University of Stavanger

**Faculty of Science and Technology**

# MASTER'S THESIS

| | |
|---|---|
| Study program/ Specialization:<br>Risk Management/ Risk Management | Spring semester, 2020 |
| Writer:<br>Amir Hosein Araskalaei | A. Aras<br>……………………………………………<br>(Writer's signature) |
| Faculty supervisor: Terje Aven | |
| Title of thesis:<br>**EVALUATION OF IT SECURITY RISK STANDARDS RELATIVE TO RISK ANALYSIS AND MANAGEMENT SCIENCE** | |
| Credits (ECTS): 30 | |
| Key words:<br>Risk management, Information Security, Risk definition in Safety settings, IT Standards, NIST, ISO/IEC 27005, OCTAVE, Uncertainty, Background knowledge. | Pages: 47<br>+ enclosure: -<br>Stavanger, 2020 |

# EVALUATION OF IT SECURITY RISK STANDARDS RELATIVE TO RISK ANALYSIS AND MANAGEMENT SCIENCE

**Amir Hosein**
**Araskalaei**

**Stavanger, Spring**
**2020**

Faculty of Science and Technology

Department of Industrial Economics, Risk Management and Planning

# Acknowledgements

This thesis has been carried out as a fulfillment of the requirements for MSc degree in Risk Management at the University of Stavanger.

I would like to express my gratitude to my supervisor, Professor Terje Aven for his guidance, constructive feedback and for enlightening my way throughout the whole thesis. I am thankful and honored to have written this thesis with Professor Aven. His support and knowledge-sharing made this path for me so pleasant and delightful.

Finally, I would like to thank my other professors, lecturers, and the members of the center for Risk Management and Societal Safety (SEROS) at the University of Stavanger for this beautiful journey during my master studies in Risk Management.

Amir Araskalaei

15.06.2020

## Table of Contents

## List of Figures

## List of Tables

# ACRONYMS

A: Actual Events in the future

A’: Events specified by the assessor

C: Actual Consequences in the future

C’: Consequences specified by the assessor

K: Background knowledge in the form of justified beliefs

RS: Actual Risk source

RS’: Risk source specified by the assessor

T: Threats (covering risk source and events)

T’: Threats specified by the assessor (covering risk source and events)

Q: A measure for describing the uncertainty (U).

U: Uncertainty

SoK: Strength of knowledge

# 1. INTRODUCTION

## 1.1 Background

The growing development of information technology has revolutionized the various aspects of human life and the functioning of organizations. Information Technology has changed the way people, organizations, and governments function and attitudes, and has revolutionized the way things are done, especially in providing different services to customers. Today, providing service and having the ability to meet expectations is one of the most important business needs, and for this reason, it is very important in organizations to have a strong, effective, and secure network. Adequate preparedness to deal with or make appropriate decisions against physical events, cybercrime, disruption, etc. in both the infrastructure and application of information technology is an inevitable approach to ensuring business reliability. Therefore, network security and information systems have become one of the most important issues and concerns of IT managers.

The most important step in securing an organization is to create a strong framework for managing security measures. It must be acknowledged that the process of building security of an organization is not possible without considering the issues of risk management and its expansion at the level of all sensitive and strategic parts of the organization. Information security risk management ensures the protection of information assets by selecting adequate and appropriate security controls, thus ensuring the benefit of the parties concerned. In this way, standard security solutions are applied to all hardware, software, communications, and their platforms to help the organization achieve success in the shadow of a safe environment.

This is exactly where IT security risk management frameworks are implemented. The Information Security Risk Management has been agreed with the aim of clearly explaining security strategies to manage information security risks of organizations within the framework of a set of business risks and as an assessment, management and support of information technology security within the organization and outside the organization.

It should be mentioned that the purpose of designing and implementing information security risk management is to create a platform for coordination between all project personnel in order to move in the direction of information security in the organization and this will not be achieved unless experts and senior managers participate and support the frameworks.

## 1.2 Objectives of the Thesis

The overall goal of this thesis is to review and evaluate the two important risks standards in information systems and add values to these standards in accordance with risk analysis and management science.

NIST SP800-39 (Managing information Security Risk) and NIST SP800-30 revision 1 (Guide for Conducting Risk Assessment) will be reviewed, their strengths and weaknesses will be highlighted, their content will be compared with the existing risk management standards and further suggestions for the improvement of a solid framework will be given.

## 1.3 Content

**Chapter 1** gives an introduction of the thesis including the background, objective of the thesis.

In **Chapter 2**, the *NIST SP800-39* (Managing Information Security Risk) and *NIST SP800-30* Revision 1 (Guide for Conducting Risk Assessment) in IT security systems are reviewed.

**Chapter 3** examines the two above-mentioned standards and compares their content in relation with risk analysis and management science and suggests points to improve the framework of these standards.

**Chapter 4** is a summary of the discussions and concluding remarks of chapters 2 and 3.

# 2. REVIEW OF NIST STANDARDS IN IT SECURITY SYSTEMS

Among several IT security standards, there are two dominant standards that are widely used in IT risk management. ***NIST SP800-39*** which concerns managing information Security Risk and the ***NIST SP800-30 (revision 1)*** which is a guide for conducting Risk Assessment. This part of the thesis reviews the most important features of these standards.

## 2.1 NIST SP 800-39

The relationship between the organization, business processes and information systems are complex and information systems need to have an integrated, organization-wide view of risk management. NIST SP 800-39 claims to provide uniform and consistent ways to manage risk throughout the entire organization, organization operations. Assets, individuals, and the nation.

800-39 claims to provide a strong basis for reciprocal acceptance of authorization decisions and facilitates information sharing. It stablishes organization-wide risk management strategies involving senior management. Furthermore, it stablishes a risk executive function or RE(F).

### 2.1.1 Objectives of NIST SP 800-39

The most important objectives of the standard are as considered as ***ensuring*** that senior leaders recognize the importance of managing risk, ***establishing*** governance structures for managing risk and ***ensuring*** the risk management at all tiers (three tiers which will be introduced later). And finally, the standard promotes the understanding of how information security risk at the system level affects mission/business processes and the entire organization.

### 2.1.2 Key Elements of NIST SP 800-39

Senior leaders of an organization are among key elements of NIST SP 800-39 standard. NIST intorduces some key elements in the standard as well as assigning risk management responsibilities to senior leaders and ***recognition*** or ***understanding*** of risk by senior leaders in the operations (senior leaders' awareness of risk in operations). It also establishes organizational risk tolerance and communicates risk tolerance across the organization. NIST provides guidance on how risk tolerance impact risk management decisions. And finally, senior leaders need to be ***accountable*** for risk management decisions and for implementation of an effective risk management program.

### 2.1.3 NIST SP 800-39 And the Multi-Tiered Risk Management

NIST 800-39 suggest a ***Multi-Tiered*** risk management model. 800-39 covers almost all three tiers but it is more focused on Tier 1 and Tier 2. NIST SP 800-37 will focus more on Risk management framework at the system level (Tier 3).

The organizational tier on top, the governance, set policies and their risk executive function is at the top and decisions are taken about what the organizational risk tolerance should be. They inform the two other tiers what the decisions are and how they should apply those decisions in tier 2 and tier 3.

It means as we move up, our strategic focus increases and by moving down, tactical focus increases accordingly. Throughout the whole process, the goal is that the information flows up and down. If the information from operating systems flows up, senior leaders become aware of the system risks and they can overview it in an aggregated way. ***The risk management*** and ***risk tolerance decisions*** need to be flowing downward from tier 1.

Tier 2 is the mission/business process tier. For example, this is what can happen at this tier:

If we consider the chief financial officer, the mission would be paying the organization's bills, paying people, taking in money, making purchases, and so on. So, there are numerous systems underneath the chief financial officer, but they all add up to one single mission. [1, pages 10-11]

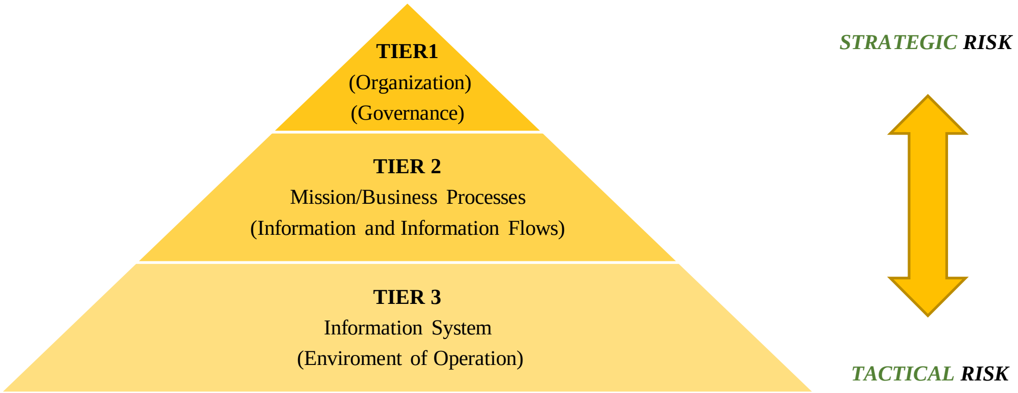


**Figure 2-1-Multi-Tiered Risk Management**

## 2.1.4 Three-tiered Risk Management Approach

The above-mentioned three-tiered risk management approach addresses risk in the context of critical mission and business functions. It fosters climate where information security (IS) risk is considered in context of design of mission/business processes, design of enterprise and security architecture and system development life cycle processes. It also facilitates understanding of how IS risk affects organization-wide and mission/business process risk.

### 2.1.4.1 Tier 1

*Organization*

The role of organization in tier 1 is that to implement risk framing by providing context to all RM activities with the organization and tries to establish and implement governance structure to provide oversight for RM activities through establishing/implementation of the RE(f), establishing overall RM strategy and risk tolerance and developing/executing investment strategies for IS.

*Governance*

Governance is defined as set of responsibilities and practices exercised by those responsible for an organization. Governance ***goals*** in NIST provide strategic direction, ensure that mission/business objectives are reached, ascertain if risks are being managed appropriately and verify that resources are used responsibly.

The desired outcomes of organization wide Risk Management governance in NIST are defined as: ***aligning*** RM decisions with mission/business functions and the organization's goals and objectives, ***executing*** RM processes to frame, assess, respond, and monitor risk in the organization's operations and assets, ***allocation*** of RM resources effectively and efficiently, and measuring, monitoring, and reporting RM performance to ensure that goals and objectives are achieved.

Also, delivering value by optimizing RM investments, is within governance goals. In governance, senior leaders determine the types of RM decisions reserved for specific senior leadership roles, types of RM decisions affecting the entire organization, types of RM decisions that can be delegated to subordinate organizations or other organizational roles and how RM decisions will be communicated to and by the RE(f)

*Risk Executive Function – RE(F)*

NIST claims that they do not mandate or dictate how the risk executive function has to look, and each organization can decide how they need to implement it. RE(F) has a functional role that provides a comprehensive, organization-wide approach to RM. It serves as the RM resource for all stakeholders and requires a mix of skills, expertise, and perspectives, and an understanding of strategic objectives and mission/business functions. An ***individual*** or a ***group*** might be in charge of RE(F).

*Risk Management Strategy*

Risk management strategy is a key output of the Risk Framing Component of risk management. It answers how organizational risk will be assessed, responded, and monitored and it includes a clear statement on risk tolerance, acceptable risk assessment methodologies, risk response strategies, a process for consistent evaluation of risk, and approaches for risk monitoring.

*Risk Tolerance*

Risk tolerance is the level of risk or degree of uncertainty that is acceptable to the organization. It is one of the key elements of the RM strategy. Risk tolerance ***affects*** the nature of RM oversight, extent and rigor of risk assessments and strategies for responding to risk.

Regarding threats, organizations that are ***more*** risk tolerant may only address threats that have been exploited at peer organizations. Organizations that are ***less*** risk tolerant may address theoretical threats.

Regarding risk response, organizations that are ***more*** risk tolerant may require very little assurance on effectiveness and they may accept more risk rather than mitigate it and organizations that are

***less*** risk tolerant may require extra assurance on the effectiveness of countermeasures and may mitigate or reject risk rather than accept it.

The degree of risk tolerance is indicative of organizational culture and it may be different for different types of threats or compromises. It is also influenced subjectively by individual senior leaders. Less risk tolerant organizations may sacrifice needed mission capabilities. On the contrary, more risk tolerant organizations may artificially minimize the risk and set themselves up for future failure.

#### 2.1.4.2 Tier 2

*Mission/Business Process Level*

In tier two, the aim is to identify and establish risk-aware mission/business processes. The key output is risk response strategy for each mission/business process. Also, senior leaders must understand the types of threat sources and threat events that may affect the mission/business process.

*Enterprise Architecture (EA)*

EA is a management practice that connects investments to measurable performance improvements. It applies a disciplined and structured approach for managing IT assets and underlying infrastructure in support of mission/business processes.

*Information Security Architecture (ISA)*

ISA is a part of the enterprise architecture that addresses system ***resilience*** and security capabilities. It helps ensure mission/business process-driven information security requirements and it is implemented consistently and cost-effectively. It also provides traceability.

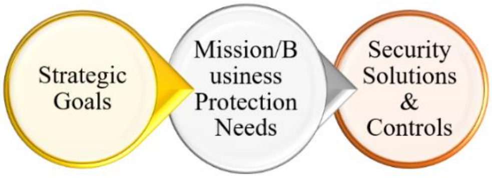

Strategic Goals
Mission/Business Protection Needs
Security Solutions & Controls

**Figure 2-2- Traceability track**

#### 2.1.4.3 Tier 3

*Information System Level*

In tier three, risk management activities occur at information system level, and are integrated into all System Development Life Cycle (SDLC) phases. It integrates risk management into the SDLC which is the ***most*** cost-effective way to secure systems and risk management decisions at each SDLC phase influence subsequent phases. (Specific guidelines for RM at the system level are found in NIST SP 800-37)

### 2.1.5 Four Components of Risk management

Based on 800-39, there are four components of risk management: ***framing risk***, ***assessing risk***, ***respond to risk*** and ***risk monitoring***, which are discussed in the following. [1, Page 6]. (Component tasks are also mentioned in appendix C)

| Component: | Definition and utilization: |
|---|---|
| **Risk Framing** | Its purpose is to produce a risk management strategy. It establishes a risk context by describing the environment in which risk-based decisions are made and also it establishes risk frame by identifying:<br>*Risk assumptions*<br>*Risk constraints*<br>*Risk tolerance*<br>*Risk priorities and tradeoffs* |
| **Risk Assessment** | The risk assessment identifies:<br>*Threats to the organization.*<br>*Vulnerability of the organization.*<br>*Potential harm (i.e., adverse consequences or impact) resulting from threats exploiting vulnerabilities.*<br>*Likelihood that harm would occur.*<br>*End results is a determination of risk (i.e., the degree of harm and likelihood of occurrence)* |
| **Respond to Risk** | It provides a consistent organizational-wide response to risk by:<br>*Developing alternative courses of action for response.*<br>*Evaluating the alternative courses of action.*<br>*Determining the most appropriate course of action.*<br>*Implementing the risk response.*<br>*And potential risk responses include:*<br>*Accept risk*<br>*Mitigate risk*<br>*Reject risk*<br>*Share/transfer risk* |
| **Risk Monitoring** | It describes how compliance is verified, how ongoing effectiveness of risk response is determined (i.e., what tools, techniques, methodologies will be used) and it monitors risk over time by:<br>*Verifying that planned response actions are implemented.*<br>*Determining ongoing effectiveness of response actions.*<br>*Identifying changes to systems that impact risk.* |

**Table 2-1- NIST Risk management components**

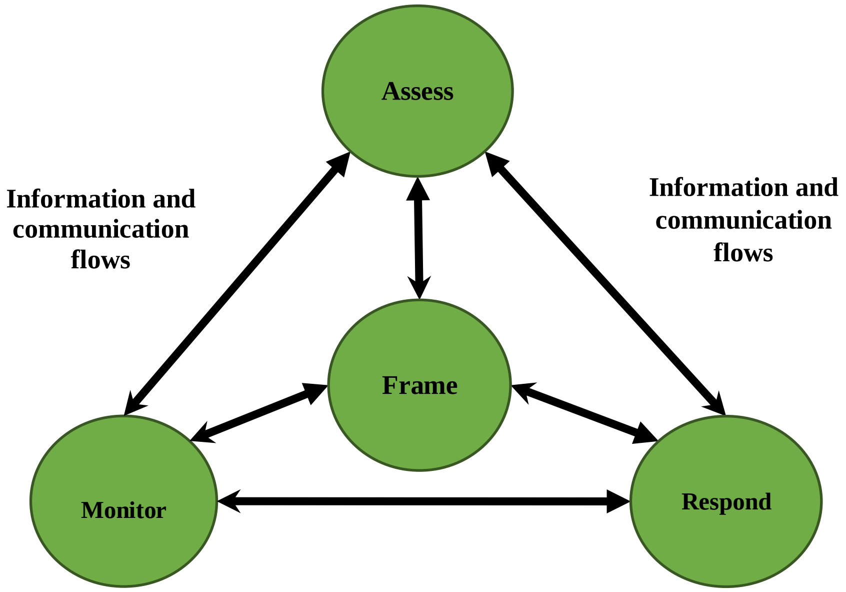

Assess
Information and communication flows
Information and communication flows
Frame
Monitor
Respond

**Figure 2-3-NIST Risk management framework**

The process diagram demonstrates the overall risk management framework. The ***frame*** establishes the context for risk organization environment and decisions within the organization itself. The ***assessment*** documents threats, vulnerability and potential harm resulting from risk. The ***respond*** deals with the assessed risk. ***Monitoring*** asks questions as well as: If the response is working? If the risk environment is changing? If the risk program is being implemented as planned and satisfies anticipated results?

## 2.2 NIST SP 800-30 Revision 1

NIST 800-30 is a guide for conducting risk assessment. There was a mandate to conduct risk assessments per FISMA (Federal information security management in 2002) requiring civilian Federal government agencies to organize their information security by starting out with a risk assessment and NIST was charged with coming up with the standards for performing these assessments. The publication focuses on the risk assessment aspect of risk management and informs us how to ***prepare*** for risk assessment, ***conduct*** risk assessment, ***communicate*** risk assessment results with CEO or any key personnel in an organization and ***maintain*** and ***monitor*** the risk assessment.

### 2.2.1 Risk assessment overview and goal

In this publication, NIST identifies actual threats and vulnerabilities within an organization, including the internal and external factors, ***impacts/damages*** to an organization after exploiting vulnerabilities and how likely it can be that the vulnerabilities will be exploited. The goal of risk assessment is a determination of risk and the degree of potential harm and likelihood of occurrence of the harm.

### 2.2.2 Risk assessment at different tiers

In section ***2.1.3,*** a three-tiered RM approach suggested by NIST has been discussed. In each tier, risk assessment has some considerations.

#### 2.2.2.1 Risk assessment at tier 1

Risk assessment at tier one supports organization-wide strategies, policies, and procedures and focuses on organization operations, assets, and individuals. It is Based on the assessment conducted across multiple mission/business lines in tier 2, considering the essential functions identified in continuity operations plan (COOP). The results are communicated to tier 2 and 3 and it leads to organization-wide mandates for immediate mitigation action.

#### 2.2.2.2 Risk assessment at tier 2

Risk assessment in tier two, supports the determination of mission/business process, protection, resiliency requirements and allocation controls to the stem of the risk. It focuses on mission/business segments and informs decisions regarding use of information systems to support business functions. It is also closely aligned with business continuity plans. Here, results are communicated to tier 1 and 3. It provides an ongoing assessment of the security of the security posture of mission/business processes.

#### 2.2.2.3 Risk assessment at tier 3

Risk assessment at tier three focuses on individual information systems. (by looking at the system development life cycles depending on the phase of life cycle). Initial risk assessment during development concludes with recommendations for ***selecting security controls*** and can be conducted during each step of risk management framework.

The steps of risk management framework are shown below:

(A detailed footage of the steps is given in Appendix D)

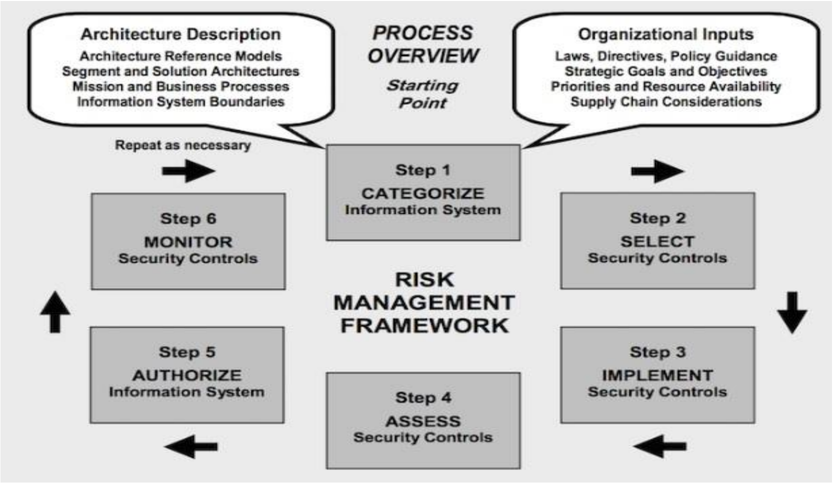

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

**Figure 2-4-NIST SP 800-37 Risk Management Framework at system level**

### 2.2.3 Risk assessment Process

NIST suggests three steps for risk assessment process. ***Preparing for the assessment, Conducting the assessment,*** and ***maintaining the assessment***.

#### 2.2.3.1 Risk Assessment – Preparation Tasks (5 Tasks)

***Task 1*** identifies the purpose of the risk assessment. It investigates if it is an ***initial assessment*** or an ***updated assessment***?

The ***initial purpose*** establishes a baseline of risk or identifies risk factors to be tracked over time.

The ***updated purpose*** may include assessment of the ongoing effectiveness of security controls, new or reduced risk from changes to systems or environments of operation and the results from compliance verification.

***Task 2*** identifies the scope of the risk assessment. The tiers will be addressed in the risk assessment, and it will be indicated what organizational parts will be affected by risk assessment. Furthermore, it discusses that how long the results will be relevant (effectiveness time frame) and what will trigger the need to update the risk assessment.

***Task 3*** identifies the specific ***assumptions*** and ***constraints***.

***Assumption areas include*** threat sources/threat events, vulnerabilities/predisposing conditions, impacts and assessment and analytic approaches.

***Constraint areas*** include available resources, skills and expertise required and operational considerations. (e.g. physical location, mission needs.)

***Task 4*** identifies sources of information to be used. The information needed as well as threat information, vulnerability information and impact information. Potential sources can be either external sources (e.g., US-Cert, ISACS) or internal sources (e.g., incident reports, security logs, business impact analyses.)

***Task5*** defines or refines risk models to be used. It uses risk factors defined in the NIST standard appendices. For each assessable risk factor, the appendices include three assessment scales with different representations.

#### 2.2.3.2 Risk Assessment – Conduction Tasks (6 Tasks)

***Task 1*** identifies and characterizes the threat sources of concern to the organization. Characteristics may define specific types of threat sources as well as intentions, targeting and capabilities.

***Task 2*** identifies threat events, relevance, and threat sources. It also identifies the many-to-many relationship between threat events and threat sources (*It will increase complexity for the RA)*, and relevance of each identified threat event is determined and has direct linkage to organizational risk tolerance. All potential threat sources are identified for each relevant threat event.

***Task 3*** identifies vulnerabilities and predisposing conditions. It also identifies predisposing conditions that affect susceptibility to vulnerabilities. It also determines which vulnerabilities and which predisposing conditions are relevant to which threat events. All potential threat sources are identified for each relevant threat event.

***Task 4*** determines the likelihood of adverse impacts occurring by considering characteristics of threat sources that could initiate events, vulnerabilities and predisposing conditions identified in task 3 and countermeasures planned or implemented to impede events. It assesses the likelihood that threat events will be initiated, likelihood that initiated events result in adverse impact and overall likelihood as combination of the first two parts.

***Task 5*** determines adverse impacts by considering the characteristics of threat sources that could initiate events, vulnerabilities and predisposing conditions identified in task 3 and countermeasures planned or implemented to impede events. It also describes adverse impacts in terms of potential harm. (The more critical a system or asset is, the higher adverse impact will be.)

***Task 6*** determines the risk to the organization from threat events by considering the impact that would result from the events and the likelihood of the events occurring. At certainty (100% probability), risk = impact.

#### 2.2.3.3 Risk Assessment – Maintaining the Risk Assessment (2 Tasks)

***Task 1*** conducts ongoing monitoring of factors that contribute to changes in risk. The objective is to maintain ongoing situational awareness of the security state of the organization and the results are used to refresh ***RA***s at the frequency deemed appropriate by the organization.

***Task 2*** updates the existing ***RA***s using results from monitoring. It is updated based on organizational determinations of frequencies and relevant circumstances; it revisits prepare step if there have been significant changes as defined by the organization.

If there have been no significant changes to the system, it updates only how risk factors have changed. The changes in new threat events, vulnerabilities, or predisposing conditions or threat source characteristics, likelihoods, or impacts.

# 3. COMPARISON OF STANDARDS AND SUGGESTIONS FOR IMPROVEMENTS OF NIST

In previous chapter of the thesis, NIST standard and its risk management and risk assessment processes were reviewed. In chapter three, the important points of the NIST will be highlighted and discussed. Also, it will be examined if NIST is the right standard to be implemented and protect an organization. One way to measure the efficiency of NIST to compare the standard to the other existing standards and ***available criteria*** in Risk management science and security settings.

Chapter three is planned in ***four parts***:

***Part one*** mentions the weaknesses of NIST in the eye of IT experts and the writer of the thesis. These weaknesses include the definition of risk, vulnerability, threat, and also several other features of the standard as well as complicated documentation of NIST, exaggerated flexibility in the process etc.

***Part two*** argues if the risk concept definition given by NIST is a comprehensive definition with respect to threats, vulnerabilities and uncertainties or the definition of risk should be revised to cover the associated values regarding risk concept.

***Part three*** compares NIST with the other two important IT standards, ISO/IEC 27000-series, OCTAVE. The reason for this comparison is to show the advantages and disadvantages an organization gains by implementing NIST. The compared features of these dominant IT standards include the size of an organization, threat-focused or control-centric approaches of the standards, flexibility of the IT standard and technical and organizational aspects of the standards.

***Part four*** introduces some techniques and methods as well as SWOT analysis and use of red teaming for a better implementation of the NIST standard.

## 3.1 NIST standard: Weaknesses

The recognized ***weaknesses*** of NIST are as following:

**1.** NIST defines risk as a function of likelihood of a given threat and the impact of the adverse event on the organization. It will be shown that risk is beyond probabilities and expected values and there is a way better definition of risk concept which security settings can rely on.

**2.** Regarding documentation, since NIST SP 800-39 cannot be used in isolation and SP 800-37 and 800-30 offer guidance for managing risk, this large number of documentation makes it quite difficult for the organizations to find clearly what they are trying to extract from the standard.

**3.** Regarding threats/Cyber-attacks:

In section ***2.2.2.3,*** the risk management framework starts with ***categorizing*** the system, selection, and control implementation, assessing security controls, authorizing information system and monitoring. So, it is not clear if ***threat assessment*** plays any role in determining and selection of the controls. [4, Baker, 2015] NIST mentions that initial risk assessment results must be used to inform impact analysis for appropriate categorization. But the word ***threat*** has not been mentioned in ***categorizing*** the system. (Figure 2-4. Page 17). NIST has an ***asset-focused*** and ***control-centric*** approach rather than a ***threat-focused*** approach and since threats and cyber-attacks are a great concern and have an increasing trend in security settings, this could cause problems.

**4.** NIST standard is obsessed with ***actuarial risk*** throughout the whole process and constantly ask about the costs of an attack for an organization. Firstly, it could be more convenient to ask about all of the consequences of an attack on an organization. And secondly, a ***preventive approach*** could be a more convenient in security settings and generally in risk management since the consequences could be devastating.

**5.** NIST's ***generalized*** view on risk assessment and risk management could be a problem since it does not dictate exact solutions to a problem. [3, Vacca, 2009]

**6.** Regarding the risk assessment, NIST uses a ***numeric scoring*** which might cause problems. NIST allows organizations choose a semi-quantitative method to score risks (as an alternative to quantitative methods in case uncertainty is high). But NIST never mentions the ***strength of knowledge*** behind these scorings.

**7.** In the last task of NIST's conduction of risk assessment ***(2.2.3.2.)***, the formula *risk = impact* at 100% probability is used. NIST uses the formula Risk = impact*likelihood. Assigning numbers as subjective probabilities may mislead the risk assessment process if the ***associated uncertainties*** and the ***strength of knowledge*** together with these probabilities are not considered.

**8.** In (***2.1.4.1),*** risk executive function introduced by NIST is flexible in a way that may cause problems due to subjectivity. There are two problems arising from too much flexibility. First, it requires an expert who has vast knowledge in different areas as well strategic objectives, mission/business functions. Secondly, since the responsibility could be given to a single person in charge of RE(f), ***subjectivity*** of an individual with a ***weak background knowledge*** of the system could cause problems in risk assessment.

9. NIST ***emphasizes*** on trust and trustworthiness between the organization and all the entities that the organization has relationship with. This could lead to higher risks to the organizations. “The belief that an ***external entity*** will behave in a ***predictable*** manner in specified circumstances” [1, page 24].
10. The design of NIST is more suitable for ***government agencies*** and less convenient for smaller organizations.
11. It could be comprehended that NIST is more focused on ***compliance*** and the ***security*** is a secondary issue.

## 3.2 The definition of risk in security settings

Risk concept is generic and regardless of the type of the standard, risk management process, and the areas of its application (safety, security, reputation, etc.), it is crucial to provide a strong basis/ accurate definition of risk concept that many standards and processes seem to have missed it.

NIST defines risk as “a function of likelihood of a given threat and the impact of the adverse event on the organization.”

It is common to define risk as a triplet of asset-threat-vulnerability in security settings where potentially intentional attacks are involved but the question is, if this definition is good enough in security settings?

We refer to the risk definition as “Risk is a two-dimensional combination of consequences C and associated uncertainties.” [8, Aven, 2015].

The author of this thesis does not claim that NIST has skipped or neglected the concept of uncertainty in its standard. ***In appendix E – More on Uncertainty,*** NIST acknowledges that “Uncertainty is inherent on the evaluation of risk” [2, NIST] or “the organization must prioritize risks by analyzing threats and vulnerabilities and associated uncertainties with risk assessment.” [2, NIST] However, it seems that there is a ***gap*** between the risk concept and uncertainty (U) in NIST standard.

In this part, a sound and strong definition of risk will be introduced, in which uncertainties, together with the triplet asset-threat-vulnerability will be considered. It will be shown that the common understanding of risk concept among NIST and generally other security setting communities should be revised, and risk concept must be seen in a broader sense.

In security settings, especially in IT security, where intentional cyber-attacks experience an increasing trend, probabilities seem to be insufficient for describing risks related to these attacks.

In the following, a general framework will be introduced that covers both safety and security. For this reason, we refer to the society of risk analysis (SRA) [11, SRA glossary, 2015], [10, Aven, 2014, Risk, Surprises and Black Swans.] and [15, Aven, 2007].

Threats are possible dangers exploiting vulnerabilities in information security systems. Based on SRA glossary [11, SRA glossary, 2015], the term threat covers both risk source (RS) and events

(A). Systems are constantly exposed to harmful events and risk sources and firewalls for example act as a barrier in IT structures and the occurrence of these harmful events and the consequences (C) depend on the performance of these barriers. [14, Amundrud, Aven & Flage, 2017]

For a better understanding of risk concept and threats we refer to a conceptual framework for linking risk, risk sources and events in the line of consequences and associated uncertainties (C, U) perspective based on [10, Aven, 2014]. This model will help with a better understanding of vulnerabilities within an organization later in this chapter.

Any attack in an information security system includes the sequence of ***Risk Source*** (RS), hazardous ***Events*** (A) and ***Consequences*** (C). System barriers as well as firewalls are set to protect the system against the Risk Sources. Systems are constantly exposed to different kind of Risk Sources and risk assessor has some ***uncertainty*** and some ***knowledge*** about these risk sources which could be expressed as the triplet (RS', Q, K). Note that Q is a measure of uncertainty (U) and RS' is the risk source specified by the assessor in risk assessment.

If system barriers fail to protect the system, the system may confront the actual risk Events (A) or the Events (A') that are specified by the assessor. Also, at the stage, the assessor has some uncertainties and some knowledge about risk Events (A) and the specified threats by the assessor could be described as (A', Q, K).

If system barriers fail to protect the system against risk Events (A), the system may confront the Consequences (C). Like the two previous stages, the assessor has some uncertainties and some knowledge regarding consequences the system will suffer from. The consequences specified by the assessor can be described as (C', Q, K).

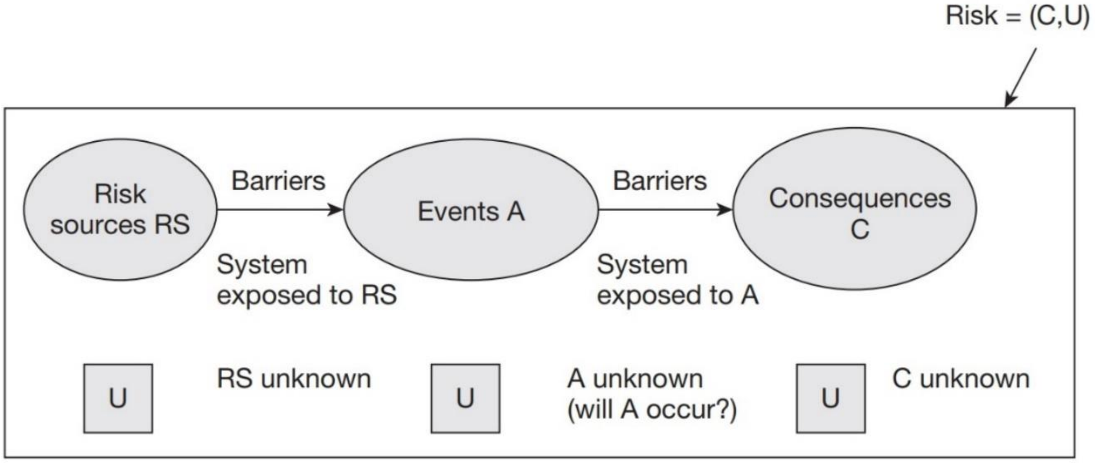


**Figure 3-1- A conceptual model linking risk, risk sources, events, and consequences. [10, Aven]**

The advantage of the setting above for defining risk concept is that when the assessor talks about threats, a better understanding of threats could be presented. A Threat can be defined as a pair of (A, U) and described by assessor as (A', Q, K). As mentioned earlier, the term threat (T) covers both risk source (RS) and events (A). Then, we may define a threat as (T, U) and describe a threat ***by an assessor*** as (T', Q, K). The triplet describes a threat/threats together with uncertainties about the occurrence of a threat and assessor's knowledge regarding the theat.

### 3.2.1 Safety versus Security

In SRA glossary, safe refers to being without unacceptable risk and when we say, safety is achieved, safety is interpreted the same way. In the same way, we refer to a system as secure when the system is being without unacceptable risk. By these definitions, it is clear that safe and secure mean one term.

### 3.2.2 Risk assessment characterisation

According to [14, Amundrud, Aven & Flage, 2017], an assessor would like to describe the future through the risk sources (RS'), events (A'), and the consequences (C'), and Q as a measure for describing uncertainty (U).

It is very important to note that the triplet (RS', A', C') is ***specified*** by the ***assessor***, and it may be different from what will happen in the real world. In the other words, (RS', A', C') may or may not ***cover*** the actual risk (RS, A, C).

We need to note that triplet (RS', A', C') and Q (measure of uncertainty) have been founded on a background knowledge (K) in the form of justified beliefs which is gained through historical data on cyber-attacks, surveys, software tests, argumentation, modeling, etc. So, if we update the risk description from before, it will be rewritten as (RS', A', C', Q, K). As it can be seen, the dimension of knowledge, or the strength of knowledge (SoK) needs to be ***included*** in description of risk.

As mentioned before, the term threat (T) covers both risk source (RS) and events (A) and the description of risk (RS', A', C', Q, K) could be also expressed as (T', C', Q, K).

### 3.2.3 Vulnerability Definition

It is almost impossible for an organization to implement an IT standard without having a deep understanding of vulnerabilities and how vulnerable their system can be.

In security context, it is common to define vulnerability as a weakness in a system that can be exploited by an attacker. Also, NIST defines vulnerability as "*a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.*" [2, page 18].

Here, NIST's definition of vulnerability can be challenged since the word "weakness" will not give the assessor a clear understanding of vulnerabilities. For this reason, we can refer to the following definition of vulnerability:

*"Vulnerability refers to the combination of consequences (C) of the activity and associated uncertainties (U),* ***given the occurrence*** *of a specific risk source/event (RS/A)."* [14, Amundrud, Aven & Flage, 2017]

The above statement could be written as (C, U|A). Vulnerability of a system should be expressed as the consequences of an attack (cyber-attack, leak of sensitive information etc.) on the system/organization (and the associated uncertainties regarding the attack) conditioned on the occurrence of an Event (A).

Also, vulnerability could be described by an assessor as (C', Q|RS'/A',K) or (C', Q, |T', K) which is interpreted as the combination of the specified consequences of an activity (attacks) on a system and associated uncertainties, given the occurrence of the specific Event (A'). the assessor's

Knowledge regarding the occurrence of the event needs to be expressed together with the within vulnerability description.

If the system's vulnerability is judged ***high***, then we can refer to the system as vulnerable and if the vulnerability is judged ***low***, then we can use the term ***robust***. (the term ***robust*** has not been mentioned in the literature of NIST)

In the following part, the strength of knowledge will be discussed.

### 3.2.4 Uncertainty assessment Q and Strength of knowledge (SoK)

So far, quantities of interest were discussed; Risk source (RS), hazardous event (A) and consequences (C). In this part, traditional and alternative ways to express uncertainties about these quantities are discussed.

#### 3.2.4.1 Use of probabilities

Use of probabilities to express the uncertainties about the quantities seems to satisfy the basic requirements for the presentation of uncertainties: [16, Bedford, 2001]

***Axioms*** which specify the formal properties of the uncertainty representation, ***Interpretations*** which connects the primitive terms in the axioms with phenomena observed and ***Measurement procedures*** which provides practical methods for interpretation of the axiom system.

The crucial point about using probabilities is that, whenever an assessor assigns probabilities, it can be interpreted as a subjective probability. For example, if the assessor assigns the probability of 0.10, it means that the assessor has the same ***uncertainty*** as randomly a specific ball will be drawn out of an urn where 10 balls exist. [17, Aven, 2013]

According to [14, Amundrud, Aven & Flage, 2017], based on an extensive review on security risk, the authors of the paper claim that only very a few experts are ***aware*** of the probabilities assigned to a quantity of interest. The reason the authors mention is that the assigned probability (0.10, random ball and urn) represents a main source of the ***poor communication*** between the security risk analyst and the other experts.

#### 3.2.4.2 Uncertainties and Background knowledge

NIST states that *"when a high degree of uncertainty in the assessment exists, organizations prefer to do a qualitative risk assessment rather than quantitative risk assessment."* [1, NIST] or regarding quantitative assessment, "*the meaning of the quantitative results may not always be clear and may require interpretation and explanation."* [2, page 23] Also, NIST acknowledges that *"uncertainty is inherent on the evaluation of risk due to imperfect knowledge of the threat."* [2, page 22]

Although NIST has made some efforts and more or less expresses its concern about the knowledge, it does not include any documentation about the strength of knowledge behind assigned probabilities.

A subjective probability can always be assigned to ***support*** decision-making. The issue with this probability is if the probability ***reflects*** a strong knowledge that will ***not*** be justified. [14, Amundrud, Aven & Flage, 2017] in the following the strength of knowledge will be discussed.

Subjective probabilities can be assigned to express uncertainties. The strength of knowledge supporting these probabilities can be either ***strong*** or ***weak***. Strength of knowledge or SoK is within the characteristic of assigned probabilities and probabilities should be expressed together with the strength of knowledge dimension (P, SoK). [8, Aven, 2015]

#### 3.2.4.3 Assessment of strength of knowledge

In order to measure the strength of knowledge of the assigned probabilities, we supplement these probabilities with a qualitative assessment of strength of knowledge.

Knowledge then will be classified under ***five*** categories from strong to weak. [19, Flage & Aven, 2009]

According to [10, Aven, 2014], Knowledge is ***Strong*** if:

- The assumptions made are reviewed to be very reasonable.
- Large amount of relevant data/information is available.
- There is a broad agreement among the experts.
- The phenomena involved are well understood
- Models are accurate and are known to give predictions with high accuracy.

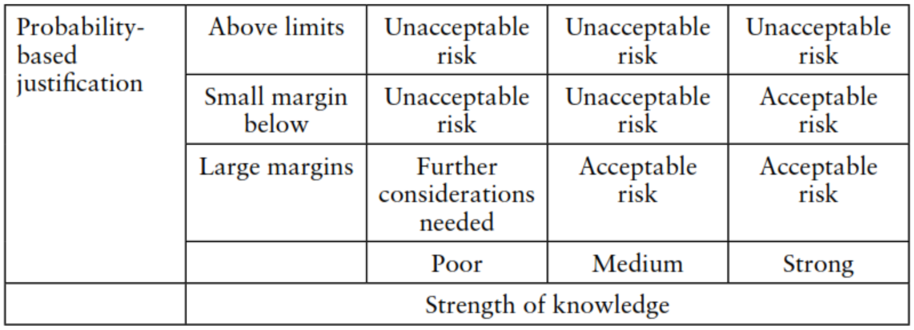
Knowledge is ***weak*** if:

- The assumptions made represent strong simplifications.
- Data are non-existent or highly unreliable.
- There is a disagreement among experts.
- The phenomena involved are poorly understood
- Models are non-existent or believed to give poor predictions.

Knowledge is ***medium*** if:

- We are somewhere between the above conditions.

The table below shows level of risk acceptance based on the level of knowledge.



| | | | | |
|---|---|---|---|---|
| Probability-based justification | Above limits | Unacceptable risk | Unacceptable risk | Unacceptable risk |
| | Small margin below | Unacceptable risk | Unacceptable risk | Acceptable risk |
| | Large margins | Further considerations needed | Acceptable risk | Acceptable risk |
| | | Poor | Medium | Strong |
| | Strength of knowledge | | | |

**Table 3-1-Risk acceptance based on the level of knowledge**

## 3.3 Comparison between standards

Before comparing the important different features of the standards, it is necessary to introduce ISO and OTCAVE standards briefly.

### 3.3.1 The ISO/IEC 27000-series

The ISO/ICE 27000-series (also ISMS/ISO27k) includes information security standards published by ISO and IEC. (ISO stands for international organization for standardization and IEC stands for International Electro technical Commission. ISO/IEC 27005 is all about information risk security and its content will be compared to NIST since they follow the same goal with different approaches.

**ISO/IEC 27005** does not specify nor recommend any risk management method and it is about a continual process of structured sequence of activities which is:

- Establishing risk management context.
- Assessing information quantitatively or qualitatively.
- Risk treatment.
- Informing stakeholders constantly.
- Monitoring and reviewing risk.

### 3.3.2 OTCAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

OCTAVE's framework is about helping organizations minimize their exposure to threats and determining of attack consequences and dealing with attacks. OCTAVE distinguishes three phases:

1. Phase 1: Building Asset-Based Threat Profiles
2. Phase 2: Identification of Infrastructure Vulnerabilities
3. Phase 3: Developing Security Strategy and Plans

### 3.3.3 Comparison of the features

In the following, different methodologies among the discussed standards will be given.

| STANDARD<br>FEATURES | NIST | ISO/IEC 27005 | OCTAVE |
|---|---|---|---|
| **Organizational (Methodology)** | -NIST's management permits third party execution.<br>-Most compatible with technology related risk assess.<br>-Rather tactical, organizational issues. | -Covering people, Process and Technology.<br>-Provides higher-level, management practices. | -It is self-directed.<br>-Only organizational resources permitted to implement the process. |
| **Organizational (Assessment team)** | -Mentioning different roles in methodology.<br>-Lack of creation of an assessment team. | -mentioning right people involved in the risk assessment | -Established an assessment team (both from organization's business and IT departments) |
| **Organizational (Information communication)** | -Using typical techniques for collecting information (Questionnaires, interviews) | -Similar methods to NIST<br>+ observing processes written in policies of organization. | -Workshop-based approach to gather information. |
| **Technical (Human resources)** | -Human resources are not organizational asset. | -Clearly covering human resource (Including employees, contractors, and third-party users.) | -Looks at human resources as mission-critical assets related to IT matters. |
| **Technical (Documentation)** | -Provides checklists for Security Requirements (Management, operational and technical areas.) | -Documents all security controls clauses explained in standard. (Clauses contain main security categories) | -Creates three catalogs: catalog of practice, threat profile, catalog of vulnerabilities |
| **Security-controlled driven? Or Risk focused?** | -Security-controlled driven | -Open approach to be chosen by the User | -Risk focused (Specifically cyber assaults) |

| | | | |
|---|---|---|---|
| **Complexity (Documentation)** | -High | -Moderate | -High |
| **Detailed quantitative analysis of security exposure?** | -Yes | -Yes | -No |
| **Users** | -Best practices for federal information systems. | -All organizations with different shapes and sizes | -Developed for larger organizations (200+ employees)<br>-Suits also smaller organizations. |

**Table 3-2- Comparison of Standards**

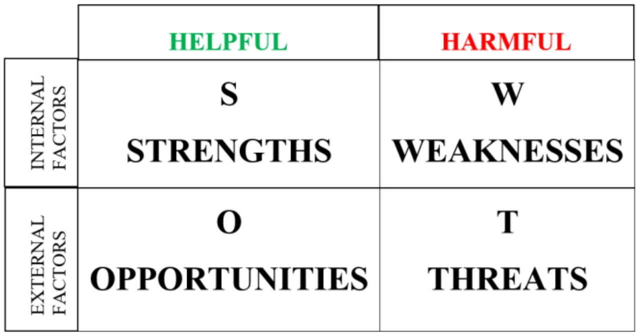
## 3.4 Further Recommendations

### 3.4.1 Threat Identification

Since NIST acknowledges that the risk management process could be a nonlinear process, so it could be better to identify the threats, characterize them, recognize the vulnerabilities before we step into Framing Risk. It should not bother the risk management process at all. There are organizations and businesses which are more interested in knowing clearly what the potential threats are at the beginning of the process.

### 3.4.2 SWOT Analysis

SWOT analysis could be a helping technique to measure the compatibility of the standard to the organization. An organization can adopt SWOT before implementing the standard. In SWOT analysis, strengths, weakness, opportunities, and threats are determined. In the following, SWOT matrix has been shown.



| | HELPFUL | HARMFUL |
|---|---|---|
| INTERNAL FACTORS | S<br>STRENGTHS | W<br>WEAKNESSES |
| EXTERNAL FACTORS | O<br>OPPORTUNITIES | T<br>THREATS |

**Figure 3-2-SWOT analysis Matrix**

For instance, SWOT analysis of NIST:

**Weaknesses:** generalized, …
**Strengths:** compatible with many organizations …
**Opportunities:** encourages the use of BAT (Best Available Technology)
**Threats:** Risk frame will need an update if newest version of attacks appear as surprises. (Since the standard is more control centered than threat-based)

### 3.4.3 Use of Red Teaming

Since NIST does not create an assessment team and it is organization’s duty to create one, in order to recognize the threats and attack and for a better assessment, read teaming could be a great help to the organization to have less surprises (Black swans) when it comes to attacks. In red teaming, which is introduced in [10, Aven, 2014], risk assessment has four processes. There are two analyst teams I and II.

***Stage 1***: Analyst team I performs risk analysis and describes risk as ($A_1$’, $C_1$’, $Q_1$, $K_1$)

($A_1$’, $C_1$’ are ***specific*** events and consequences identifies in the analysis, Q is a measure of uncertainty and K is background knowledge based on data, information, justified beliefs, …)

***Stage 2:*** Analyst team performing a self-evaluation of ($A_1$’, $C_1$’, $Q_1$, $K_1$) and focuses on the strength of knowledge $K_1$. The new risk description will be then: ($A_2$’, $C_2$’, $Q_2$, $K_2$). In many cases there will be no change in A’, C’ and Q.

***Stage 3:*** In stage three, the analyst team II will challenge the analyst team I and their assumptions and models. This is called as “the devil’s advocate”. They will argue the occurrence of events with negligible assigned probabilities and they look for so-called unknown knowns. The intention in stage three is to identify the potential surprises. (Black swans)

***Stage 4:*** In stage four, the two analyst teams will together establish risk description ($A_3$’, $C_3$’, $Q_3$, $K_3$) by means of the findings from both teams. This method can strengthen the decision-making process. In the following figure the whole process has been shown. [10 Aven, 2014]

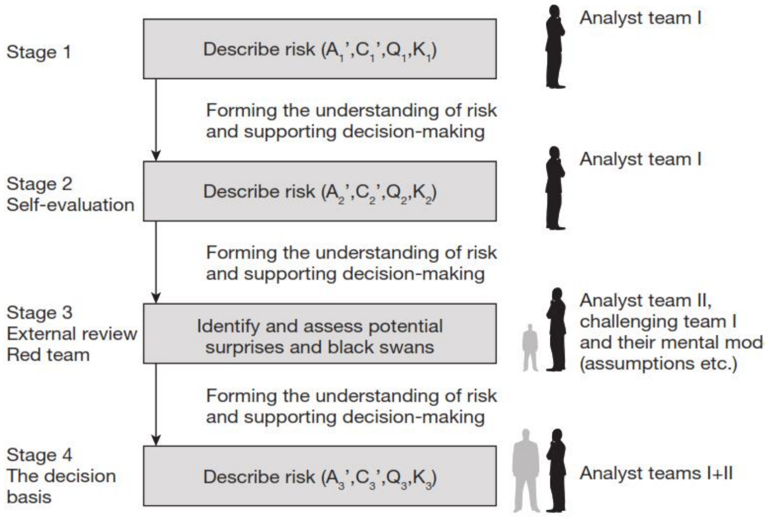

Stage 1
Describe risk (A1’,C1’,Q1,K1)
Analyst team I
Forming the understanding of risk and supporting decision-making
Stage 2 Self-evaluation
Describe risk (A2’,C2’,Q2,K2)
Analyst team I
Forming the understanding of risk and supporting decision-making
Stage 3 External review Red team
Identify and assess potential surprises and black swans
Analyst team II, challenging team I and their mental mod (assumptions etc.)
Forming the understanding of risk and supporting decision-making
Stage 4 The decision basis
Describe risk (A3’,C3’,Q3,K3)
Analyst teams I+II

**Figure 3-3-Two-team risk assessment approach**

# 4. DISSCUSION AND CONCLUSION

In previous chapters, NIST standard was reviewed, the weaknesses within its risk management framework were identified, discussed, and evaluated. Also, suggestions for improvement were introduced to add values to NIST standard in accordance with risk analysis and management science.

We return to risk concept. Since risk concept is generic, providing a sound and strong risk concept will enable the organizations to have a better understanding of risks and associated uncertainties and this will lead to a better implementation of the standard regardless of the type of the IT security standard.

It was discussed that it is redundant to define risk concept in ***two*** different way:

1. The common understanding of risk concept in security community as a triplet of asset-threat-vulnerability.
2. Risk as two-dimensional combination of consequences and associated uncertainties. [8, Aven, 2015].

It was shown that not only these two definitions are not in conflict but also the latter definition defines a generic risk concept that covers risk in safety, security, reputational, … contexts.

For this reason, first, values were identified and then threats (covering both Risk source (RS) and Events (A)) and consequences (C) related to these values were defined together with the associated uncertainties related to the occurrence of these Events.

After the concept of risk was established, risk was characterised as the basis of risk assessment through (T', C', Q, K) or (RS', A', C', Q, K), interpreted as specified threats and consequences with associated uncertainties based on the background knowledge of the ***assessor***. it was mentioned that these determined values may or may not cover the actual threats and consequences on the system.

Next, the strength of knowledge (SoK) was discussed where the knowledge of the assessor could be strong, weak, or medium with respect to the introduced criteria.

This way of risk characterizing risk could give any organization or system a sound description of risk in any context.

It was mentioned that ***vulnerability*** of a system should be defined as the combination of the consequences of an activity (cyber-attack, leak of sensitive information etc.) on the system/organization and the associated uncertainties conditioned on the occurrence of a specific Event (A), also expressed as (C, U|A). We described vulnerability as (C', Q, |T', K) which is interpreted as the specified consequences on the system/organization with the associated uncertainties regarding the threat given the occurrence of the specific Event (A'). the assessor's Knowledge regarding the occurrence of the event needs to be expressed together with the within vulnerability description.

Use of ***probabilities*** to express uncertainties about a quantity could be a useful tool for the assessor as long as the probabilities are seen together with the strength of knowledge behind these probabilities. Then, the pair (P, SoK) was introduced. The assessor considers the strength of knowledge while assigning the probabilities which could be an answer to NIST's problem regarding the semi-quantitative method for assigning probabilities when the uncertainty is high. NIST does not mention or consider the (P, SoK) pair. NIST assigns probabilities regardless of strength of knowledge behind the numbers or uses probability intervals in situations where the uncertainty is considered high.

Another point is that likelihood and ***uncertainty*** dimensions in the context of risk cannot be ignored if the management team wants to make accurate decision.

As discussed, NIST has a controlled-centered. An organization may choose to follow one of the two approaches. The point is that controlled-centered approach to IT risks may function slower than a threat-focused one. But it should be mentioned that the threat-focused approaches may not pay attention to the environment which they are applied in.

There is a misconception that organizations need to choose between several standards, and one is superior to the other. IT security standards have their own weaknesses and strengths. They can be combined and together to cover these weaknesses. The available IT security standards specify several processes to be followed, those processes make a generic framework at the end. They may be combined, or the sequences may be subjected to change. The standard may be applied internally to the organization itself or set controls for businesses the organization has with other businesses.

Regarding the risk management process of the existing IT security standards, NIST could be regarded as a complex standard since NIST 800-39 is used together with SP 800-37 and 800-30 that offer guidance for managing risk. This large number of documentations makes it quite difficult for the organizations to find clearly what they are trying to extract from the standard.

It was mentioned that since NIST is best suited for federal information systems and smaller organizations are not advised to use implement the standard.

NIST has a risk management framework which starts with categorizing the system. it categorizes the system ***without*** mentioning the words "threat" and uncertainties (U) associated with these threats. IT standards should prioritize threats in a world where an increasing trend of threats and cyberattacks has been observed. However, NIST acknowledges that the risk management process could be a nonlinear process, so it could be better to identify the threats, recognize the vulnerabilities before we step into Framing Risk. Furthermore, some organizations and businesses are more interested in knowing clearly what the potential threats are at the beginning of the process to consider them in their policies.

Since NIST standard lacks the creation of an assessment team and also does not instruct the organizations how to create an assessment team, involving red teaming in risk assessment process could be a helpful method to decrease uncertainties and provide the assessment team with a decision with lower degree of uncertainty and consequently less surprises.

SWOT analysis could be a helping technique to measure the compatibility of the standard to an organization. An organization may have a better understanding of strengths, weakness, opportunities, and threats it may confront by implementing the specific standard.

Appropriate implementation of any risk management framework requires the determination of the business impact and a clear picture of risk acceptance criteria of the organization. Also, strong knowledge of organizational risks is required while implementing any of these standards. All stakeholders must be involved; Senior management, IT professionals, information security experts and generally all those who a part of protecting organization's assets. This could be done only and only if all stakeholders at all level of the organization communicate and work together.

Here are some other points to bear in mind while implementing IT standards:

- A deep understanding of organizational risks and clearly determining organization's risk tolerance.
- Implementing the standard that best fits organization's goal.
- It is important to look at the chosen standard as a long-term coexisting element of the organization. A successful implementation of a standard requires a long-term practice and finding the weaknesses and strength within an organization.

# 5. Appendices

## 5.1 Appendix A - Risk Terminology

(Based on the Society for Risk Analysis [11, SRA, 2015] & [8, Aven, 2015])

**Knowledge:**

There are two types of knowledge:

Know-how skill and know-that of propositional knowledge (justified beliefs). Knowledge is gained through scientific methodologies and peer-review, experience, and testing.

**Uncertainty:**

Defined as lack of knowledge about observable quantities. (Uncertainty can be expressed by probabilities and it is recommended that uncertainty (U) will be expressed by probabilities (P) and the strength of knowledge (SoK) behind these probabilities.

(ISO and NIST do not include this definition.)

**Threat:**

Risk source commonly used in security applications.

**Threat regarding an attack:**

A stated or inferred intention to initiate an attack with the intention to inflict harm, fear, pain, or misery.

**Management review and judgement:**

Process of summarizing, interpreting, and deliberating over the results of risk assessment and other assessments, as well as of other relevant issues to make decisions.

**Risk assessment:**

Systematic process to comprehend the nature of risk, express and evaluate risk, with the available knowledge.

**Black swan (Surprises):**

A surprisingly extreme event relative to the present knowledge/beliefs.

Three types of such events:

- Unknown unknowns: Events that were completely unknown to the scientific environment.
- Unknown knowns: unknown events to some, known to others: Events that are not listed on the known events by the person who carried out a risk analysis, but the event is known to the others.

- Events that are on the list of known events in the risk analysis, but they are judged to have negligible probability of occurrence and believed not to occur.

## 5.2 Appendix B - Risk Models, Threats, Vulnerability, Adverse Impact (NIST)

### Risk Models

Risk models define risk factors to be assessed and the relationships between these factors. Risk models use factors to assess the overall level of risk and they can communicate level of risk. A good model includes communication components or a language for communicating to folks within management about where the risk level and it helps guide response to risk and includes details of scoring and evaluating the various factors, to define a risk and finally it must incorporate organizational risk culture (risk tolerance). Risk tolerance of an organization is defined as how much risk an organization can tolerate and what types of risk are tolerated and what risks are not. All the stated features help understand better the risk model introduced by NIST in the following.

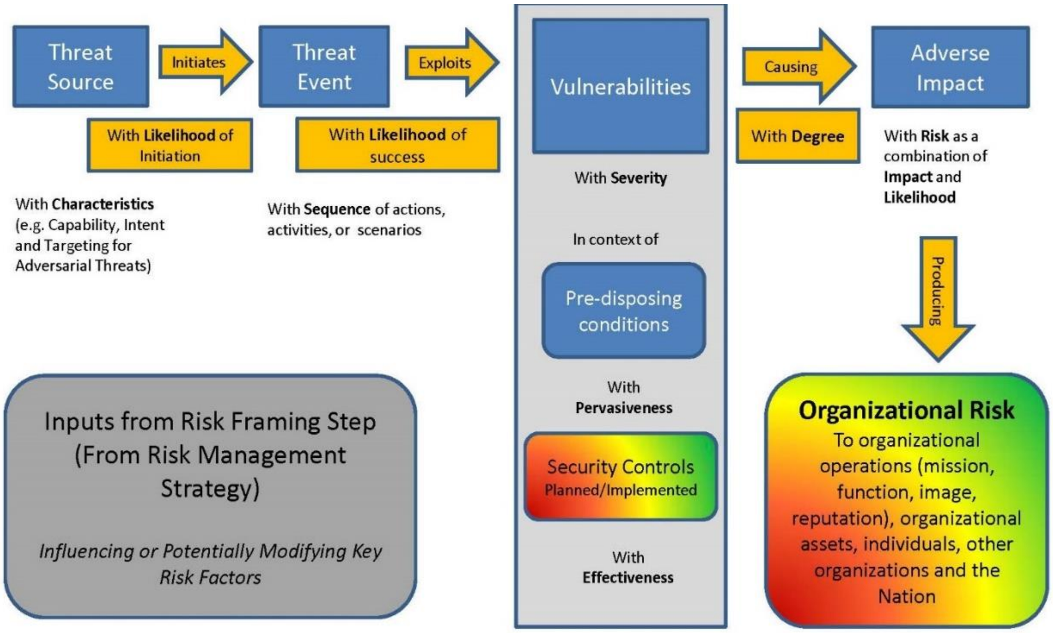

Threat Source
Initiates
Threat Event
Exploits
Vulnerabilities
Causing
Adverse Impact
With Likelihood of Initiation
With Likelihood of success
With Degree
With Risk as a combination of Impact and Likelihood
With Characteristics (e.g. Capability, Intent and Targeting for Adversarial Threats)
With Sequence of actions, activities, or scenarios
With Severity
In context of
Pre-disposing conditions
Producing
With Pervasiveness
Security Controls Planned/Implemented
With Effectiveness
Inputs from Risk Framing Step (From Risk Management Strategy)
Influencing or Potentially Modifying Key Risk Factors
Organizational Risk
To organizational operations (mission, function, image, reputation), organizational assets, individuals, other organizations and the Nation

**Figure B-1-Generic risk model with key risk factors- NIST SP800-30**

In this generic risk model, defined by NIST 800-30, the threat source in upper left initiates having some likelihood, initiating a threat event. The threat event consistent a sequence of actions, activities, or scenarios we have. And there is an agent undertaking things that are tempting to exploit vulnerabilities and the exploitation has some likelihood of success or not. The vulnerability exists with severity and with the context of predisposing conditions with pervasiveness. And there are security controls that can help mitigate vulnerabilities. So, we have threat source, threat events and vulnerabilities causing an adverse impact with risk as a combination of impact and likelihood where impact involves some damage or harm done to information assets or IT assets.

**Threats, Vulnerability, Adverse Impact:**

Threat is defined by any circumstance or event with the potential to adversely impact via unauthorized access, destruction, disclosure, or modification of information and/or denial of service.

A threat source is the intent and method targeted at the exploitation of vulnerability or a situation and method that may accidentally exploit vulnerability.

**Threat sources:**

Based on NIST 800-30 threat sources can be classified as following:

**Purposeful attacks** which are the purposeful attacks and they can be perpetrated by:

Individuals (both insiders and outsiders), Groups, organizations, and nation-States

**Human errors** which may be accidental and not on purpose but still we need to address how we are going to protect against them.

**Environmental disruptions** which may include bad weather and tornadoes.

**Structural** threats which may include equipment failures which may cause problems and cause that we lose the availability minimums.

## 5.3 Appendix C – More on NIST SP 800-39

**Governance Models**

| Type | Definition | Characteristics |
|---|---|---|
| **Centralized** | Authority, responsibility, and decision-making power are held by a central body. | Requires strong, well-informed central leadership.<br>Less autonomy for subordinate organization. |
| **Decentralized** | Authority, responsibility, and decision-making power are delegated to individual subordinate organizations. | Accommodates divergent mission/business needs at the cost of overall consistency.<br>Increased effectiveness with strong risk info sharing policies. |
| **Hybrid** | Authority, responsibility, and decision-making power are distributed between a central body and subordinate organizations. | Central body manages RM for decisions affecting entire organization.<br>Subordinate organizations manage RM for their specific missions |

**Table C-1-NIST governance models**

**Tasks of the four Components of Risk management**

**Step 1: Risk Framing**

| **TASK** | **TASK DESCRIPTION** |
|---|---|
| Task 1-1<br>RISK ASSUMPTIONS | Identify assumptions that affect how risk is assessed, responded to, and monitored within the organization. |
| Task 1-2<br>RISK CONSTRAINTS | Identify constraints on the conduct of risk assessment, risk response, and risk monitoring activities within the organization. |
| Task 1-3<br>RISK TOLERANCE | Identify the level of risk tolerance for the organization. |
| Task 1-4<br>PRIORITIES AND TRADEOFFS | Identify priorities and trade-offs considered by the organization in managing risk. |

**Step 2: Risk Assessment**

| **TASK** | **TASK DESCRIPTION** |
|---|---|
| Task 2-1<br>THREAT AND VULNERABILITY IDENTIFICATION | Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate. |
| Task 2-2<br>RISK DETERMINATION | Determine the risk to organizational operations and assets, individuals, other organizations, and the Nation if identified threats exploit identified vulnerabilities. |

**Step 3: Risk Response**

| **TASK** | **TASK DESCRIPTION** |
|---|---|
| Task 3-1<br>RISK RESPONSE IDENTIFICATION | Identify alternative courses of action to respond to risk determined during the risk assessment. |
| Task 3-2<br>EVALUATION OF ALTERNATIVES | Evaluate alternative courses of action for responding to risk |
| Task 3-3<br>RISK RESPONSE DECISION | Decide on the appropriate course of action for responding to risk. |

| | |
|---|---|
| Task 3-4<br>RISK RESPONSE IMPLEMENTATION | Implement the course of action selected to respond to risk. |

**Step 4: Risk Monitoring**

| **TASK** | **TASK DESCRIPTION** |
|---|---|
| Task 4-1<br>RISK MONITORING STRATEGY | Develop a risk monitoring strategy for the organization that includes the purpose, type, and frequency of monitoring activities. |
| Task 4-2<br>RISK MONITORING | Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes. |

## 5.4 Appendix D – More on NIST 800-30 Revision 1

**Risk Assessment approaches**

We have 3 different approaches to assess risk: Quantitative, qualitative, and semi-quantitative.

***Quantitative*****:** It is based on numbers where proportionality of values is maintained in and out of the context of the assessment, higher degree of repeatability. Qualitative-like subjective interpretations may still be involved. Benefits may be outweighed by costs in time, effort, and tools.

***Qualitative***:

It is based on non-numerical levels such as low, moderate, and high. Results are typically easier to convey to decision makers. Extra work is required to ensure repeatability and reproducibility.

***Semi-Quantitative*****:** (somehow qualitative with just a more granular scale)

It is based on scales or representative numbers whose values/proportions are not maintained in other contexts, e.g., 0-15, 16-35, 35-70, 71-85, 86-100). In the other words, it is just a way for making designation more granular and it might help prioritize risk and have a better understanding of where we are standing. ***Expert judgment is needed to assign values appropriately/reduce subjectivity.***

**Analysis approaches**

***Threat-oriented*** approach which starts with identification of the threat sources.

***Asset/impact-oriented*** approach which starts with identification of high value assets or highly adverse impacts.

***Vulnerability-oriented*** approach which starts which predisposing conditions or exploitable weaknesses in systems or environments of operation.

There are a few other types of analysis which may come to consideration:

***Graph-based analysis*** which allows the use of specific threat events to generate multiple attack scenarios.

***Rigorous analysis*** which is used to account for the many-to-many relationships between risk factors.

**The steps of risk management framework:**

**Step 1 – Categorize**

It uses initial risk assessment results to inform impact analysis for appropriate categorization: what information is being processed on this system, the impact of it, both from the standpoint of confidentiality and integrity and availability and the risk assessment results might help by revealing what the impacts are.

Prepare for security control selection. (by knowing what risks are and might be associated with and what controls can be used to mitigate that)

**Step 2 – Select**

It uses initial risk assessment results during control selection to tailor the baseline appropriately, and to identify common controls with potential single points of failure. (Controls provided by another entity implemented at system level.)

It uses updated risk assessments to modify initial control selection based on most recent threat and vulnerability data: There might be need of going back and if new threats emerge then we need to add new control and go back to step two in the risk management framework and select some new controls.

**Step 3 – Implement**

There are different ways of implementation of risk assessment and the key is to choose the most effective way by using the initial risk assessment results to determine most effective way to implement controls and cost-benefit analysis and/or risk tradeoffs.

It uses updated risk assessments to help determine if the current implementation is still effective.

**Step 4 – Assess**

It assesses if all the implemented controls work effectively by using the initial or updated risk assessment results to determine the type of security assessment to be conducted, frequency of security assessments, level of rigor for security assessments, assessment methods used, and number of objects assessed. It also uses the results from control assessments to identify residual risk (vulnerabilities) and the updated risk assessment results to determine severity of residual risk (vulnerabilities)

**Step 5 – Authorize**

It uses initial or updated risk assessment results to inform authorizing officials as they make risk-based decisions to approve authorization to operation, deny authorization to operate and require additional safeguards.

**Step 6 – Monitor**

If the controls are effective and what is risk if they are not or if there is a problem at some level. It updates risk assessments during monitoring step based on ongoing effectiveness of security controls, changes to systems and environments of operation and compliance with policies. Monitoring results provide information on new vulnerabilities to be addressed through the risk assessment process.

## NIST 800-30 Appendices

Since NIST 800-30 provides supplementary information regarding risk assessment in appendices which must be used together with its literature, the list of appendices and their application is given below:

**A/B/C: References, Glossary, and Acronyms respectively**

**D: Threat sources**

Table D1: Inputs to threat SOURCE identification.
Table D2: Taxonomy of Threat Sources.
Table D3: Assessment scale for adversary capability.
Table D4: Assessment scale for adversary intent.
Table D5: Characteristics of adversary targeting.
Table D6: Assessment scale for range of effects.
Table D7: Template for ID of adversarial threat sources.
Table D8: Template for ID of non-adversarial threat sources.

**E: Threat events**

Table E1: Inputs to threat EVENT identification.
Table E2: Examples of Adversarial Threat Events.
Table E3: Examples of NON-Adversarial Threat Events.
Table E4: Relevance of Threat Events.
Table E5: Template for ID of Threat Events

**F: Vulnerabilities and predisposing conditions**

Table F1: Inputs-Vulnerabilities/Predisposing Conditions.

Table F2: Assessment scale for Vulnerability Severity.
Table F3: Template for ID of Vulnerabilities.
Table F4: Taxonomy of Predisposing Conditions.
Table F5: Assessment scale for pervasiveness of predisposing conditions.
Table F6: Template for ID of Predisposing Conditions.

**G: Likelihood of occurrence**

Table G1: Inputs to determination of likelihood.
Table G2: Assessment scale for likelihood of adversarial event initiation.
Table G3: Assessment scale for likelihood of non- adversarial event initiation.
Table G4: Assessment scale for likelihood of threat event resulting in adverse impacts.
Table G5: Assessment scale for overall likelihood.

**H: Impact**

Table H1: Inputs to determination of impact.
Table H2: Examples of adverse impacts.
Table H3: Assessment scale for impact of threat events.
Table H4: Assessment scale for range of effects of threat events.
Table H5: Template for ID of adverse impacts.

**I: Risk**

Table I1: Inputs to determination of risk.
Table I2: Assessment scale for level of risk.
Table I3: Assessment scale for level of risk combining likelihood and impact
Table I4: Column descriptions for adversarial risk table.
Table I5: Template for adversarial risks.
Table I6: Column descriptions for non-adversarial risk table.
Table I7: Template for non-adversarial risks.

**J: Risk prioritization**

**K: Summary of Tasks**

## 5.5 Appendix E – More on uncertainty

### NIST's statement on Uncertainty

The term uncertainty has been mentioned several times in NIST standard and in the following, these statements on uncertainty are given as:

Uncertainty is inherent on the evaluation of risk due to: [2, NIST]

- Future will not necessarily resemble the past.

- Imperfect knowledge of the threat.
- Hidden vulnerabilities in the technologies in use.
- Unrecognized dependencies which may lead to unpredicted impacts.

Risk tolerance is the level of risk or degree of uncertainty and uncertainty can affect risk tolerance of an organization. [1, NIST] & [2, NIST]

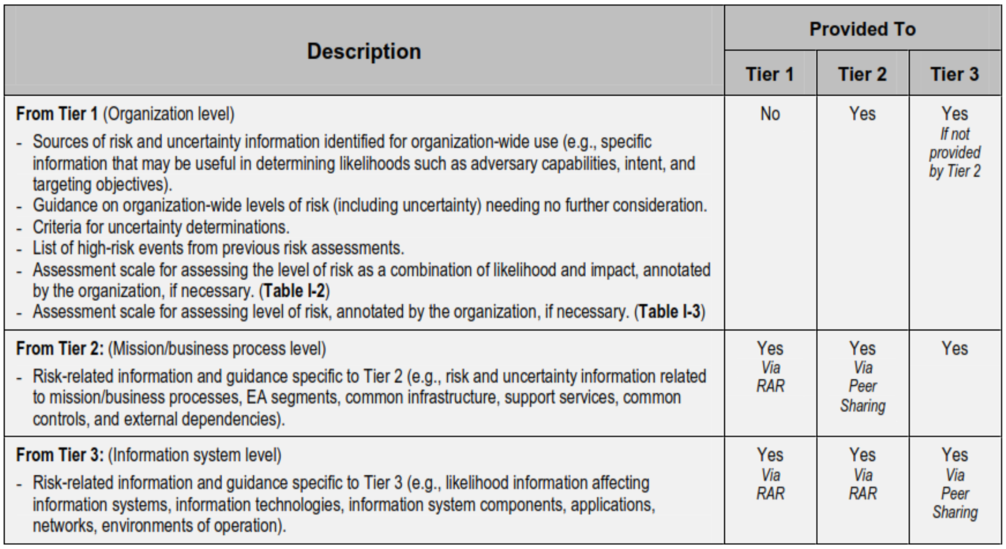
The second step in risk assessment is to conduct the risk assessment. To accomplish this, the organization must prioritize risks by analyzing threats and vulnerabilities and associated uncertainties with risk assessment. [2, NIST]

When it comes to threats, risk determination could be coarse due to uncertainty in likelihood of occurrence and impact values and secondly the potential mischaracterization of threats. [2, NIST]

When a high degree of uncertainty in the assessment exists, organizations prefer to do a qualitative risk assessment rather than quantitative risk assessment. (Since the role of expert in assigning values is more evident and that) [1, NIST]

In framing risk (the first step of risk management based on NIST), risk assumptions, risk constraints, priorities and tradeoffs, risk tolerance and uncertainty must be involved. [2, NIST]

In the following, Table I-1 [2, page 86] provides input to risk and uncertainty determination task.



| Description | Provided To | | |
|---|---|---|---|
| | Tier 1 | Tier 2 | Tier 3 |
| **From Tier 1** (Organization level)<br>- Sources of risk and uncertainty information identified for organization-wide use (e.g., specific information that may be useful in determining likelihoods such as adversary capabilities, intent, and targeting objectives).<br>- Guidance on organization-wide levels of risk (including uncertainty) needing no further consideration.<br>- Criteria for uncertainty determinations.<br>- List of high-risk events from previous risk assessments.<br>- Assessment scale for assessing the level of risk as a combination of likelihood and impact, annotated by the organization, if necessary. (**Table I-2**)<br>- Assessment scale for assessing level of risk, annotated by the organization, if necessary. (**Table I-3**) | No | Yes | Yes<br>*If not provided by Tier 2* |
| **From Tier 2:** (Mission/business process level)<br>- Risk-related information and guidance specific to Tier 2 (e.g., risk and uncertainty information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). | Yes<br>*Via RAR* | Yes<br>*Via Peer Sharing* | Yes |
| **From Tier 3:** (Information system level)<br>- Risk-related information and guidance specific to Tier 3 (e.g., likelihood information affecting information systems, information technologies, information system components, applications, networks, environments of operation). | Yes<br>*Via RAR* | Yes<br>*Via RAR* | Yes<br>*Via Peer Sharing* |

**Table E-1-Inputs-Risk-Uncertainty**

## A broader view on uncertainty

The need to have a deep understanding of uncertainty in IT security plays an important role in avoiding threats and the devastating consequences as much as possible. As the whole literature of NIST on certainty has been given above, it could be observed that, the concept of uncertainty has not been developed enough and could be brought to the higher levels where we can establish a better understanding of this important component of risk. It will also improve the quality of risk executive function RE(F) that in NIST standards, a person or a group of people may be in charge of establishing it and it will strengthen the background knowledge and reduces the uncertainties associated with it.

For this reason, we can refer to Risk analysis [8, Aven, 2015] and Risk, Surprises and Black Swans [10 Aven, 2014], where the concept of uncertainty has been fully developed and discussed.

**Uncertainty definition**

Qualitative description of uncertainty: [11, SRA glossary, 2015]

- For a person/group of people is not knowing the absolute value of quality or future consequences of an activity.
- Imperfect information/knowledge about a hypothesis, quantities, or occurrence of an event.

Uncertainty metrics:

- A subjective probability
- The pair (Q, K), where Q is a measure of uncertainty and K is the background knowledge supporting Q.

Uncertainty could be defined as lack of knowledge about observable quantities and it can be expressed by probabilities. It is recommended that uncertainty (U) will be expressed by probabilities (P) and the strength of knowledge (SoK) behind these probabilities. [8, Aven, 2015]. (ISO and NIST do not include this definition.)

**Decision-making under uncertainty**

Decision-making processes involve uncertainties and high risks. [13, Aven, 2003] has introduced a model decision making under uncertainty. The elements are:

- Decision situation stakeholders
- Goal setting, preferences, and performance measure
- Use of different analysis to support the decision-making.

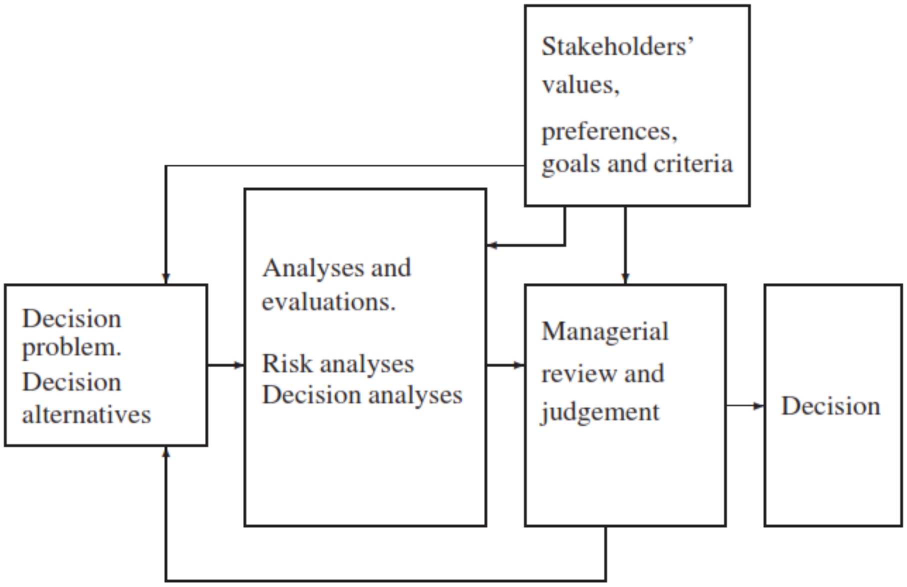

Stakeholders' values, preferences, goals and criteria
Decision problem. Decision alternatives
Analyses and evaluations.
Risk analyses Decision analyses
Managerial review and judgement
Decision

**Figure E-1 Decision-making under uncertainty [13, Aven, 2003]**

Managerial review and judgement are a final step before decision-maker makes the final decision. (Managerial review will be discussed completely in Appendix A.). Following the model carefully, it gives the decision-makers the possibility to document and trace the process.

There other important aspect of the process is the background information of the analysis. What assumptions were made for the analysis?

Since the first pier in NIST is the organizational tier and senior leaders are in charge of the outlines and strategies which will be implemented in tiers 2 and 3, it's the responsibility of CEO (decision-maker, manager) to undertake considerations and weigh the information with respect to uncertainty in order to balance different concerns. [8, Aven, 2015]

# REFERENCES

[1] NIST, N. I. o. S. a. T.-. (2011). SP800-39 Managing Information Security Risk in (pp. 88). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-39/final

[2] NIST, N. I. o. S. a. T.-. (2012). SP800-30 Guide for Conducting Risk Assessments in (pp. 95). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[3] John R. Vacca. 2009. Computer and Information Security Handbook. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[4] Wade Baker. 2015. Threat Intelligence within the Risk Management Process

[5] Nathaniel L. Hunstad. 2011. The Application of NIST Special Publication 800-39 for Small Businesses and Organizations By

[6] *Haes, S.D.; Grembergen, W.V. (2015).* "Chapter 5: COBIT as a Framework for Enterprise Governance of IT". *Enterprise Governance of Information Technology: Achieving Alignment and Value*, Featuring COBIT 5 (2nd ed.). Springer. pp. 103–128. ISBN 9783319145471. Retrieved 24 June 2016.

[7] Rene Rivera, 2004, Comparison of the OCTAVE and NIST's Special Publication 800-30 Methodologies, University of Houston, ITEC 6324

[8] Aven, T. (2015), Risk Analysis, John Wiley & Sons.

[9] Aven, T. (2003). How to approach risk and uncertainty to support decision-making. Wiley, N.Y.

[10] Aven, T. (2014). Risk, Surprises and Black Swans. London: Routledge, https://doi-org.ezproxy.uis.no/10.4324/9781315755175

[11] Aven, T., Ben-Haim, Y., Andersen, H. B., Cox, T., Droguett, E. L., Greenberg, M., Thompson, K. M. (2015). SRA glossary. The Society for Risk Analysis

[12] OCTAVE$^{SM}$ Method Implementation Guide Version 2.0 Volume 1: Introduction Christopher J. Alberts Audrey J. Dorofee June 2001

[13] Aven, T. (2003) Foundations of Risk Analysis. John Wiley & Sons Ltd., New York, NY.

[14] Amundrud, Ø., Aven, T., & Flage, R. (2017). How the definition of security risk can be made compatible with safety definitions. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 231(3), 286–294. https://doi.org/10.1177/1748006X17699145

[15] Aven T. A unified framework for risk and vulnerability analysis and management covering both safety and security. Reliab Eng Syst Safe 2007; 92: 745–754.

[16] Bedford T and Cooke R. Probabilistic risk analysis. Cambridge: Cambridge University Press, 2001, p.20.

[17] Aven T. How to define and interpret a probability in a risk and safety setting (Discussion paper with general introduction by Reniers G). Safety Sci 2013; 51: 223–231

[18] Aven T, Baraldi P, Flage R, and Zio E. Uncertainty in risk assessments. New York: Wiley, 2014, p.46.

[19] Flage, R. and Aven, T. (2009) Expressing and communicating uncertainty in relation to quantitative risk analysis (QRA). Reliability and Risk Analysis: Theory and Applications, 2(13), 9–18

[20] International Organization for Standardization - International Electrotechnical Commission Joint Technical Committee1, ISO/IEC 27002- Information technology -- Security techniques -- Information security management systems -- Requirements, 2007.

[21] International Organization for Standardization-International Electrotechnical Commission Joint Technical Committee1, ISO/IEC 17799 Information technology — Security techniques — Code of practice for information security management, 2005.

[22] National Institute for Standards and Technology, An introduction to Computer Security – The NIST Handbook – SP 80012, NIST 1995, http://csrc.nist.gov.

[23] Information Security Forum, The Standard of Good Practice for Information Security, ISF 2007, https://www.isfsecuritystandard.com/SOG P07/index.htm.

[24] Erik Guldentops, Tony Betts, Gary Hodgkiss, Aligning COBIT, ITIL and ISO 17799 for Business Benefit, http://www.isaca.org 2007

[25] Jimmy Heschl, Cobit Mapping: Overview of International IT Guidance - 2nd edition, IT Governance Institute USA http://www.isaca.org 2007

[26] Federal Office for Information Security (BSI), BSI Standard 100-1 Information Security Management System, http://www.bsi.de/english/publications/bsi _standards/index.htm 2008

[27] Maclean, Don. The NIST Risk Management Framework: Problems and recommendations. A Peer-Reviewed Journal, Volume 1 / Number 3 / Winter 2017–18, pp. 207-217(11)

[28] Federal Office for Information Security (BSI), BSI Standard 100-2 IT-Grundschutz Methodology, http://www.bsi.de/english/publications/bsi _standards/index.htm 2008

[29] Federal Office for Information Security (BSI), BSI Standard 100-3 Risk Analysis based on IT-Grundschutz, http://www.bsi.de/english/publications/bsi _standards/index.htm 2008.

[30] An Overview of Information Security Standards, The Government of the Hong Kong Special Administrative Region, 2008, www.infosec.gov.hk/english/technical/files /overview.pdf

[31]https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/is-the-nist-cybersecurity-framework-enough-to-protect-your-organization

[32] https://www.sisainfosec.com/blogs/comparison-between-iso-27005-octave-nist-sp-800-30/

[33] https://threatconnect.com/blog/threat-intelligence-within-risk-management/