this activity we look at critical assets and threats from phase one in relation to your computing infrastructure. The focus in this process is the threat tree for human actors using network access, since that tree characterizes the range of scenarios that threaten the critical asset due to deliberate exploitation of technology vulnerabilities by individuals. Hence, this action is constrained to distinguishing information technology components that may be used as part of network attacks against critical assets. The figure 3.15 illustrates the relationship between a threat tree and infrastructure components.

Figure 3.15: The Relation between a threat tree and infrastructure components. [4]



This approach is also valid for examining threat scenarios for human actors using physical access. By examining the physical threat scenarios, you could identify important components from your physical infrastructure that could be used during attacks.

Process 5 workshop

In this workshop, it's advised that the team or the participants are the core analysis team members as well as any supplemental personnel that this team decides to

take in, and since this workshop will include some activities that would require technological expertise, it's advised to include information technology personnel. It's important to review all the activities that process 5 holds and make sure that the team has the necessary knowledge and skills to complete the tasks successfully. Some of the skills that are suggested are :

- Understanding of the organization's business environment and how business staff legitimately use information technology in the organization
- Understanding of the organization's information technology environment and knowledge of its network topology
- Good communication skills
- Good analytical skills
- Understanding of common exploits of technology vulnerabilities and the types of tools used to check for technology vulnerabilities.

The ultimate objective of phase 2 in Octave method is to to identify technological weaknesses in the computing infrastructure, this includes network services, architecture, operating systems, and applications, these vulnerabilities could be regrouped in the following categories [8]:

- Design vulnerabilities— a vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability
- Implementation vulnerabilities— a vulnerability resulting from an error made in implementing software or hardware of a satisfactory design
- Configuration vulnerabilities— a vulnerability resulting from an error in the configuration and administration of a system or component.

the figure 3.16 summarizes the workshop activities in process 5

Figure 3.16: Process 5 workshop activities [5]

Activity	Description
Identify key classes of components	The analysis team establishes the system(s) of interest for each critical asset. The team then identifies the classes of components that are related to the system(s) of interest.
Identify infrastructure components to examine	The analysis team selects specific components to evaluate. The team selects one or more infrastructure components from each key class to evaluate. In addition, the team also selects an approach and specific tools for evaluating vulnerabilities.

3.4.4 Process 6 (phase 2)

Process 6 represents the second task in phase 2, after identifying the key components in process 5, process 6 requires the results of an extensive technical task to carry out the workshop. After identifying the key components in process 5, the first task that is required before the workshop is a vulnerability evaluation process on the identified components. This task is conducted using automated tools. Based on the approach used in process 5, the same participants are advised to conduct the vulnerability evaluation, and since this task is considered more technical compared to the previous ones and the tools require specialized information technology and security knowledge , it's important that the participants have the appropriate skills to run the tests. The participants or the test runners are also responsible for reviewing and analysing the results and preparing an initial summary of technology vulnerabilities. The vulnerability evaluation task including preparing the initial summary is a heavy process and can take several days to complete, below are some of the skills that the participants must have to deliver the summary and to have a successful workshop.

- Understanding of the organization's information technology environment and knowledge of its topology
- Understanding of common exploits of technology vulnerabilities
- Knowledge of how to use and interpret the results of vulnerability evaluation

tools

- Good communication skills
- Good analytical skills

The participants suggested during the workshop in process 6 are the core analysis team members, selected members of the technology staff and the people who performed the vulnerability evaluation. The workshop usually takes around three hours, and the leader is required to make sure the technology evaluation task is complete and the people who run the tests are available to present the initial summary. After completing the technology evaluation and delivering the initial summary, it's time to start the workshop. process 6 consists of one workshop, that include three steps:

Step1:Review and Refine the Initial summary

In this step the analysis team reviewed the initial summary generated in the pre workshop task, and the participants who delivered the summary lead the review. The vulnerability evaluation was applied to each critical asset, and in this step the following information must be understood:

- The types of vulnerabilities found and when they need to be addressed
- The potential effects on the critical assets
- How the technology vulnerabilities might be addressed (applying a patch, hardening a component, etc.)

The evaluation summary is subject to change during the discussion if found appropriate. After the review and refinement of the summary is done, the new version must be documented and saved along with the detailed reports generated by the tools for future references when fixing vulnerabilities.

Step 2: Identify Actions and Recommendations

As a result of reviewing and refining the summary, actions or recommendations for addressing the technology vulnerabilities might be identified, one of the things that should be considered in this step is looking for vulnerability patterns, identifying patterns of technology vulnerabilities can reveal problems with the current security practices in the organization. All actions and recommendations should be documented, it will be used in process 8 while creating protection strategy, risk mitigation plans, and an action list.

Step 3: Perform a Gap Analysis

In this step, what you do is review the threat profiles created in process 4, but with a different perspective after conducting the vulnerability evaluation and reviewing the vulnerability summary. Performing a gap analysis on the threat profile for each critical asset you created during process 4 will allow you to reexamine the unmarked branches of the threat tree for human actors using network access. Do the technology vulnerabilities associated with the critical asset's key infrastructure components indicate that there is a more than negligible possibility of additional threats to the asset? Is a question to consider while reviewing the unmarked branches of a threat tree. Marking any new threats in the appropriate branches with comments and marks is necessary.

3.4.5 Process 7 (phase 3)

The previous workshops focused on collecting data about threat, assets and vulnerabilities, while the workshop in process seven allows you to use this data in the analysis that takes in consideration the organization mission and objectives. The participants in the workshop are the usual analysis team plus any additional personnel if needed. These participants are advised to have the following skills in order for the workshop to succeed:

- Understanding of the organization's business environment
- Understanding of the organization's information technology environment
- Good communication skills

- Good analytical skills

The workshop in process 7 consists of 3 main activities:

- Identifying the impact of threats to critical assets
- Creating risk evaluation criteria
- Evaluate the impact of threats to critical assets

1.Identify The Impact Of Threats To Critical Assets

Before jumping into the workshop, it's advised to review the information collected on the critical assets, since the workshop is based on the information collected in process 4, it's important to highlight the following for each critical asset:

- Security requirements
- Threat profiles
- Areas of concern

This information will indicate the importance of each asset and how it is threatened. The next step after reviewing the information, is creating a Narrative Impact Descriptions for each of the critical assets. Must keep in mind the difference between impact and outcome, where the outcome is the effect of the threat directly on the critical asset while the impact is the effect on the organization as a whole, for example the impact on the organization's operations or the personnel. Some of the areas to consider the impact on are:

- Reputation/customer confidence
- Safety/health issues
- Fines/legal penalties
- Financial

- Productivity

These impacts are somewhat general, and they are subject to modification, depending on the organization and their activity.

To conduct the Narrative Impact Description, first you select a critical asset and review it's threat profile along with selecting which of the threat outcomes (disclosure, modification, loss/destruction, interruption) are part of the scenarios in the profile, then the method suggests the following questions that will help with the description:

- What is the potential impact on the organization's reputation?
- What is the potential impact on customer confidence?
- What is the potential impact on customers' health or safety?
- What is the potential impact on staff members' health or safety?
- What fines or legal penalties could be imposed on the organization?
- What is the potential financial impact on the organization?
- What is the potential impact on the organization's or customers' productivity?
- What other types of impact could occur?

2.Creating risk evaluation criteria

The objective of this step is to create risk evaluation criteria that would help the organization to prioritize their known risks. To do so, it's important to review relevant information about the organization such as:

- Strategic and/or operational plans that outline the major business objectives of your organization
- Legal requirements, regulations, and standards of due care with which your

organization must comply

- Insurance information related to information security and information protection

- Results from other risk management processes used by your organization

The evaluation criteria it Is highly contextual meaning that every organization has to come up with its own criteria based on the nature of the organization, the size and also their activity. After reviewing the appropriate information and understanding any existing organizational risk limits based on strategic and operational plans, liability and insurance related issues, it's time to define the evaluation criteria. The method suggests a set of questions to use in the discussion for each area of impact:

- What defines a "high" impact on the organization?

- What defines a "medium" impact on the organization?

- What defines a "low" impact on the organization?

You need to define specific measures to rank risks (high,medium,low) in the organization for each case. For example low impact on productivity could be a few hours or couple of days, while high impact could be few weeks.

3.Evaluate The Impact Of Threats To Critical Assets

This activity is built on the previous steps, it uses the evaluation criteria defined earlier to evaluate the impact descriptions stated in the first activity in process 7. Also in this step, it's important to review the previous data, specifically the evaluation criteria, threat profiles and impact descriptions for each critical asset.

For each critical asset, first review the impact descriptions for each threat outcome, next assign an impact measure to each impact description. The results must be documented. Risk profiles can be created by adding impact values to the threat profiles, as a result you get a set of risk scenarios for each critical asset. By finishing this activity process 7 is now done, and you can move to the next and last process.

So far the risk analysis technique used was a scenario planning based, due to the lack of subjective data. However it's possible to include probability to your threat profiles through the following activities [9].

- Describe the probability of threats to critical assets.
- Create probability evaluation criteria.
- Evaluate the probability of threats to critical assets.

3.4.6 Process 8 (phase 3)

Finishing process 7 means that you have successfully identified the organization's risks on it's critical assets and evaluated the potential impact on your organization of those risks. The first workshop in this process represents the transition from identifying risks to addressing them. Unlike the previous processes, process 8 consists of two workshops, workshop A (process 8A) and workshop B(process 8B).

3.4.7 Process 8A (phase 3)

Workshop A has an objective of analyzing all the previous risk-related data collected throughout the evaluation and trying to improve the organization's security status. The participants in this workshop are the core analysis team and any additional personnel if found needed. The method suggests the following skills to have among the participants of the workshop:

- Understanding of the organization's business environment
- Understanding of the organization's information technology environment
- Understanding of the planning practices of the organization
- Ability to develop plans

- Good communication skills

Like some of the previous workshops, this one also requires some preparation before starting, the following data must be consolidated and compiled:

- The survey results from processes 1 to 3.
- The contextual information (security practices and organizational vulnerabilities) from processes 1 to 3.

The amount of information generated in the previous processes varies from one organization to another, depending on the size and other criteria, if the organization is big, the previous processes can take weeks to finish, so it's important to review the information. The information review task can be done either individually or in a group before the workshop. In addition to the data consolidated and compiled in the pre workshop phase, the following information must be reviewed for each critical asset:

- Threats to the critical assets
- Areas of concern for the critical assets
- Potential impact on the organization for each threat and associated impact values
- Technology vulnerabilities for selected components
- Recommended actions resulting from the infrastructure vulnerability evaluation

After reviewing the appropriate information needed, the workshop consists of three activities:

- Create protection strategy
- Create mitigation plans

- Create action list

Create protection strategy

"Protection strategy is the policy an organization develops to enable, initiate, implement, and maintain its internal security. It tends to incorporate long-term, organization-wide initiatives". The strategy presents a set of steps that the organization should follow to maintain/improve the security state. The method suggests that the strategy should be structured around the catalog of practices. The protection strategy should touch basis with each of the following practice areas:

- Security awareness and training
- Security strategy
- Security management
- Security policies and regulations
- Collaborative security management
- Contingency planning/disaster recovery
- Physical security
- Information technology security
- Staff security

In this activity, you try to define appropriate actions for each of the previous areas, and also the direction of the security efforts in the organization. Due to the limited resources, it's not possible to apply the protection strategy as it is nor immediately. After completing the evaluation, the activities in the strategy must be prioritized and then focus on implementing the critical ones. During this activity, you will use security practice information from process 1 to 3. The survey results from all the organization levels should be considered. It's likely to find inconsistencies in the survey results, but it's your task to get the picture and make sense of

the information. The surveys may indicate the current security practices in the organization, some respondents might indicate that some practices are not used by the organization, and some would say that are used, so keep in mind that the survey results are not 100 percent reliable. So it's important to look for consistencies in the results. It's also important to interpret the information from the inconsistencies found in the security policies, where for example management will confirm the existence of some policies that the survey participants might have answered otherwise. The protection strategy concerns two areas, Strategic Practice Areas And Operational Practice Areas.

To develop a Protection Strategy for Strategic Practice Areas, you must consider the following:

- The current practices in this area that your organization should continue to use
- The current practices in this area that your organization needs to improve
- New practices that your organization should adopt.

The method provides a set of questions to use concerning the Strategic Practice Areas:

Security awareness and training

- What can you do to maintain or improve the level of information security training that all staff members receive (consider awareness training as well as technology-related training)?
- Does your organization have adequate in-house expertise for all supported technologies? What can you do to improve your staff's technology expertise?
- What can you do to ensure that all staff members understand their security roles and responsibilities?

Security strategy

- Are security issues incorporated into your organization's business strategy?

What can you do to improve the way in which security issues are integrated into your organization's business strategy?

- Are business issues incorporated into your organization's security strategy? What can you do to improve the way in which business issues are integrated into your organization's security strategy?

- What can you do to improve the way in which security strategies, goals, and objectives are documented and communicated to the organization?

Security management

- Does management allocate sufficient funds and resources to information security activities? What level of funding for information security activities is appropriate for your organization?

- What can you do to ensure that security roles and responsibilities are defined for all staff in your organization?

- Do your organization's hiring and retention practices take information security issues into account (also applies to contractors and vendors)? What could you do to improve your organization's hiring and retention practices?

- What can you do to improve the way in which your organization manages its information security risk?

- What can you do to improve the way in which security-related information is communicated to your organization's management?

Security policies and regulations

- What can you do to ensure that your organization has a comprehensive set of documented, current security policies?

- What can you do to improve the way in which your organization creates, updates, and communicates security policies?

- Does your organization have procedures to ensure compliance with laws and regulations affecting security? What can you do to improve how well your organization complies with laws and regulations affecting security?

- What can you do to ensure that your organization uniformly enforces its security policies?

Collaborative security management

- Does your organization have policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners)? What can your organization do to improve the way in which it protects information when working with external organizations?

- What can your organization do to improve the way in which it verifies that external organizations are taking proper steps to protect critical information and systems?

- What can your organization do to improve the way in which it verifies that outsourced security services, mechanisms, and technologies meet its needs and requirements?

Contingency planning/disaster recovery

- Does your organization have a defined business continuity plan? Has the business continuity plan been tested? What can you do to ensure that your organization has a defined and tested business continuity plan?

- Does your organization have a defined disaster recovery plan? Has the disaster recovery plan been tested? What can you do to ensure that your organization has a defined and tested disaster recovery plan?

- What can you do to ensure that staff members are aware of and understand your organization's business continuity and disaster recovery plans?

The Protection Strategy for Operational Practice Areas has an objective of identifying strategies to enable operational practices in your organization.To develop this strategy the method suggests the following questions:

- What training and education initiatives could help your organization maintain or improve its practices in each area?

- What funding level is appropriate to support your organization's needs in each area?

- Are your policies and procedures sufficient for your organization's needs in each area? How could they be improved?

- Who has responsibility for each area? Should anyone else be involved?

- What other departments in your organization should be involved in each area?

- What external experts could help you with each area? How will you communicate your requirements? How will you verify that your requirements are met?

For example, information technology staff members receiving training in secure system administration, could be a strategy to enable your organization's information technology security practices. The second protection strategy will address the Operational Practice Areas, to develop the strategy, the method suggests the following questions:

- What training and education initiatives could help your organization maintain or improve its practices in each area?

- What funding level is appropriate to support your organization's needs in each area?

- Are your policies and procedures sufficient for your organization's needs in each area? How could they be improved?

- Who has responsibility for each area? Should anyone else be involved?

- What other departments in your organization should be involved in each area?

- What external experts could help you with each area? How will you communicate your requirements? How will you verify that your requirements are met?

Create Risk Mitigation Plans

The mitigation plan focuses on critical assets rather than the whole organization, its objective is to mitigate direct risks towards the organization's critical assets. It usually contains actions, or countermeasures to address the threats. The octave method suggests that the mitigation plan should be structured based on the four threat categories for each critical asset. The method suggest to apply these four steps to create the Risk mitigation plans:

Step 1: Select Mitigation Approach

In this step you decide the mitigation approach for each Risk. it means that, for each risk you decide whether to accept it or mitigate it by defining what actions are designed to counter the threat and reduce the risk.

Step 2: Select Mitigation Actions

After deciding which risks are to accept and which are to mitigate, for each unaccepted risk you select the actions designed against the threats on the critical assets. The method suggests the following questions to consider for each critical asset while choosing the mitigation actions for each threat category:

- What actions could you take to recognize or detect this type of threat as it is developing?
- What actions could you take to resist or prevent this type of threat from developing?
- What actions could you take to recover from this type of threat if it develops?
- What other actions could you take to address this type of threat?
- How will you test or verify that this mitigation plan works and is effective?

The sum of the actions concluded from this task are to be evaluated and prioritized based on the cost-benefit of each action along with the organization's budget and constraints. Then you focus on implementing the highest-priority mitigation actions.

Step 3: Review Mitigation Plans for Themes and Gaps

This step addresses any themes or inconsistencies that the mitigation plan might have, it's important to go through all the actions selected and make sure that the elements in the mitigation plan are consistent with each other. It is also important to select the actions that reduce risks for more than one critical asset and give these actions priority.

Step 4: Incorporate Strategic Themes into Protection Strategy

Finally, after selecting any recurring themes from the previous step, you decide which themes are suitable to integrate in the protection strategy. An example of a theme would be advanced training to the users to configure and maintain systems and networks securely [10].

3.4.8 Process 8B (phase 3)

After successfully finishing the first part of process 8, the next step is workshop 8b, this workshop focuses more on the next step after octave. The participants in this workshop are the main analysis team plus the senior managers. The idea of this workshop is to put the results of the previous processes such as, protection strategy, risk mitigation plans, and the action list into the senior managers perspective. The method suggests the following skills needed for the workshop to succeed:

- Facilitation skills
- Ability to present to and work with senior managers
- Good communication skills
- Good analytical skills

Before meeting the senior managers, a briefing should be prepared for presentation, this briefing should contain two parts: The first part is the information collected in the previous processes The second part is the results of the evaluation

along with protection strategy, risk mitigation plans, and action list. The activities in this workshop are the following:

- Present risk information
- Review and refine protection strategy, mitigation plans and action list
- Create next steps

Present risk information

The information gathered from the previous processes, concerning Risk are presented to the senior managers:

- Current practices and organizational vulnerabilities
- Asset information
- Risk profiles for critical assets

Review and refine protection strategy, mitigation plans and action list

In this step, the protection strategy, the mitigation plans and the the action list are presented to the senior managers and at the end of the presentation, the managers can participate in the refining of the items presented, it's important for the managers to be present to take advantage of their perspective and make sure that all the aspects of the organization are being addressed appropriately.

Create next steps

This step presents the end of the evaluation phase. All the data needed from the risk assessment is available now. The task now is to decide with the senior managers on what to do next, and determine how to apply the assessment's results. The method suggests the following questions to discuss with the senior managers:

- What will your organization do to build on the results of this evaluation?

- What will you do to ensure that your organization improves its information security?

- What can you do to support this security improvement initiative?, What can other managers in your organization do?

- What are your plans for ongoing security evaluation activities?

This workshop should end with the decision of how to implement the protection strategy, risk mitigation plans, and action list by determining the following [11]:

- what steps will be taken after the evaluation,

- who will be responsible for the next steps,

- when these steps will be completed.

3.5 Existing comparing frameworks

The main reason behind the number of risk assessment methodologies developed throughout the years, is the importance of risk assessment as a process. Another reason for that would be the absence of a unified method that would fit the different organizations no matter the size, the nature or the expertise. However choosing between these methods is not an easy task, also the absence of an agreed upon comparing framework for these methods makes the decision even harder. Nevertheless, there have been some studies and research papers that try to compare some of the methods and their features. The study looked through the following propositions:

3.6 Information Security Risk Assessment:A Method Comparison

The first proposition is information security risk assessment: a method comparison, by Gaute Wangen. The idea behind this work is to compare the effectiveness and the accuracy of his framework CURF, which is a framework created as an all-inclusive approach to compare different information security risk assessment methods. The framework itself is interesting, but the study mentions the work of comparing its results to a real qualitative approach that was proposed by him and his colleagues at the Norweigian university of science and technology (NTNU), The CURF framework is based on eleven ISRA methods, but the qualitative research that was proposed by the department was based on three methods, Octave A, ISO/IEC 27005:2011 and the Norwegian National Security Authority's (NSM's) Guidelines in Risk and Vul- nerability Assessments (NSM- ROS).

Gaute Wangen claims that the other frameworks that compare the ISRA methods use an evaluation that proceeds from the criteria at the top to methods at the bottom, which makes it difficult to determine the cause-effect relationships between method and results. While his proposed method which is CURF does the opposite by using the bottom-up approach which he claims it solves this problem by providing a way to review each ISRA method regardless of the predetermined criteria. The method also structures its tasks within ISO27005's risk management process.

The case study was in a form of a project, conducted by a group of students as part of an undergraduate ISRM course, the students were divided into 3 groups where each group had 6 to 10 students, all groups were giving 6 weeks of basic ISRA training and were provided with project supervision from associate professor, a doctoral researcher and a student assistant, the students also had access to an ISRA expert who is the NTNU's chief information security advisor. Each group applied one of the ISRA methods and used as supporting material, the method's primarily documents that outlined process steps, the documents appendices and they had access to supplemental literature plus the open sources.

The output of this project was the sum of the findings from each group as a formal report that was presented to various system and process stakeholders. The report

contained identified risks, an analysis of those risks and proposed treatments.

The project did not focus only on the results of each ISRA method, but also on the user experience. A survey was designed to reflect the experience of the students applying the method in terms of their satisfaction with the method, usefulness and the extent of the need to use the supporting literature to apply it. Without getting into the details of how the qualitative data was handled, the figure 3.17 summarizes the results.

Figure 3.17: Findings of the survey [43]

Method	Advantages	Disadvantages	Supplemental material needed
OCTAVE A	Adaptable; systematic, comprehensive process; worksheets easy to use once learned; focus on organizational drivers	Hard to learn and understand; probability not prioritized; too rigid	Probability estimates; asset evaluation; threat identification; ISRA explanations in native language
ISO27005	Detailed descriptions; well structured; easy to use as a comprehensive reference	Heavy reading; hard to grasp; much information irrelevant for a single ISRA project	Threat assessments; probability and consequence estimates; terminology definitions and ISRA explanations in native language
NSMROS	Well-defined and well-explained process; straightforward introduction to ISRA; tasks easy to distribute; written in Norwegian	Task description too generic; no examples; vague estimation metrics	Templates; examples; how to conduct an ISRA; scoping tools

The main idea behind this experience is to compare the four methods based on a specific tasks selected from the ISRA reports, each of the methods were given a completion score ranges where 0 to 2 refers to not addressed, 3 to 5 partially addressed, and 6 to 8 with fully addressed. The figure 3.18 elaborates the values assigned to each method for each task.

Figure 3.18: Completion score for every task [44]

Report or assessment area	Tasks	OCTAVE A	ISO/IEC27005	NSMROS	Completeness score (row)
Case description	Organizational drivers	6	2	4	12
	Risk management criteria	8	8	7	23
	Organizational goals and business objectives	5	8	4	17
	Completeness score for case description	19	18	15	—
Risk identification	Stakeholder identification	8	8	8	24
	Asset identification	8	8	6	22
	Asset evaluation and criticality	8	8	3	19
	Asset container identification	7	3	0	10
	Threat identification	8	8	4	20
	Threat assessment	3	8	1	12
	Areas of concern and vulnerability identification	8	8	8	24
	Vulnerability assessment	0	8	5	13
	Control identification	0	8	4	12
	Control assessment	0	6	0	6
	Outcome identification	8	8	8	24
	Completeness score for risk identification	58	81	47	—
Risk estimation	Impact-area prioritization	8	3	4	15
	Threat motivation	6	7	0	13
	Threat capability (know-how)	0	1	0	7
	Threat capacity (resources)	1	1	0	7
	Qualitative consequence estimation	8	8	8	24
	Qualitative probability estimation	7	8	7	22
	Risk scenarios	8	8	8	24
	Risk matrix or table	6	7	7	20
	Completeness score for risk estimation	43	55	34	—
Risk evaluation and treatment	Risk prioritization	8	8	7	23
	Treatment plan	8	8	8	24
	Cost–benefit analysis	8	8	6	22
	Residual risk	4	6	4	14
	Completeness score for risk treatment	28	30	25	—
Completeness score for all 26 tasks and subtasks		148	184	121	—

3.7 Comparison of risk analysis methods Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide

The second proposition is a research paper by Amril Syalim, Yoshiaki Hori and Kouichi Sakurai, the authors chose to compare four risk assessment models which are Mehari, Magret, NIST800-30 and Microsoft's Security Management Guide. The comparison was based on two criteria, the first criterion is the steps that each method introduces to conduct risk assessment, and the second criterion is the content,documentation and the supporting material that each method provides. After going through each method and the steps introduced in them, the authors suggest that although each method has its different steps whether in terms of content or number, all four methods follow the three general risk assessment steps:

- Threat identification
- Vulnerability identification
- Risk determination

However the following three methods, Mehari, Magerit and Microsoft Security Management Guide do not include the control recommendations, it's introduced in the next step after risk analysis in the risk management process. This was the author's conclusion when it comes to the steps introduced by each method. In terms of documentation and supporting materials, the authors say that all the methods provide a detailed guide for risk assessment, but only Mehari, Magerit and Microsoft Security Management Guide provide supplementary documents that help with the process of risk assessment [42].

3.8 A conceptual framework of info structure for ISRA

The next proposition is a framework suggested by Palaniappan Shamala, Rabiah Ahmad and Mariana Yusoff. The idea behind this article is to create a frame-

work to compare six information security risk assessment methods, which are: CRAMM, CORAS, OCTAVE, ISRAM, ISRA on BM and NIST 800-30. What this article provides is an info-structure framework that depicts the sum of data that each ISRA method requires in order to be conducted, in other words, this framework will allow the organization to have an idea of what information the ISRA method requires, and since most of the ISRA methods tasks are being conducted in teams or require participants, the organization will have an idea based on the skills of the personnel or the scope specified on which method will be best suitable for it, without the need to do the study.

In this research paper the study conducted was based on six phases, where the first phase was deciding the six methodologies that will be the subject of this research, second phase was dividing the ISRA methods into four main features namely, management requirement, establishment of organizational context, identification of assets, threats and vulnerabilities, and risk management improvements [39].

The info-structure framework was created through two comparative studies. The first study concluded that all the subject methodologies have common features, however based on the first study, the author concluded that each of the methods have been created to serve a specific goal, thus the following features :

- risk model/phase,
- steps and structure,
- tiers involvement,
- involvement of people in management,objectives
- ways of information gathering techniques
- level of application
- objectives
- ways of information gathering techniques

- level of application

Are considered to be different and unique for each method. The second study was dedicated to define sub-features for each main feature mentioned earlier. This study concluded that all practitioners must have the skill, qualification, experience and training to collect the needed information for the assessment and to perform the evaluation tasks further in the process. In addition to that, management input is important to validate the initial step of ISRA. The sub-features selected for each feature are the following:

Management requirement:

- Practitioners need to be qualified, experienced and trained
- Needs of business, operation and IT/IS risk assessment document
- Management input

Organizational context

- Objectives/goals
- Scope and boundary of the security review SWOT analysis
- Information about critical assets
- Current security practices/requirement

Identification of assets

- Information asset
- Data assets
- Physical assets
- Software assets

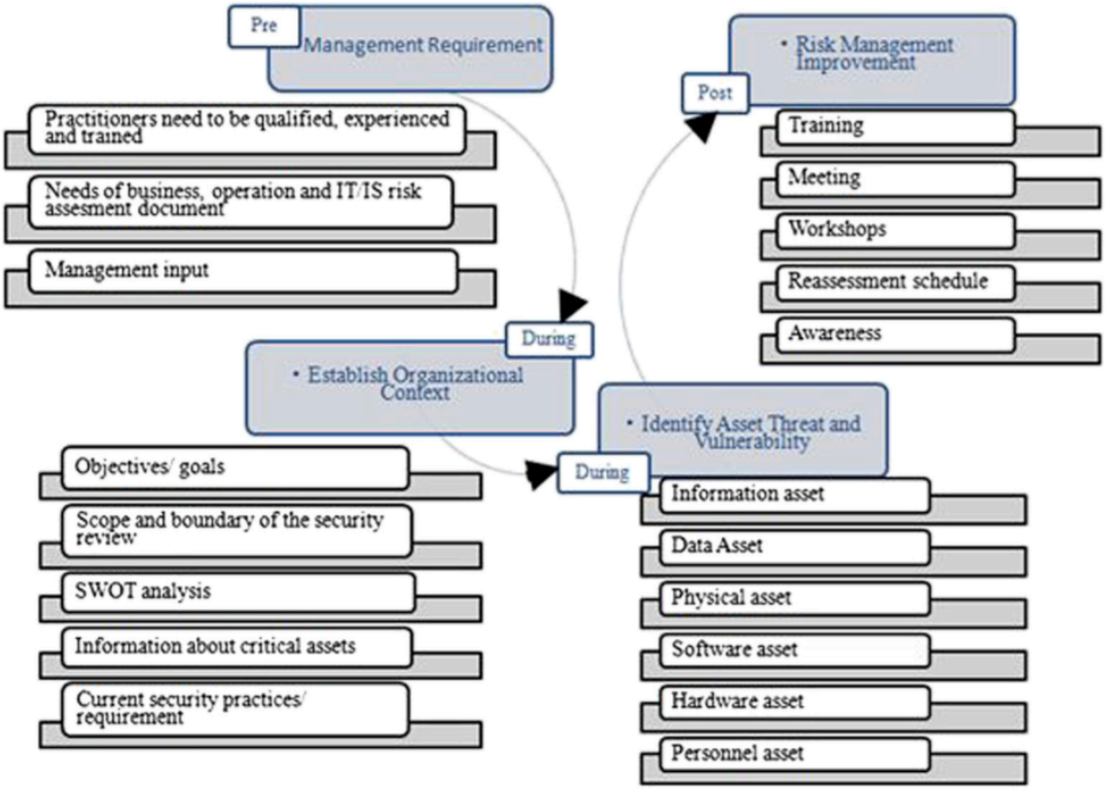
- Hardware assets
- Personnel assets

Risk management improvements

- Training
- Meeting
- Workshops
- Reassessment schedule Awareness

For threats and vulnerabilities, the author claims that the ISRA practitioners have considered the relationship between critical assets, the threats to those assets and the vulnerabilities that can expose these assets to threats. In general all organizations will have a similar list of critical assets but the threats to these assets will vary based on the scope of the information security of the organization. The figure 3.19 depicts the concept of the info-structure for ISRA.

Figure 3.19: ISRA info-structure [37]



The author describes the main goal of this study and the info-structure framework as a general view of flow, types of information to be gathered and requirements to be met before any risk assessment is conducted. The authors suggest that this framework can be used to complete all the required planning followed by selection of suitable methodologies [39].

The figure 3.20 depicts the comparison of the six methodologies conducted in phase 5:

Figure 3.20: Method comparison [38]

Elements/Features		ISRA methodologies					
		Professional organization			Research project		International organization
		CRAMM	CORAS	OCTAVE	ISRAM	ISRA on BM	NIST 800-30
Management requirements							
Practitioners need to be qualified, experienced and trained		√	√	√	√	√	√
Needs of business risk assessment document		√	√	√	√	√	×
Needs of operational risk assessment document		×	×	√	√	√	√
Needs of IT/IS risk assessment document		×	√	√	√	√	√
Management input		√	√	√	√	√	√
Establish organizational context							
Objectives/goals		√	√	√	?	√	√
Scope and boundary of the security review		√	√	√	√	√	√
SWOT analysis		√	√	√	√	√	√
Information about critical assets		×	√	√	√	×	√
Current security practices/requirement		×	√	√	√	×	√
Information related to the operational/business function		×	√	×	×	√	√
Schedule and deliverables		√	×	×	×	×	×
Person who use/support the IT system		×	×	×	×	×	√
Identify assets threats and vulnerabilities							
ASSETS	Data asset	√	?	√	?	√	√
	Software asset	√	?	√	?	√	√
	Information asset	√	?	√	√	√	√
	Physical asset	√	?	√	?	√	√
	Personnel/people	√	?	√	?	√	√
	Hardware asset	√	?	√	?	√	√
	Various facilities assets	√	?	√	?	√	?
Risk management improvement							
LACK	Training	√	√	√	√	√	?
	Meeting	√	√	√	√	√	?
	Workshops	√	√	√	√	√	?
	Reassessment Schedule/Updating risk	√	√	√	√	√	?
	Risk monitoring	×	×	√	√	√	?
	Awareness	√	√	√	√	√	?

√-Fulfils criteria.
×-Does not fulfil criteria.
?-Could not find in the documents whether fulfils or does not fulfil.

3.9 Comparative Study of Information Security Risk Assessment Models

The next proposition is a comparative study that has been done by Filipe Macedo and Miguel Mira da Silva. The study consists of comparing a number of information security methodologies. . The process of this study was the following:

- Widely explore the risk management theme and identify existing information security risk assessment models.
- Select the models that will be subject of detailed comparison based on concise criteria.
- Thorough study of each information security risk assessment model, aiming to produce a comparative analysis.
- Model comparison based in the theoretical study made until this point.
- Case study in a real organization (implementing the studied models).
- Comparison of the theoretical study and case study results.

The author understood the size of the data concerning the ISRA methodologies and the appropriate documentation for each one of them, so they decided to focus on the methods that fit a certain criteria. The initial list that the authors considered for the study was the following: (OCTAVE, Mehari, MAGERIT, IT-Grundschutz, EBIOS, IRAM, SARA, SPRINT, ISO 27005, NIST SP 800-30, CRAMM, MIGRA,MAR, ISAMM, GAO/AIMD-00-33, IT System Security Assessment, MG-2 and MG-3, Dutch A and K Analysis, MARION, Austrian IT Security Handbook, Microsoft's Security Risk Management Guide and Risk IT). The first criteria used to downsize the original set of methodologies :

- The model has to be a method and not a guideline or a framework
- The method has to acknowledge and identify information security risks.

- The documentation and supporting materials has to be available and free.

- The method has to be relevant nowadays and not obsolete or discontinued.

This selection shortlisted the methods to six models, which were OCTAVE, EBIOS, MAGRET, IRAM, IT-Grundschutz and Mehari. The second set of criteria that the author applied on the new selection were the following:

- Complexity, Effort and preparation (this criterion tries to reflect the level of preparation, information, effort and skills needed to implement the model, and the level of detail and scope of the risk analysis results)

- Approach of the model (the risk assessment approach each model advocates (e.g. self- assessment, interviews, workshops)

- Tool (if the model provides supporting tools and how can we obtain them)

- Origin (in this study three possible sources for a model were considered: Academic, Governmental or Commercial)

- Geographical spread (countries in which the model is known to have been implemented)

Applying these criteria to the subject set of models lead to three final methods: OCTAVE, IRAM, IT-Grundschutz. And the last criteria that were applied are: *Concept definition:* The author claims that the three models don't diverge, thus this criterion does not make a difference in comparing between them.

Approach to information security risk assessment: The author claims that OCTAVE is considered to be a simpler approach due to the absence of technical details and taking a business perspective, which makes it suitable for smaller teams, also it's adaptable measures that can be customized based on the organizational needs. On the other hand, IRAM is considered more complex, it focuses on information systems which makes it more technical but still business-centered. IRAM uses a workshop approach with interviews and questionnaires.the author also considers it adaptable. The author claims that IT- Grundschutz takes a traditional approach and provides some supporting material, such as a list of relevant threats and re-

quired countermeasures, however the method is considered more complex as it helps organizations to establish an information Security Management System.

Results and output: for this criterion the author explains that OCTAVE being the simplest model, It does not provide much information. It only provides the essential on critical assets and relevant risks to these assets, while IRAM and IT-Grundschutz produce the same output but more detailed and in different ways. In addition to that, IRAM produces detailed reports with threats, vulnerabilities and security requirements. whereas IT-Grundschutz calculates the IT security level of the organisation and suggests technical recommendations.

Complexity: For the last criterion the author claims that OCTAVE is the model that requires the least preparation, while IRAM is more detailed and requires more preparation and higher level of expertise, and lastly IRAM being very detailed, requires more preparation and expertise than both and also takes more time to conduct [27].

4 Results

4.1 The Criteria

The decision of conducting risk management within an organization is a big commitment, it takes a lot of time and resources. Part of this decision is determining which method to use for the risk assessment phase. Each organization is different, and has particular criteria, and so are risk assessment methodologies. Each methodology was created to serve a specific goal and fulfill specific needs. On today's market, there are a lot of methodologies, some are from professional organizations and some are from independent researchers. So in order for an organization to choose which methodology to go with, a study takes place, and this study is proper to the nature of the organization. This study suggests some criteria that an organization might find interesting to look into in these methodologies, and help deciding or narrowing the scope for selecting the appropriate methodology.

4.1.1 Terminology

Information security risk assessment is a broad topic, it touches base with multiple aspects of the subject structure, and usually tries to engage a number of the organization's personnel, they usually come from different backgrounds and hold different sets of skills. The different risk assessment tasks usually collect information from the participants, whether through questions or brainstorming sessions. The feedback required from the participants is related directly to their understanding of the situation.

The terms used during the process are not exclusive to information security or IT, they're being used in many different fields, however the meaning of these terms can be different in the IT world. Due to this predicament, terminology in risk assessment is a point of discussion, and the participant's conception of these terms usually affect the results of the tasks.

4.1.2 Is the methodology based on any standards

The term standards in IT is a set of rules and regulations that are advised to follow in order to insure a certain outcome or to regulate a certain practice. There are a lot of technical standard organizations, and ISO being one of the most famous ones. depending on the size and the nature of the organization, there are usually a number of standards involved, it could be international standards, national standards, information standards, etc.., having a method that is based on a certain standard can be a way of understanding the structure of this method and how compatible it could be with the organization.

4.1.3 Techniques used in the process

Most of the methodologies tend to collect some sort of information at some point in the process, and each one of these methods uses one of the data collection techniques such as, interviews, surveys, focus groups, etc. Some organizations might prefer one technique over the other, so this can be a criteria for the study.

4.1.4 How big is the preparation phase

generally most of the Risk assessment methods consist of two phases, the preparation phase and the analysis phase. Where the preparation phase consists of putting together all the necessary material while the analysis phase consists of evaluating and assessing the findings. The size of the preparation phase can provide an idea about the proportions of the methodology.

4.1.5 How involved are the organization's personnel

One of the Key selection criteria in the risk assessment methodologies is whether the tasks require internal or external expertise, this criterion can be conclusive for some organizations. Risk assessment or risk management in general is a project that management allocates a budget for, and whether to hire external expertise or not can be a decisive criterion.

4.1.6 How accessible the method is to the participants

Risk assessment methodologies vary in terms of complexity and skills requirements. Understanding the required skills to conduct its tasks is an important aspect to consider before going forward with a certain methodology.

4.1.7 What sort of documents the method provides

Every methodology provides some sort of material that would help the user understand the structure of the method and describe the overall process. These materials are usually in the form of documents, and sometimes tools.

4.1.8 The formula used for risk

Risk is usually represented as a formula, however not all methodologies identify risk as a value, depending on the type of the method (qualitative or quantitative) some methodologies represent it as an interval of qualitative values such as high, medium and low. The formula that's being used can be an indication of the complexity of the method and the type of calculation that an organization should expect from it.

4.1.9 Nature of the methodology

Risk assessment methodologies are categorized based on their nature, the method is considered quantitative, if it uses numeric values and qualitative if it uses terms to describe the value (high-medium-low). The quantitative type tends to be more in depth and more accurate, but on the other hand this requires specific values and heavy calculation compared to the qualitative type. Each of these criteria will applied to the selected methodologies suggested by the study and the finding are as follows.

4.1.10 CORAS

Terminology

when it comes to coras, the terminology is part of the coras project but not the actual methodology, the coras framework is divided into three parts: Library, terminology and methodology, so Coras as a project gives great importance to the terminology and place it at the same level as the methodology along side with the library in the Coras framework, in one hand the terminology used in the CORAS project is based mainly on accepted standards of security and risk management, which means that a large portion of scholars and researchers are using the same terminology which means that there's a community that can back up and help maintaining the method. In other hand the terminology has been tested over several years through both scientific publications and by interviewing several people of various backgrounds on their understanding of the CORAS concepts. The CORAS Model-based Method for Security Risk Analysis page 5

Is the methodology based on any standards

In risk management, the CORAS method takes into consideration the Australian/New Zealand Standard for Risk Management, AS/NZS 4360:2004 (curently replaced by ISO/IEC 27005), the ISO/IEC 17799 (currently replaced by ISO/IEC 27002) Code of Practice for Information Security Management (currently known as ISO/IEC 27002), the ISO/IEC 13335 Guidelines for the management of IT-Security which was withdrawn. However these standards are considered outdated considering the time this method was created. In terms of system documentation, the CORAS method presents them in the form of the Reference Model for Open Distributed Processing.

Techniques used in the process

During the preparation phase, the tasks are conducted during meetings among the analysis team and some additional technical participants when needed, during these meetings, the information collected is presented using UML, in the form of asset diagrams, threat diagrams, risk diagrams.

How big is the preparation phase

As it was mentioned, the CORAS method is conducted through 8 steps, and if we consider the preparation phase as all the tasks that lead to the analysis phase, we can say that phase 1 to phase 5 in CORAS are the preparation phases which present more than half of the process.

How involved are the organization's personnel

When it comes to CORAS, the method suggests that a team of analysts should be assigned to conduct the five steps, and it's advised that the team should be diverse and knowledgeable about security. So the team conducting the method is internal, meaning that there's no need for external expertise to conduct the method.

How accessible the method is to the participants

the CORAS method was designed to be conducted by internal participants, which means, there's no need to hire external expertise, so the method is considered somewhat accessible, also the method is model based, so most of the outputs from the workshops are represented as UML diagrams such as asset diagrams, threat diagrams, risk diagrams and treatment diagrams. Which is a very comprehensive way of presenting the findings of the workshops and an easy way to keep the participants connected to the tasks and easy to pick up in case of misunderstanding or confusion.

What sort of documents the method provides

the official website for the method is somewhat informative, with a link to the publication related to the method , there are also a few material available on the internet such as, the book "Model-Driven Risk Analysis the coras approach" 2011 edition and The CORAS Model-based Method for Security Risk Analysis which is more of an official supporting document for the CORAS method, however both of these documents have not been updated in a while now.

The formula used for risk

The coras method is considered a qualitative method, meaning that the values given to risks are in the form of intervals (low-medium-high) rather than concrete numbers. So there's no formula used in the CORAS method.

Nature of the methodology

The CORAS method is considered qualitative of nature, does not rely on any numerical data, and risk is not evaluated based on a formula or numeral values.

4.1.11 OCTAVE

Terminology

The creators of the CORAS project method understood the importance of terminology and the challenges it brings to the table, so they gave it a great importance and presented it in the same level as the library and the methodology in the CORAS framework. So the absence of the terminology aspect in octave can be considered a weakness, however The method introduces a brief definition of some of the terms, but I think that is not enough. Maybe the analysis team should emphasize more on the key terms that will be used in the workshops to have a common understanding of them and avoid any misconception that can lead to incoherent results.

Is the methodology based on any standards

It's not mentioned if the method is based on any official standards.

Techniques used in the process

There aren't any specific techniques that the method suggests in terms of collecting information, however, it suggests brainstorming in most of the workshops.

How big is the preparation phase

Considering that the preparation phase in the method is all the tasks that must be conducted before starting the analysis, the octave method allocates the first two phases for the preparation, and the third phase is dedicated to risk analysis.

How involved are the organization's personnel

The octave method is based on the self-directing concept, meaning that the analysis team is part of the organization and all of the participants are members of the organization. No external expertise is used during the process.

How accessible the method is to the participants

The method itself is not very complicated, since it's a qualitative method and does

not use any formulas to calculate risk, which makes it accessible to most of the organization personnel, however some of the tasks in the workshop require some technical skills, and some security knowledge. Meaning that in order to conduct the method the analysis team should be somewhat knowledgeable about security and also some basic IT skills. For a basic system user, some of the tasks can be challenging, and this is something that the analysis team leader should be aware of, when choosing the participants.

What sort of documents the method provides

the book managing information security systems an octave approach gives a detailed description of the method and the language used is very understandable. The Method also provides some supporting documents that are useful during the assessment such as a list of security controls that can be used during the workshops, the MedSite use case with a final report, generic threat profiles, etc.

The formula used for Risk

As It's mentioned before, the method is considered qualitative, meaning that the typical process does not depend on a formula or a risk value to do the analysis, however, the octave method provides an option of incorporating probability into the mitigation plane, but also in an interval value, without any quantitative data.

Nature of the methodology

The method is considered qualitative since it does o't handle any quantitative data, however the method has the option of incorporating probability into the mitigation plan with interval values.

4.1.12 ISRAM

Terminology

the method does not really mention the topic of terminology, or suggests any discussion about the understanding of the key terms used in the method.

Is the methodology based on any standards

the method does not specify any standards that it might be based on. however the used formula to calculate the single risk value is based on the the fundamental risk formula (NIST, 2001;McEvoy and Whitcombe, 2002;USGAO, 1999)

Techniques used in the process

as mentioned before, the ISRA method is considered a hybrid method, combining both qualitative and quantitative concepts. The qualitative part that relies on collecting data from the participants is conducted using surveys, where the questions are created during step 3.

How big is the preparation phase

it's is safe to say that the preparation phase is the process from step one until step seven, starting from the fact of acknowledging the need for risk assessment, all the way until applying the formula and obtaining the single risk value.

How involved are the organization's personnel

the method is considered more complicated that the other methods, since it uses mathematical formula and calculates risk values, however it's designed to be conducted by internal participants and it allows staff members and management to get involved in the process

How accessible the method is to the participants

the method is designed to assess complex IT systems and the quantitative part that consists of applying the formula is not an easy task, it takes some technical skills and some training to match the figures and collect the arguments from the surveys, so the method is somewhat complex and requires some training in both the IT part for non technical personnel and also some mathematical knowledge to apply the formula and to extract the data from the surveys.

What sort of documents the method provides

Compared to the other methods such as FRAP in terms of providing supporting documents like security controls list or OCTAVE in providing prototypes of threat profiles, ISRA method does not provide any material that would help the practitioners during the tasks.

The formula used for Risk

The method is considered a hybrid method which is part quantitative and part qualitative, a formula is used to obtain the single risk value based on the values collected from the surveys.

Nature of the methodology

It's a hybrid, which means the method is considered both qualitative and quantitative, by combining collecting data in forms of surveys and applying a formula on the findings to obtain a numerical value as a single risk value.

4.1.13 FRAP

Terminology

The method does not emphasize on the matter of terminology in a direct manner, however it focuses on 5 key terms that will be used in the process. The method gives a brief definition of each of them. I don't think that these brief definitions are enough, the risk assessment process is a wide topic that touches bases with a lot of IT aspects. Terminology is something that the method should give more importance to, since most of the tasks require some sort of feedback from multiple personnel of the organization that also come from different departments and backgrounds.

Is the methodology based on any standards

The method does not mention any standards that were used as a basis during its development.

Techniques used in the process

The workshops in the method use a brainstorming approach to collect point of views of the participants, under the assistance of the FRAP facilitator.

How big is the preparation phase

Most of the FRAP method can be considered a preparation phase, since it's structure is based on reviewing the existing controls and cross reference them with the identified risks mentioned during the brainstorming sessions. What would be considered an analysis is the creation of the final report, where the project lead and the business manager get together to determine which controls will be most effective and who will implement them and by what date.

How involved are the organization's personnel

The FRAP method relies completely on the internal expertise, all the participants including the FRAP facilitator is a member of the organization, however, the method suggests that the participants should have a specific set of skills, in order to achieve the expected results.

How accessible the method is to the participants

Although, the FRAP method suggests that no external expertise is needed to be in the team, some of the tasks require technical skills and security knowledge, not everyone would be suitable to participate, the FRAP team should be selected carefully and includes technical expertise.

What sort of documents the method provides

The FRAP method is considered a research method, it was not created by an organization, so the documentation is not as rich and diverse as other methods, however the FRAP method provides some use case example to help understand the steps and have an idea about what sort of output you can expect from it. Some of the supporting material would be the control list that the method provides to use during the FRAP session,and also an example of the final report, how it is supposed to look like and what information it's advised to have.

The formula used for Risk

The FRAP method is considered qualitative, it does not use any numerical values. The risks are being assigned letters as a form of classification. Therefore the method does not use any formula to calculate risk.

Nature of the methodology

As it was mentioned before, the FRAP method does not handle any calculation nor numerical values, it's considered a qualitative method.

5 Discussion

5.1 Comparison

There are a lot of risk assessment methods that are circling the market and being used by different organizations. Some of these methods are created by professional organizations,and some are the work of independent researchers. The reason behind this number of methodologies and approaches is maybe that the method creators noticed something missing from the other methods, or maybe some of these methods have overlooked a certain aspect, or did not deliver accurate results.

The methods that have been subject to this study are considered different in nature, characteristics, structure and tasks. However they all share the same need to identify risks and the appropriate arguments for the organization to use to evaluate them and be able to choose which risks to accept and which to mitigate. The criteria that were suggested to be applied on these methods are related to different aspects of the risk assessment process. These criteria give a scope on the composition of the method and what you can expect from it, and also what the method expects from the organization applying it.

The first criterion is the Terminology, which we can see that the four methods have different perspectives on. The CORAS project, for example, gives great importance to it, by aligning it in the same level as the methodology, which means that CORAS acknowledges the issue that the misconception of the terms used in risk management in general, can be a challenge and can affect the results of the process. Evoking the topic will raise awareness among participants to pay attention to their inputs, and not provide broad or inconsistent information during the workshops. Conducting risk assessment among participants that are fully aware of the meaning of each term in the security context ensures the reliability of the data collected and promotes accuracy in the final results.

The second criterion is whether the method is based on any recognized standards. Taking in consideration the agreed upon standards and best practices, gives the

method a certain credibility and consistency for its structure, on the other hand a lot of organizations base their systems and structure on recognized standards, which can be a common ground to decide on the appropriate method for the project.

The third criterion is the technique that is being used to collect data during the preparation phase, this criteria is not very critical since most of the methods provide some customizing space, depending on the organization, however it can show how the participants are supposed to interact with each other during the workshops or meetings.

The fourth criterion is the proportion of the preparation phase, usually the tasks suggested by the method are responsible for the size of the data that needs to be collected, the more data you have and the more diverse it is, the more accurate and consistent the results will be. However the density of the preparation phase is also related to the amount of work that the method expects, if the organization is not ready to allocate such ressources, a method with miniature preparation phase would be more suitable for it.

The fifth criterion is the involvement of the team, some of the methods rely on the organization's expertise to conduct the tasks, and some suggest external participants to lead the assessment. If the organization is ready to invest in the project and willing to hire external expertise, that would boost the accuracy and efficiency of the results, not all organizations have the necessary skills amongst their personnel to follow the risk assessment process, however the option of hiring external expertise raises the cost of the project. If the organization's budget is limited, or can not cover the extra costs, then a method that provides the option of using the internal expertise is the right choice.

The Sixth criterion is the supporting documents that the method provides. Some of the methods provide the blueprints to follow to achieve the final purpose, however, especially if the organization is going with internal expertise, some of the tasks are not the typical daily mission of these participants, especially the technical part, having additional instruments such as the security control list provided by the FRAP method or the generic threat profiles provided by OCTAVE can be very useful and overcome some challenges that the participants might face.

The seventh criterion is the formula used for risk calculation. When you hear cal-

culation, the first thought that comes to mind is numbers, this criteria concerns quantitative methods in particular, choosing a method that uses a specific formula to calculate risk means that the results will be more accurate and the evaluation will be supported by numerical figures which gives it a certain legitimacy, however handling the numbers and the calculations make the process more complex and time consuming. If the accuracy of the risk value is important to the organization, going with a quantitative method that calculates risks and presents it with numerical value is a good fit. And if the organization is less interested in the accuracy of the calculation rather than complexity of the process, then a qualitative method that represents risks as in non-numerical values is a better fit.

The final criterion is the nature of the method, whether it's qualitative or quantitative, generally quantitative methods tend to be more accurate but also more complex, while qualitative methods are supposed to be less accurate but also less complex. There is no wrong choice when it comes to this criterion, it depends on the organization purpose of this project, the resources allocated to it and the expected results from it. If the risk evaluation is expected to be sensitive and requires computable figures, then the quantitative nature would be more suitable for the cause, otherwise if the evaluation can settle for empirical data, then qualitative methods should be enough.

5.2 Further work

There is no question that information security risk management is a broad field and still has room for research and study. There is a lot of effort being put into improving the discipline and keeping it up to date with technology. Each new innovation or solution that is being offered to the public introduces new security gaps and challenges. This study aimed to contribute to this field and provide added value to the already existing work. However, there are still room for improvement and evolution, some of the ideas that would contribute to this study would be

Real case scenarios

Apply the methods on real case scenarios, that would result in findings that are based on real data and real use cases, and maybe use the same scenario for the different methods to compare them based on the results. In other words, compare the methods in terms of final rapports rather than just their documentation.

Actual feedback from practitioners

It would be very interesting to discuss the nature of each method with actual practitioners that have used it before, and get their feedback on the experience and the results, through a survey.

Automated tool

What would be a great addition to the field is an automated tool that takes as an input the characteristics of an organization, such as the size, the scope, the assets etc., and get as an output, the suitable method for it or a few suggestions that would narrow the search, and help the organization to skip the study phase.

6 Conclusion

Information security risk management is considered to be the backbone of information security within an organization, it gives a structured and well established process to approach the security posture of an organization, it revolves around risk, but it touch basis with every aspect of the establishment, it involves risks, assets, threats, vulnerabilities, human factor, it can even discuss forces of nature.

Risk assessment on the other hand is part of risk management but it's the step that requires the most effort and consumes the most resources. It's structured on steps where each step uses the findings of the previous one. The risk assessment process can be overwhelming and hard to carry out at once. For this reason, a lot of specialized organizations and researchers put together methodologies to organize the practise and make it more comprehensive. However, the absence of a certified or agreed upon method made it hard to choose or prioritize one over the other, also the absence of an official tool or a framework to benchmark the different methods puts a certain responsibility on the users of these methods. Knowing that the process consumes a decent amount of resources, choosing the right method is critical for a risk management project, and the act of experimenting with multiple methods can be a costly move. The purpose of this study was to break down a number of methods and identify a set of criteria that an organization should consider before choosing a method, and this can also be considered a prototype to a comparison framework that could replace the study that the organization conducts on the possible methodologies.

The four methods have a lot in common since they all serve the same purpose, which is to identify the risks that the organization faces with its current security status, these risks are presented in a way that would be possible to evaluate whether in a form of numerical values such in the case of ISRAMM or empirical values in the form of high, medium or low such in the case of OCTAVE.

The difference between these methods lies in what kind of data to use, how it's being collected and how it's being evaluated. The diversity of the methods does not mean that some are wrong and some are right but more in what case one method would be a better fit than the other. The circumstances involved in the selection

are related to the organization subject to the assessment, it's size, the scope of the assessment, the technical skills of the personnel, the budget allocated for the project, the resources available to the project, etc. The criteria that were mentioned in this study are an example of the features that define a method and make it unique. Some of these features serve accuracy, some thoroughness and some practicality. It is up to the organization to figure out which one to adopt for the project. The absence of a unified methodology gives a lot of room for more research and innovation, and because the nature of security risks is not static, creating new approaches and improving the existing methodologies is critical to keep up with novelties in IT in general and security in particular.

Bibliography

[1] The coras model-based method for security risk analysis. pages 73–78, 2006.

[2] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., USA, 2002.

[3] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., USA, 2002.

[4] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., USA, 2002.

[5] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., USA, 2002.

[6] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., USA, 2002.

[7] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., USA, 2002.

[8] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., USA, 2002.

[9] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., USA, 2002.

[10] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., USA, 2002.

[11] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., USA, 2002.

[12] Bob Blakley, Ellen McDermott, and Daniel E. Geer Jr. Information security is information risk management. In Victor Raskin, Steven J. Greenwald, Brenda Timmerman, and Darrell M. Kienzle, editors, *NSPW*, pages 97–104. ACM, 2001.

[13] A. Ekelhart, S. Fenz, and T. Neubauer. Aurum: A framework for information security risk management. In *2009 42nd Hawaii International Conference on System Sciences*, pages 1–10, 2009.

[14] Bjørnar Solhaug Ketil stølen Fredrik Vralasen Folker den Barber Gyrd Bændeland Heidi E. I. Dahl Iselin Engan Ida Hogganvik Mass S. Lund. The coras model-based method for security risk analysis. pages 2–3, 2006.

[15] Shon Harris and Maymi Fernando. *CISSP exam guide*. McGraw-Hill Education, 2019.

[16] Bilge Karabacak and Ibrahim Sogukpinar. Isram: information security risk analysis method. *Computers and Security*, 24(2):149, 2005.

[17] Bilge Karabacak and Ibrahim Sogukpinar. Isram: information security risk analysis method. *Computers and Security*, 24(2):150–151, 2005.

[18] Bilge Karabacak and Ibrahim Sogukpinar. Isram: information security risk analysis method. *Computers and Security*, 24(2):151–155, 2005.

[19] Mass Soldal. Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-Driven Risk Analysis The CORAS Approach*. Springer Berlin, 2014.

[20] Mass Soldal. Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-Driven Risk Analysis The CORAS Approach*. Springer Berlin, 2014.

[21] Mass Soldal. Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-Driven Risk Analysis The CORAS Approach*. Springer Berlin, 2014.

[22] Mass Soldal. Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-Driven Risk Analysis The CORAS Approach*. Springer Berlin, 2014.

[23] Mass Soldal. Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-Driven Risk Analysis The CORAS Approach*. Springer Berlin, 2014.

[24] Mass Soldal. Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-Driven Risk Analysis The CORAS Approach*. Springer Berlin, 2014.

[25] Mass Soldal. Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-Driven Risk Analysis The CORAS Approach*. Springer Berlin, 2014.

[26] Mass Soldal. Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-Driven Risk Analysis The CORAS Approach*. Springer Berlin, 2014.

[27] Filipe Macedo and Miguel Mira da Silva. Comparative study of information security risk assessment models. 2012.

[28] Thomas R.Peltier. Facilitated risk analysis process (frap). page 11, 2000.

[29] Thomas R.Peltier. Facilitated risk analysis process (frap). page 12, 2000.

[30] Thomas R.Peltier. Facilitated risk analysis process (frap). page 13, 2000.

[31] Thomas R.Peltier. Facilitated risk analysis process (frap). page 15, 2000.

[32] Thomas R.Peltier. Facilitated risk analysis process (frap). page 18, 2000.

[33] Thomas R.Peltier. Facilitated risk analysis process (frap). page 19, 2000.

[34] Thomas R.Peltier. Facilitated risk analysis process (frap). page 20, 2000.

[35] Thomas R.Peltier. Facilitated risk analysis process (frap). pages 1–5, 2000.

[36] Thomas R.Peltier. Facilitated risk analysis process (frap). pages 5–20, 2000.

[37] Palaniappan Shamala, Rabiah Ahmad, and Mariana Yusoff. A conceptual framework of info structure for information security risk assessment (isra). *Journal of Information Security and Applications*, 18(1):50, 2013.

[38] Palaniappan Shamala, Rabiah Ahmad, and Mariana Yusoff. A conceptual framework of info structure for information security risk assessment (isra). *Journal of Information Security and Applications*, 18(1):51, 2013.

[39] Palaniappan Shamala, Rabiah Ahmad, and Mariana Yusoff. A conceptual framework of info structure for information security risk assessment (isra). *Journal of Information Security and Applications*, 18(1):45–52, 2013.

[40] Mikko T. Siponen and Harri Oinas-Kukkonen. A review of information security issues and respective research contributions. *ACM SIGMIS Database*, 38(1):60–80, 2007.

[41] Bjørnar Solhaug and Ketil Stølen. The coras language – why it is designed the way it is. *Safety, Reliability, Risk and Life-Cycle Performance of Structures and Infrastructures*, page 3155–3162, 2014.

[42] Amril Syalim, Yoshiaki Hori, and Kouichi Sakurai. Comparison of risk analysis methods: Mehari, magerit, nist800-30 and microsofts security management guide. *2009 International Conference on Availability, Reliability and Security*, 2009.

[43] Gaute Wangen. Information security risk assessment: A method comparison. *Computer*, 50(4):56, 2017.

[44] Gaute Wangen. Information security risk assessment: A method comparison. *Computer*, 50(4):58, 2017.

[45] Evan Wheeler and Kenneth Swick. *Security Risk Management: Building*

an Information Security Risk Management Program from the Ground Up. Elsevier Syngress, 2011.