A Comparative Analysis on Risk Assessment Information Security Models

K.V.D.Kiran
Faculty
Vaddeswaram
GunturDt
KLEF University (K L U)

L.S.S.Reddy, Ph.D
ProVC
Vaddeswaram
Guntur Dt
KLEF University (K L U)

N.Lakshmi Haritha
Student
M.Tech 2nd Year
Mother Thersa Group of Inst,
Vijayawada

ABSTRACT

This study equates a choice of methods that allow an organization to weigh their information security risk. The initial models went through two selection iterations before we end up with the final three Risks assessment models. The main purpose of the study is to compare and clarify the different activities, inputs and outputs required by each information security risk assessment models and also analyze which ones address information security risk effectively. The resulting information helps evaluating the models' applicability to an organization and their specific needs. In order to verify and validate the conclusions taken from the theoretical study of the three final models, a practical experience was put into practice in a real organization.

Keywords

Risk Assessment Models, Information Security Risk

1. PROBLEM

Most of the organizations find it difficult and costly to deal with the Information Security in a proper way. When a new vulnerability or a new virus is recognized or detected, the consequences can be comprehensive on the fly. In addition, it is clear that interoperability between organizations is significant and will become more important in the future. To provide fast and suitable response to security incidents and to ensure interoperability between organizations, there is a need for a systematic and pre-defined tactic to deal with Information Security challenge.

2. INFORMATION SECURITY RISK ASSESSMENT

Information security risk assessment is the progression that identifies and valuates the risks to information security by defining the likelihood of occurrence and the resulting impact. It uniquely recognizes threats, categorizes assets and rates system vulnerabilities as it provides key information and strategies to implement effective controls. The following sections involve the discussion on Risk analysis and Evaluation and also describe the comparison analysis on assessment models through selection criteria.

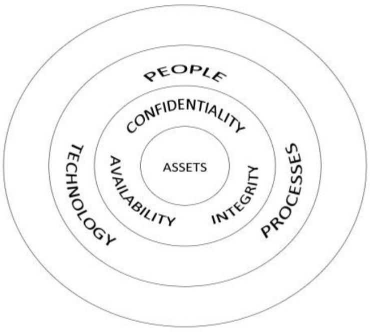

Fig 1 : Information Security

3. INFORMATION SECURITY RISK ANALYSIS

Risk analysis and identification generally involves:

i. **Identification of assets :** Information (databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, working or support procedures, business endurance plans, fallback arrangements, audit trails, and archived information);

   Software Assets (application software, system software, development tools, and utilities);

   Physical Assets (computer equipment, communications equipment, removable media, and other apparatus);

   Services (computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning);

   People, and their qualifications, skills, and experience; Intangibles, such as prominence and image of the organization.

ii. **Identification of legal and business requirements** relevant for the identified assets.

iii. **Collecting all policies, procedures and controls** currently in place. Assess whether or not the existing policies, procedures and controls implemented are satisfactory.

iv. **Identification of substantial threats or risk sources**. These threats can be fragmented into Human and Nonhuman elements. (Acts of nature, acts of war, accidents, among others malicious acts originating from inside or outside the organization).

v. **Identification of vulnerabilities for the identified assets**.

Asset is defined as whatever having value to an organization.

Threat is a latent cause of an unwanted incident, which may consequence harm to a system or organization.

Vulnerability is a weakness of an asset or group of assets that can be exploited by one or more threats. It is the susceptibility to injury or attack. In computer security, the term vulnerability is applied to a weakness in a system which allows an attacker to intrude upon the integrity of that system.

A **requirement** is a singular documented need of what a specific asset should be, do or respect.

Impact can be defined as the severity of the consequences of an event or incident. In the background of information security, the impact is a loss of availability, integrity, and confidentiality of information.

Likelihood is the probabilities of a threat to show up.

4. INFORMATION SECURITY RISK EVALUATION

Risk evaluation or estimation is the process used to assign values to consequences, their likelihood and to the level of risk. It involves:

i. Assessment of the probability of the threats and vulnerabilities to ensue;

ii. Calculation of the effect that each threat would have on each asset;

iii. Determination of quantitative (measurable) or qualitative (descriptive) value of risk.

One significant thing to take into thought is that these three variables rarely are independent from each other. In information security, there's a possible relation between asset value, impact and probability. For example, it's more likely a hacker will exploit a vulnerability that causes a bigger impact than one with small impact. Likewise, a valuable asset has more probability of being compromised than a valueless one. Therefore, in this field we have to take into consideration more than simply random or unintended acts. And besides this relation, we should remind ourselves that given enough time and determination, people can circumvent almost every security measure. Therefore this motivation factor should be seriously addressed in the information security risk assessment course.

In addition to this relation, new threats and vulnerabilities are unceasingly appearing and when considering risks to information infrastructures, the number, type, and variation are overwhelming. Despite being hard to keep up with all these new vulnerabilities and threats, they need to be managed satisfactorily or else the organization future and existence can be endangered.

5. A COMPARTIVE ANALYSIS ON INFORMATION SECURITY RISK ASSESSMENT MODELS

There are several models and methods with different approaches that aid in the risk assessment process. This study will address the methods that support the risk assessment process and those which can be applied to information security. Thus, methods that are not classified as risk assessment or risk management oriented or that are general management oriented (i.e. corporate governance) frameworks like Coso, Cobit or Basel II have been let off from the study.

Risk assessment models can be separated into quantitative and qualitative.

5.1 Qualitative vs. Quantitative Models

Risk assessment models can be parted into quantitative and qualitative. Quantitative models use measurable, objective data to determine asset value, probability of loss, and accompanying risk(s). The goal is to try to calculate objective numeric values for each of the components gathered during the risk assessment and cost-benefit analysis.

Qualitative methods use a relative measure of risk or asset value based on ranking or separation into expressive categories such as low, medium, high; not important, important, very important; or on a scale from 1 to 10. A qualitative model evaluates the impact and likelihood of the identified risks in a rapid and cost-effective manner. The sets of risks recorded and analyzed in qualitative risk assessment can provide a foundation for a attentive quantitative assessment. Both qualitative and quantitative approaches to security risk management have their advantages and disadvantages. Certain situations may call for organizations to implement the quantitative approach. Alternatively, organizations of small size or with limited resources will probably find the qualitative approach much more to their liking. The following table abridges the benefits and drawbacks of each approach:

Table1. Benefits: Quantitative vs. Qualitative

Quantitative	Qualitative
• Risks are prioritized by financial impact; assets are prioritized by financial values. • Results facilitate management of risk by return on security investment. • Results can be expressed in management-specific terminology • Accuracy tends to increase over time as the organization builds historic record of data while gaining experience.	• Enables visibility and understanding of risk ranking. • Easier to reach consensus • Not necessary to quantify threat frequency. • Not necessary to determine Financial values of assets. • Easier to involve people who are not experts on security or computers.

Table2. DrawBacks: Qualitative vs. Quantitative

Quantitative	Qualitative
• Impact values assigned to risks are based on subjective opinions of participants. • Process to reach credible results and consensus is very time consuming. • Calculations can be complex and time consuming. • Results are presented in monetary terms only, and they may be difficult for non-technical people to interpret. • Process requires expertise, so participants cannot be easily coached through it.	• Insufficient differentiation between important risks. • Difficult to justify investing in control implementation because there is no basis for a cost benefit analysis. • Results are dependent upon the quality of the risk management team that is created.

6. EXISTING MODELS

6.1 Introduction

This chapter elucidates clearly how the study was carried out. It exposes the methods and processes used to do the comparative study starting with a substantial list of information security risk models. The chapter includes a thorough study of the most relevant models and a comparison between those same models.

6.2 Model Selection

There are several models and methods that help in the risk assessment process. This study will address the methods that support the risk assessment process and those which can be practical to information security. This model provides an outline of existing Information Security Risk Assessment methods, and a comparison that evaluates those different methodologies. It aims to describe and compare properties of Information Security Risk Assessment methods in a concise manner. Unless otherwise stated, the words “model” and “method” are used in this document to refer to an “information security risk assessment method or model”, though often times the full phrase is also used.

After a period of some research some models were identified as suitable for evaluating information security risk. These models are the following:

i. OCTAVE
ii. Mehari
iii. MAGERIT
iv. IT-Grundschutz
v. EBIOS
vi. IRAM
vii. SARA
viii. SPRINT
ix. ISO 27005
x. NIST SP800-30
xi. CRAMM
xii. MIGRA
xiii. MAR
xiv. ISAMM
xv. GAO/AIMD-00-33
xvi. IT System Security Assessment
xvii. MG-2 and MG-3
xviii. Dutch A&K Analysis
xix. MARION
xx. Austrian IT Security Handbook
xxi. Microsoft’s Security Risk Management Guide
xxii. Risk IT

As was stated before, this is a non-exhaustive list.

General Information (includes Name, Website, Owner, Country)

Description (a brief description of the method and its approach)

Target Organizations (the model was created to be used in this kind of organizations)

Risk estimation method (quantitative or qualitative risk level estimation?)

This list of characteristics is limited to the specific purpose of this study and does not presume the quality (i.e. efficiency and effectiveness) of the products.

6.3 First iteration selection criteria

The first selection iteration plays to exclude some of the models based in a criteria described below. These criteria assess four essential model features. If a model doesn’t hold any of those properties it will be excluded from the universe to study.

The criteria used in this selection iteration are the following:

i. **Method/Guideline**

Is the model really a method? Or just a standard or guideline?

Method is defined as an orderly arrangement of parts or steps to achieve an end, a regular and systematic procedure of accomplishing something.

Guidelines are advice or instructions given in order to guide or direct an action. A standard is a set of rules widely recognized or engaged (especially because of its excellence) that control how people develop and manage materials, products, services, technologies, tasks, processes, and systems.

Exclude the model if it isn’t a method.

ii. **Identifies Information Security Risks**

Does the document identify Information Security Risks?

Information security means guarding information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

The Security Risk level of a system is a mixture of the importance of maintaining the Availability that system, the Integrity of data housed on or managed by that system and the Confidentiality of sensitive information deposited on that system.

Exclude the method if it doesn’t identify Information Security risks.

iii. **Price and availability of documentation**

Is the information publicly available sufficient to properly evaluate and compare the model with others? Does the information comfort to answer all criteria questions?

What’s the assessed price to obtain all documentation and tools needed to implement the model?

iv. **Last review**
When was the model last revised or updated? *Exclude if discontinued, obsolete or not updated/reviewed in more than a decade.*

6.4 Criteria applied to each model

After the defining the selection criteria, each model was scrutinized and evaluated using those criteria.

NAME	Method or Guideline?	Identifier IS Risks	Documentation?	Last Review	2nd Iteration?
OCTAVE	Method	Yes	Free	Up-to-date	Yes
Mehari	Method	Yes	Free	Up-to-date	Yes
MAGERIT	Method	Yes	Free	Up-to-date	Yes
IT-Grundschutz	Standard and Method	Yes	Free	Up-to-date	Yes
EBIOS	Method	Yes	Free	Up-to-date	Yes
NIST SP800-30	Guideline	Yes	Free	Up-to-date	No
CRAMM	Method	Yes	Expensive	Up-to-date	No
MIGRA	Method	Yes	Expensive	Up-to-date	No
MAR	Guideline	No	Free	Up-to-date	No
ISAMM	Method	Yes	Unavailable	N/A	No
GAO/AIMD-00-33	Guidelines and Case Studies	Yes	Free	N/A	No
IT System Security Assessment	Guideline	Yes	Unavailable	N/A	No
MG-2 and MG-3	Guideline	Yes	Unavailable	N/A	No
Security Risk Management Guide	Guideline	Yes	Unavailable	N/A	No
Dutch A&K Analysis	Method	Yes	Unavailable	Obsolete	No
MARION	Method	Yes	Unavailable	Obsolete	No
Austrian IT Security Handbook	Guideline	Yes	Unavailable	Up-to-date	No
Microsoft security risk management guide	Guideline	Yes	Free	Up to date	No
RiskIT	Framework	No	Available	N/A	No

Table 3. Selection Criteria for all the different models

6.5 Chosen Models

As a result of applying the 4 criteria described above, 16 of the 22 initial models were excluded. These models didn't conform with one or more criterion and for that reason they won't be studied in more understanding.

Nonetheless, six models were in conformance with all the criteria. These models are: Octave ,Mehari, Magerit, IT-Grundschutz, Ebios and IRAM. Only these models will be measured after this point.

6.6 Second Iteration Selection Criteria

Despite having reduced the initial universe of models to almost one fourth, six is still a significant number of models to study in detail (considering the present time and people limitations of this work). Therefore, the universe of models will again be reduced through another set of standards. The 5 selected criteria are described below:

i. 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. To express this criterion in a more quantitative manner, models are classified under three levels of complexity:

Little groundwork needed; less detail/accuracy in the output. Quick assessment; Some preparation needed; medium output detail/accuracy.

Broad preparation and effort needed; more detail/accuracy on the output.

ii. Approach of the model

The risk assessment approach each model advocates (e.g. self-assessment, interviews, workshops). This criterion doesn't pretend to analyze the approach in great detail. It will only consider the main ideas and strategies of each model. A more comprehensive analysis will take place in the next section.

iii. Tools

If the model provide supportive tools and how can we obtain them. This criterion is divided into the following categories:

- Free tool;
- Paid tool (but with a trial period);
- Paid tool (with no trial available);
- No software tool but has supporting documentation (e.g. worksheets ,questionnaires, forms);
- No supporting tools.

iv. Origin

In this study three likely sources for a model were considered. These entities can be:

Academic;

Governmental;

Commercial.

v. Geographical spread

Countries in which the model is known to be implemented.

6.7 Comparison Criteria

This section familiarizes the criteria that will be used to evaluate and compare the three information security risk assessment models in more detail. Some of the models' characteristics were already analyzed during the selection process described above. Some of these assessment criteria are similar to the criteria used before, but in this section the models will be analyzed in more complexity. Below we have the description of the new set of criteria:

i. Concept definition

This criterion pretends to clarify and distinguish the three information security risk assessment models by identifying and describing their basic and most relevant concepts. It evaluates the resemblances and differences between the concept definitions each model proposes.

The concepts that will be under evaluation in this study are: Risk, Asset, Vulnerability, Threat, Impact, Control (or Risk Treatment), Residual Risk, and Security Requirements or Objectives.

ii. Approach to information security assessment

The risk assessment approach each model advocates (e.g. self-assessment, interviews, workshops).This measure analyses the approach with greater detail than the previous section analysis and also compare the three final models consequently. To assess the approach at this stage models are characterized under the following aspects:

- Description (of the approach)
- Main activities
- How risk is calculated

iii. Results and output

This criterion analyses the detail of each models' output after the risk assessment is completed. It tries to evaluate the quality, clarity of the information produced. It also differentiates models that generate qualitative and quantitative data, and models that recommend information security controls of countermeasures, allowing the organization to continue the risk management course.

iv. Complexity

This criterion tries to reproduce 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. This criterion was also used in the selection process, but in this section the final models will be equated in more detail.

To asses this level models are characterized under the following aspects:

- Level of detail;
- Inputs / Preparation needed (ease of gathering the needed information);
- Techniques;
- People involved;
- Effort;
- Time;
- Skills needed;

The above mentioned criteria will be applied to the three models in the following sections.

6.8 Comparing concept definitions of three models

Risk: All three models have a very similar meaning for risk. All of them consider risk as a function of the probability/likelihood of a threat materializing over a vulnerability, and the impact/consequences of that incident.

Asset: All the three models focus their risk assessment approach on information .The variance is that OCTAVE distinguishes the information itself from its container, i.e. the physical or electronic form where information exists is a different notion in OCTAVE (called information container), while the other two models don't separate the actual information from its containers, considering it all as one model.

Vulnerability: IRAM and IT-Grundschutz have the same definition for vulnerability and they both consider this concept in their approaches in a very similar way. On the other hand, OCTAVE, in spite of identifying the concept of vulnerability, doesn't include a vulnerability assessment in its methodology. It identifies the containers of each information asset and only considers threats to those containers.

Threat: All three models define threat very similarly as a potential undesirable security event.

The differences are, for example, that OCTAVE only identifies a threat when a threat actor exploits a vulnerability. This definition is the same as the one in IT-Grundschutz for Applied Threat. IT-Grundschutz also defines Basic Threat as a threat that hasn't yet exploited a vulnerability. IRAM defines threat and also Security Incident. A security incident occurs when threats happen.

Impact: All three models define Impact as the consequences of a security incident on business with no significant differences amongst them.

Control/Risk Treatment: All definitions are alike, despite the use of numerous terms form the same concept (control, safeguard, mitigation approach, risk treatment, security precaution, protective measure)

Residual Risk: Similar definitions. Residual risk is the risk that remains after the risk treatment process.

Security Requirements or Objectives: Requirements that explain how each asset should be protected. All three models take into attention the three main information security vectors, Confidentiality, Integrity and Availability.

6.9 Approaches

i. OCTAVE

Description

OCTAVE is mainly a self-directed information security risk assessment method. It was designed to be used in cases where people from an organization manage and direct an information security risk assessment for their own organization. It takes a business rather than a technologic-centric opinion of security risks. It identifies information-related assets (e.g., information and systems) that are key to the organization and weigh risk analysis activities on those assets judged to be most critical to the organization . The OCTAVE's tactic focuses primarily on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result. OCTAVE can be performed in a workshop-style, collaborative setting and is supported with guidance, worksheets, and questionnaires, which are included in the model. However, OCTAVE is also well suited for use by entities who want to perform risk assessment without wide organizational involvement, expertise, or input. OCTAVE has flexible measures, with the ability to be customized to organizational needs. However, OCTAVE doesn't provide a software tool or Excel tables to help the assessment process. It only provides the needed paper documentation.

Activities

Phase 1: Build Asset-Based Threat Profiles – This is an managerial evaluation. Staff members from the organization contribute their outlooks on what is important to the organization (information-related assets) and what is now being done to safeguard those assets (elicitation workshops). The analysis team fuses the data and selects the assets that are most significant to the organization (critical assets). The team then describes security requirements for the critical assets and identifies threats to the critical assets, generating threat profiles.

Phase 2: Identify Infrastructure Vulnerabilities – This is an assessment of the information infrastructure. The analysis team finds key information technology systems and components that are related to each critical asset. The team then examines the key mechanisms for weaknesses (technology vulnerabilities) that can lead to unapproved action against critical assets (technological view of information security).

Phase 3: Develop Security Strategy and Plans – During this part of the evaluation, the analysis team spots risks to the organization's critical assets and decides what to do about them. The team creates a protection methodology for the organization and mitigation plans to address the risks to the critical assets, based upon an analysis of the information collected.

Risk Calculation

First OCTAVE defines the risk evaluation criteria for impact and probability, forming a common understanding of the qualitative measures (high, medium, low). Then these values (high, medium, low) are allotted automatically to each risk/impact by the assessment team based on the evaluation criteria

The method uses an Expected Value Matrix
(Loss = Impact/consequence x Probability).

ii. IRAM

Description

IRAM is a workshop based information risk assessment model (typically conducted through face-to-face dialogues with business and IT staff). IRAM is very well structured and laborious model that focus its analysis on the organization's information systems and determines key information threats to those systems. IRAM's approach helps to determine the criticality and prominence of information systems. Despite having been intended to meet the demanding needs of information risk analysts in modern risk-oriented organizations, IRAM's approach proved to be very practical, flexible and above-all easy-to-use. It's a process oriented methodology that provides a great deal of backing documentation, forms, tables and tools.

Activities

Phase 1 - Business Impact Assessment
Phase 2 - Threat and Vulnerability Assessment
Phase 3 - Control Selection

Risk Calculation

Tables, forms and formulas provided by the tools. The actual risk calculation formula is not openly available. The tools calculate the risk ratings by design.

iii. IT-GRUNDSCHUTZ

Description

IT-Grundschutz provides a method for an organization to inaugurate an Information Security Management System (ISMS). It includes both generic IT security recommendations for establishing an applicable IT security process and detailed technical references to achieve the necessary IT security level for a specific field. So, the key approach in ITGrundschutz is to provide a framework for IT security management, offering information for normally used IT components (modules). IT-Grundschutz modules include lists of germane threats and essential countermeasures in a relatively technical level. These elements can be extended, complemented or adapted to the needs of an organization. Under the customary risk analysis approach, first of all the threats are identified and given a likelihood of occurrence. The results of this analysis are then used to select the appropriate IT security measures, subsequently the residual risk can be assessed. For IT-Grundschutz this task has already been accomplished for each module, and the appropriate IT security measure, selected for a typical office environment. When applying IT-Grundschutz this task is reduced to a target versus actual comparison between the security measures recommended in the ITGrundschutz Catalogues and those already implemented. Security procedures that are found to be absent or inadequately implemented reveal security shortages that can be rectified by implementing the recommended security measures. Only where the shield requirements are significantly higher is it necessary to also perform a supplementary security analysis, weighing up the cost-effectiveness of employing additional measures.

Activities

1. The information and business processes that are to be protected must be identified;
2. All the relevant threats pertaining to the information and business procedures that are to be protected must be identified;

3. Vulnerabilities which the threats can use to yield effect must be identified;
4. The possible harms due to a loss of confidentiality, integrity or availability must be identified and evaluated;
5. The assumable repercussions on the business activities or fulfillment of tasks through IT security instances must be analyzed;
6. The risk of suffering damages due to IT security happenings must be assessed.

Risk Calculation

Traditional risk analysis approach, first of all the threats are recognized and assigned a likelihood of occurrence. Reiterate this task for each module.

7. CONCLUSION

Risk assessment is a vital cog in the wheel of Information Security Management. It is important for enterprises to adopt a systematic and well-structured process for assessing information security risks to its assets. The main purpose of the study is to compare and clarify the different activities, inputs and outputs required by each information security risk assessment models and also analyze which ones address information security risk effectively. The resulting information helps evaluating the models' applicability to an organization and their specific needs. In organize to authenticate and legalize the conclusions taken from the theoretical study of all these models and hence, reduce risk

7. REFERENCES

[1] K.V.D.Kiran "A Novel Risk Analysis and Mitigation methods in Distributed banking system ",International Journal of Advances in Engineering & Technology , Vol 6,No 4,2012 pp:1593-1602.

[2] Sun, L.., Srivastava, R., Mock, T.: An Information systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions. Journal of Management Information Systems, Vol. 22, No. 4, Spring 2006: 109-142 (2006)

[3] Alberts, C.: Common Elements of Risk. Technical Note CMU/SEI-2006-TN-014, Carnegie Mellon University (April 2006)

[4] SPRINT: Risk Analysis For Information Systems, User Guide, Version 1.0. The European Security Forum (1997)

[5] Bayne, J.: An Overview of Treath and Risk Assessment. SANS Institute, as part of the Information Security Reading Room (2002)

[6] A Risk Management Standard. AIRMIC, ALARM, IRM, London (2002)

[7] Jeremy Hilton,Pete Burnap and Anas Tawileh: Methods for the identification of Emerging and Future Risk, ENISA (2007)

[8] Inventory of risk assessment and risk management methods. ENISA ad hoc working group on risk assessment and risk management (2006)

[9] Alberts, C. and Dorofee, A. 2001. *An Introduction to the OCTAVE Method*. Software Engineering Institute, Carnegie Mellon University, USA.