Comparison of Risk Functions

Christian Franck Jayanta Poray
Petr Sobeslavský

University of Luxembourg

January 31st, 2008

Abstract

A comparison of the risk functions of NIST and MEHARI, NIST and Octave Allegro, and NIST and Security Pattern. The possible inputs and the possible outputs as well as the calculation of the risks are analysed in detail. Eventually there is a discussion about a common core, followed by a suggestion of an abstract model which can contain all of the existing models.

Contents

Chapter 1

Introduction

A core step in risk management is the calculation of the existing risks. Different methodologies do this in different ways. We look at the risk functions that are used in NIST, MEHARI, Octave Allegro and Security Pattern.

We assume in this document that all the work related to identification and the valuation of the inputs has already been made, and that the inputs are readily available.

First we analyse the risk functions which are used in the different methodologies. We explain what the inputs and the outputs of the risk functions are and how the risk is calculated.

In a second part, we compare NIST with MEHARI, NIST with Octave Allegro, and finally NIST with Security Pattern. We point out the similarities and the differences between the risk functions of these methods.

Finally, we attempt to identify a common core to all of the risk functions, and we try to find an abstract model which can contains all of them.

Part I

Risk functions in different methodologies

Chapter 2

NIST[1]

2.1 Overview

As illustrated in the following figure, the risk associated to a threat is determined based on the values of impact and likelihood. Both values can be described in a quantitative or in a qualitative way.

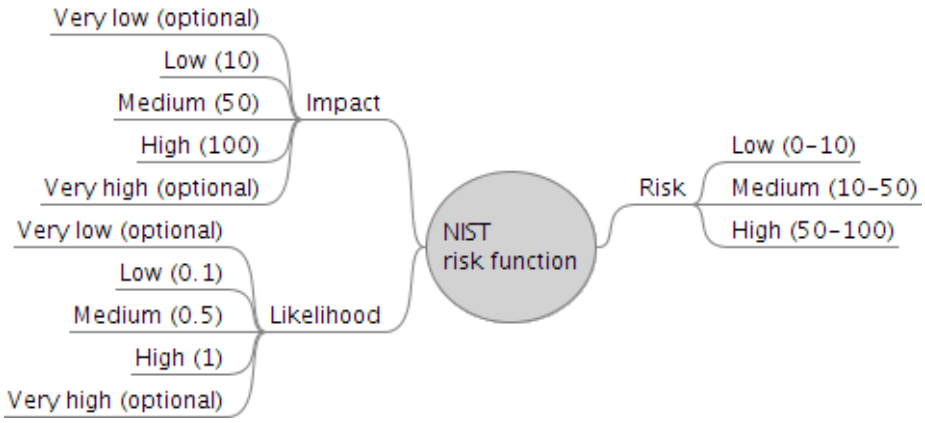

Figure 2.1: NIST risk function overview

2.2 Inputs

2.2.1 Impact

The impact of a successful threat exercise of a vulnerability, depends on the mission of the system, of the criticality and the sensitivity of the data.

[1] The information found in this chapter is mainly based and partially extracted from [1] and [3].

Quantitative measures

If it possible to quantify the impact in terms of lost revenue, cost of repairing and similar measurable values, then it is possible to express the impact with a value between 1 and 100.

Qualitative measures

If it not possible to quantitatively measure the impact (intangible assets), it is possible to use a qualitative scale. Often a 3 level scale is used in the NIST approach[2] :

1. **High:** Exercise of this vulnerability will have serious consequences. It may result in very costly loss of resources, significant harm to the organisation, serious injury or human death.
2. **Medium:** Exercise of this vulnerability may result in costly loss of resources, harm to the organisation or result in human injury.
3. **Low:** Exercise of this vulnerability may result in the loss of some resources and may noticeably affect the functioning of the organisation.

The mapping of quantitative to qualitative values is as follows: 1-10 is low, >10-50 is medium and >50-100 is high.

2.2.2 Likelihood

To evaluate the likelihood, the threat source motivation and capability, the nature of the vulnerability and the existence and effectiveness of current controls have to be considered.

Quantitative measures

If it possible to quantify the likelihood, then it is possible to express the likelihood with a value between 0 and 1.

Qualitative measures

In a qualitative approach, there are usually 3 levels:

1. **High:** There is a high reason to believe that this will happen and there are no effective controls to prevent the vulnerability from being exercised.
2. **Medium:** There is reason to believe that this will happen, but there are controls in place which can help to prevent the vulnerability from being exercised.
3. **Low:** It is unlikely that this will happen and controls are in place which should prevent the vulnerability from being exercised.

The probabilities assigned for each threat likelihood level are: 1.0 for High, 0.5 for Medium and 0.1 for Low.

[2]Depending on the granularity required the 3x3 matrix can be expanded to a 4x4 or 5x5 matrix, adding 'very high' and 'very low' impacts.

2.3 Risk function evaluation

Basically, the risk value is obtained by multiplying the likelihood and the impact of a threat. The following table shows how to determine the risk based on quantitative or qualitative impact and likelihood values.

Impact	Likelihood: Low 0.1	Likelihood: Medium 0.5	Likelihood: High 1.0
High 100	Low risk 100 x 0.1 = 10	Medium risk 100 x 0.5 = 50	High risk 100 x 1.0 = 100
Medium 50	Low risk 50 x 0.1 = 5	Medium risk 50 x 0.5 = 25	Medium risk 50 x 1.0 = 50
Low 10	Low risk 10 x 0.1 = 1	Low risk 10 x 0.5 = 5	Low risk 10 x 1.0 = 10

Figure 2.2: NIST risk evaluation table

2.3.1 Description of risk levels

1. **High:** There is a strong need to put in place corrective measures as soon as possible.
2. **Medium:** Within a reasonable period of time, corrective measures should be taken..
3. **Low:** Correctives measures can be taken or the risk can just be accepted.

Chapter 3

MEHARI[1]

3.1 Overview

As illustrated in the following figure, the risk associated to a threat is determined based on the values of impact and likelihood. Both values are described in a qualitative way.

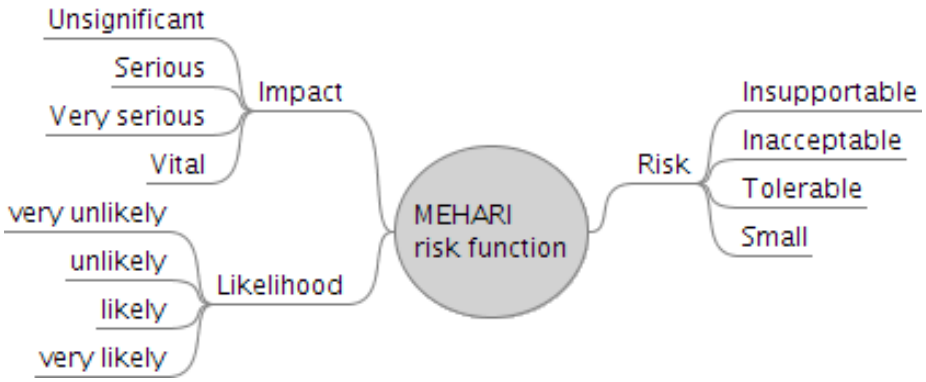

Figure 3.1: MEHARI risk function overview

3.2 Inputs

3.2.1 Impact

The magnitude of impact is one of the following values:

1. **Unsignificant:** Practically no noticeable impact on the results of the organisation or on its image.
2. **Serious:** Marked impact on the operations, but consequences are supportable.

[1] The information found in this chapter is mainly based and partially extracted from [1] and [2].

3. **Very serious:** Very serious malfunctions of the organisation, without necessarily compromising its future.

4. **Vital:** Very serious impact endangering the survival of the organisation,

3.2.2 Likelihood

The magnitude of likelihood is one of the following values . These values take into consideration all already implemented controls.

1. **Very unlikely:** It is very unlikely that the risk scenario occurs.

2. **Unlikely:** This scenario, reasonably, could be considered never to happen.

3. **Likely:** This scenario could easily occur in more or less short term.

4. **Very likely:** The scenario can be considered to certainly occur in a relatively short term.

3.3 Risk function evaluation

The risk for a threat is evaluated using the following table.

Impact \ Likelihood	Very unlikely	Unlikely	Likely	Very likely
Vital	Tolerable risk	Inacceptable risk	Intolerable risk	Intolerable risk
Very serious	Tolerable risk	Inacceptable risk	Inacceptable risk	Intolerable risk
Serious	Small risk	Tolerable risk	Tolerable risk	Inacceptable risk
Unsignificant	Small risk	Small risk	Small risk	Tolerable risk

Figure 3.2: MEHARI risk evaluation table

Immediate reaction is required for insupportable and unacceptable risks. Tolerable or small risks could be accepted.

Chapter 4

OCTAVE Allegro[1]

4.1 Overview

As shown in the following figure the risk associated to a threat is evaluated from its impact on different impact areas and probability:

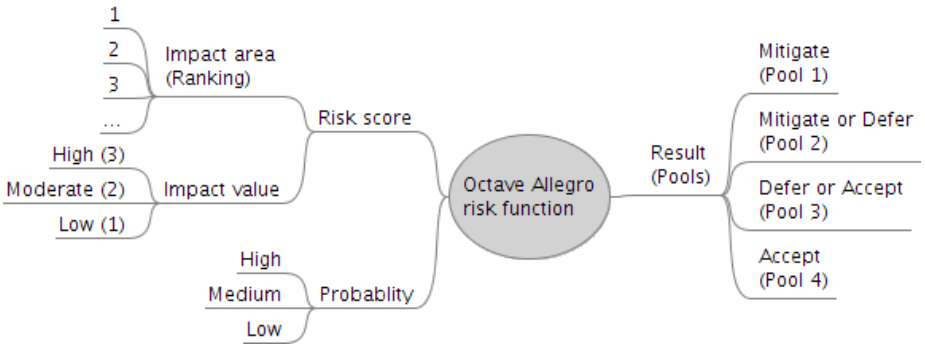

Figure 4.1: Octave allegro risk function overview

4.2 Inputs

4.2.1 Impact area

At first general impact areas are identified and ranked according to its importance for the organization.

4.2.2 Impact value

Impact values are assigned quantitative values as follows:

- **High:** This corresponds to 3.

[1] The information found in this chapter is mainly based and partially extracted from [5].

- **Moderate:** This corresponds to 2.
- **Low:** This corresponds to 1.

4.2.3 Probability

Probability of each risk is evaluated on a qualitative scale with the values:

- **High**
- **Medium**
- **Low**

4.3 Risk evaluation

4.3.1 Risk score

For each risk its impact on each impact area is evaluated and a following table is created. The risk score is then a sum of impacts on impact areas.

Impact area	Ranking	Impact value	Score
Impact area 1	R1	IV1	S1 = R1 * IV1
Impact area 2	R2	IV2	S2 = R2 * IV2
Impact area 3	R3	IV3	S3 = R3 * IV3
Impact area 4	R4	IV4	S4 = R4 * IV4
Impact area 5	R5	IV5	S5 = R5 * IV5

Total score:	S = S1 + S2 + S3 + S4 + S5

Figure 4.2: Risk score

4.3.2 Risk function

The threats are assigned to one of four pools, according to the relative risk matrix shown in figure 4.3.

4.3.3 Description of the pools

The pools which indicate the mitigation approach to take for a threat:

- **Pool 1:** Mitigate
- **Pool 2:** Mitigate or Defer
- **Pool 3:** Defer or Accept
- **Pool 4:** Accept

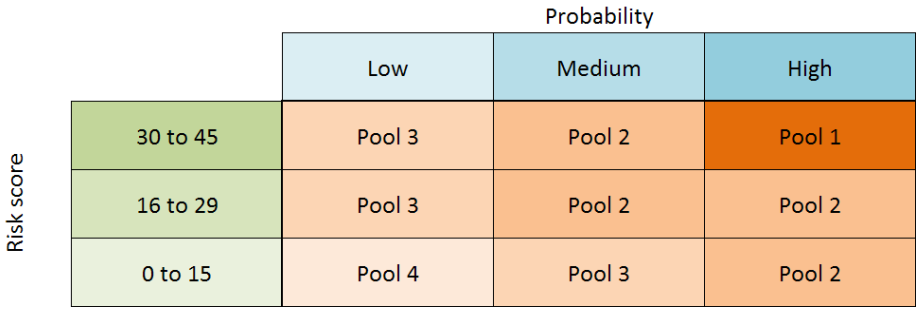

Figure 4.3: Relative risk matrix

Chapter 5

Security pattern[1]

5.1 Overview

In security pattern, the risk that exits for a given asset is determined based on the values of threat, vulnerability and asset value. Values are described in a qualitative way.

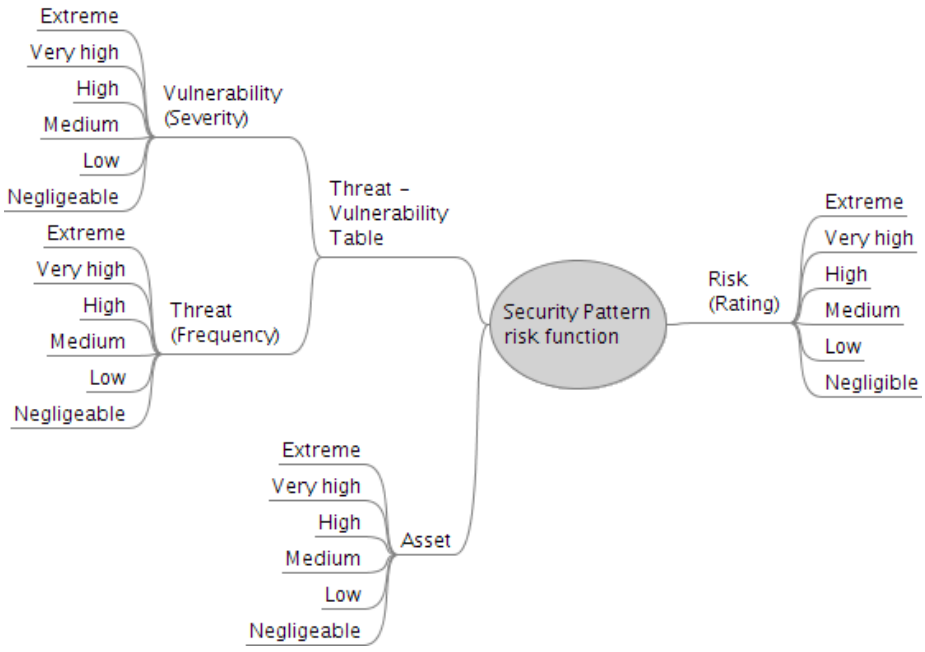

Figure 5.1: Overview Security patterns risk function

[1] The information found in this chapter is mainly based and partially extracted from [4].

5.2 Inputs

5.2.1 Threats

A threat is any action or event with the potential to cause harm (based on ISO/IECIS 13335-1). There are several causes of threats like environmental issues (flood, earthquake, storm), organizational management problem, human errors, technical failures, deliberate acts (hacking, theft, use of malicious codes etc.) Possible threat values are:

1. **Negligible:** The occurrence of this threat action is very unlikely within a human lifetime.
2. **Low:** The threat action rarely takes place.
3. **Medium:** The threat action occurs infrequently.
4. **High:** The threat action regularly happens.
5. **Very high:** The threat action occurs very often.
6. **Extreme:** The threat action is continually occurring.

5.2.2 Vulnerability

Vulnerability is the measure of weakness for the organization. Vulnerabilities can be physical (no access control, no guards), logical (no security patch, no anti-spyware) or network related (no security gates).

1. **Negligible:** This is a theoretical vulnerability only exploitable with massive infrastructure or computing power, or a minor distraction to business processes and no compromise of security properties would occur.
2. **Low:** The vulnerability would be very difficult to exploit, with no real gain, or slight disruption of service or mild compromise of security properties would occur.
3. **Medium:** The vulnerability is difficult to exploit, and exposes some systems, or significant disruption of service and compromise of confidentiality, availability, or integrity of assets would occur.
4. **High:** Exploiting the vulnerability would be a challenge but it exposes many systems, or human physical injury, some distruction of systems would occur.
5. **Very high:** The vulnerability is easily exploitable and found in most systems, or some loss of life and major destruction of systems would occur.
6. **Extreme:** The vulnerability is trivially exploitable and commonly found, or major loss of life and destruction of systems would occur.

5.2.3 Asset value

There are mainly two categories of assets: information assets (like employee data, financial data, intellectual property...) and physical assets (like buildings, raw materials, products, employees...). The value of an asset can be one of the following

1. **Negligible:** The asset has insignificant important for the enterprise. It is easily replaced or repaired. It has little to no security requirements and represents no health impact.
2. **Low:** This asset is of minor financial value. Compromise of it results in little business impact.
3. **Medium:** The asset is of moderate value. It has some security needs and financial value. Compromise of it would impede the enterprise's mission.
4. **High:** The asset is highly value because of its security requirements or customer focus. Its loss would result in considerable harm to customer services and reputation.
5. **Very high:** The asset represents or supports a critical business function for the enterprise. Loss or damage of it results in severe financial, security or health repercussions.
6. **Extreme:** The enterprise places the highest possible value on this asset. Its compromise results in human deaths, immediate and total loss of business services or financial bankruptcy.

5.3 Risk function evaluation

For the risk evaluation, first an asset valuation table is created and a thread-vulnerability table is created for each asset.

Threat action	Frequency	Vulnerability	Severenity
Threat 1	F1	Vulnerability 1	S1
		Vulnerability 2	S2
Threat 2	F2	Vulnerability 3	S3

Figure 5.2: Example of a threat vulnerability table

Then a risk equation is used to calculate the risk posed for each asset:

Risk (A) = SUM[Threat*Vulnerability](A) * Asset Value (A)

After this the assets and their corresponding risk values are put into a table in decreasing order of risk (see figure 5.3).

The total range of the risk values is divided into 6 equal parts and the numerical values are mapped to a 6 qualitative degrees as shown in the figure figure 5.4.

The final result is a table showing the assets and their corresponding risk in a qualitative way (see figure 5.5).

Asset	Risk value
Asset 1	V1 (MaxValue)
Asset 2	V2
Asset 3	V3
Asset 4	V4
Asset 5	V5
Asset 6	V6
Asset 7	V7
Asset 8	V8
Asset 9	V9

(where V1 > V2 > V3 >V4 >V5 >V6 >V7 >V8 >V9)

Figure 5.3: Assets and associated risk values

Rating	Range
Extreme	5/6 * MaxValue to MaxValue
Very High	4/6 * MaxValue to 5/6 * MaxValue
High	3/6 * MaxValue to 4/6 * MaxValue
Medium	2/6 * MaxValue to 3/6 * MaxValue
Low	1/6 * MaxValue to 2/6 * MaxValue
Negligible	0 to 1/6 * MaxValue

Figure 5.4: Mapping form risk ranges to qualitative degrees

Asset	Risk
Asset 1	Extreme
Asset 2	Very high
Asset 3	Very high
Asset 4	High
Asset 5	Medium
Asset 6	Medium
Asset 7	Low
Asset 8	Low
Asset 9	Negligible

Figure 5.5: Final result: Assets and associated qualitative risk

Part II

Comparison of the different risk functions

Chapter 6

NIST and MEHARI

6.1 Comparison

6.1.1 Inputs

The inputs are very similar. Both methodologies are based on impact and likelihood. MEHARI exclusively uses qualitative values, while in NIST it is possible to use quantitative and qualitative values.

There are normally 3 (up to maximally 5) in levels in NIST while in MEHARI there are exactly 4.

6.1.2 Calculation

In the two cases there is a table mapping the inputs to the outputs.

6.1.3 Output

The risk is determined per threat in NIST and in MEHARI. It is a qualitative output. In NIST there are normally 3 (up to maximally 5) levels while in MEHARI there are exactly 4.

6.2 Conclusion

In MEHARI, there are exactly 4 possible qualitative inputs for impact and likelihood, and there are exactly 4 qualitative outputs. In NIST, there are 3 to 5 possible qualitative or quantitative inputs for impact and likelihood, and there are 3 to 5 qualitative outputs.

The MEHARI risk function could be seen as a special case of the NIST risk function, where there are exactly 4 levels and no quantitative values.

Chapter 7

NIST and OCTAVE Allegro

7.1 Comparison

7.1.1 Inputs

In NIST and in Octave Allegro, Impact and probability of occurrence of a threat are considered. Additionally in Octave Allegro, a list with different impact areas is considered.

7.1.2 Calculation

Both risk functions have form of a table mapping inputs to output. But in OCTAVE Allegro, Impact value is not used directly, but is used to calculate a value is called Risk score first. This is the result of evaluation of the impact of a risk occurrence on different impact areas.

7.1.3 Output

Output is qualitative in both approaches. In OCTAVE Allegro there are 4 levels (pools), while in NIST there are 3 to 5 degrees.

7.2 Conclusion

Both methodologies calculate a risk associated with existing threats. While in NIST the impact is directly used for the calculation of the risk, in Octave Allegro the impact of a risk is considered in association with impact areas. The NIST output is qualitative with 3 to 5 level scale, while in Octave Allegro it is qualitative with a 4 level scale.

Chapter 8

NIST and Security pattern

8.1 Comparison

8.1.1 Inputs

The inputs are different. In NIST, it is Impact and Likelihood, while in Security pattern the inputs are: a threats vulnerability table and asset values.

8.1.2 Calculation

The calculation is also very different. NIST uses a table to calculate the risk from impact and likelihood. Security pattern calculates the combined risk value for one asset and then maps these values to a qualitative scale.

8.1.3 Output

NIST determines the risks per threat. The risks values are independent values

Security pattern determines the risk per asset. The risk is expressed qualitatively and is relative to the other risks of the other assets.

8.2 Conclusion

NIST and Security pattern are fundamentally different approaches, with a completely different focus. While NIST shows the risks associated with existing threats, Security pattern shows existing risks for the different assets. The results of Security pattern are relative, while the results for NIST are absolute.

Part III

A common core and a proposal for a new abstract model

Chapter 9

Identification of a common core

9.1 Introduction

In this chapter we want to find a common core in the risk functions to all of the previous approaches. Is there any similarity between all of them?

9.1.1 Different families of risk functions

Not all the risk functions are similar, in fact we can identify two different families. First, we have functions that calculate the risks of the different threats, and second we have functions that calculate the risks for the different assets. This is illustrated in the following figure.

Figure 9.1: Different families of risk functions

We cannot find a common core for all of the approaches. Security pattern calculates the risk for assets and is thereby significantly different from the others. NIST, MEHARI and Octave Allegro calculate the risks of threats and they have common properties. So it is better to leave out Security pattern and to find the common core of the remaining three approaches.

9.2 Common core of NIST, MEHARI and Octave Allegro risk functions

These risk functions all calculate the risk par threat and present common parts which are described in detail below.

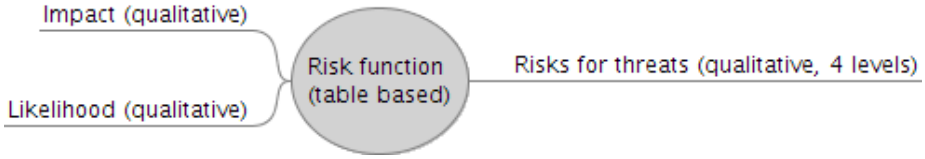

Figure 9.2: Common core of risk functions

9.2.1 Inputs

They are all mainly based on impact and likelihood of threats. All offer the possibility to use qualitative values.

9.2.2 Calculation

In each of the approaches, a table is used to map impact and likelihood values to risk values.

9.2.3 Outputs

The outputs of all approaches are qualitative, and they all offer the possibility to use a precision of 4 levels to express the final degree of risk.

Chapter 10

New abstract model integrating all methods (NAMIAM)

We have developed an abstract model which integrates all four methodologies. It is based on input similar to the input of Octave Allegro. In our model it is possible to calculate both risk per threat and risk per asset. The result can be obtained in both relative and absolute values, which can be later used for prioritization of security needs as well as for evaluation of overall system security.

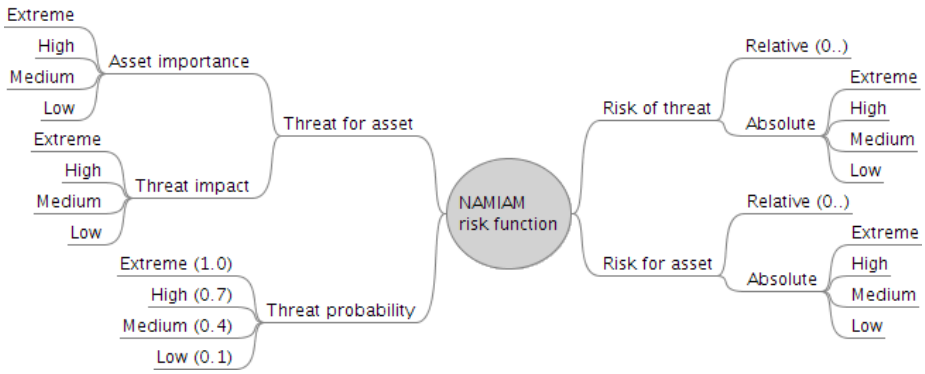

Figure 10.1: NAMIAM risk function overview

10.1 Inputs

10.1.1 Assets

At first, important assets in the organization are identified and their importance is evaluated on a four degree qualitative scale. The qualitative value is then represented as a number:

Degree	Asset importance value
Extreme	4
High	3
Medium	2
Low	1

Figure 10.2: Degree - asset importance

Asset name	Asset importance
Collection	4
Employee data	3
Staff	3
Financial data	2
Building	2
Vehicles	1

Figure 10.3: Example of asset table

10.1.2 Threats

In the second step the threats are identified. The probability of the threat is evaluated on a continuous scale from 0.1 to 1.0. If the exact value cannot be evaluated, the threat probability is assigned a number according to its qualitative representation:

Degree	Threat probability
Extreme	1.0
High	0.7
Medium	0.4
Low	0.1

Figure 10.4: Degree - Threat probability

Then the impact of the threat on each asset is analyzed and represented by a qualitative degree and its corresponding numeric value:

Degree	Threat impact value
Extreme	4
High	3
Medium	2
Low	1

Figure 10.5: Degree - Threat impact value

Threat name	Threat probability	Asset name	Threat impact
Fire	0.7	Collection	4
		Employee data	1
		Building	3
Flood	0.1	Collection	3
		Building	2

Figure 10.6: Example of risk table

10.2 Risk of threat calculation

In order to calculate the total risk of one threat we have to consider all assets affected by execution of the threat. For each asset the impact score is calculated by multiplying asset importance with impact of the threat.

If we summarize the impact scores and multiply the result with the probability of the threat, we obtain a Relative threat risk value. It can be used to find threats with higher and lower importance in mitigation.

If we choose the maximum impact score and multiply it with the threat probability, we obtain an Absolute threat risk value. It is a real number in the interval $<0; 16>$. It can also be represented in qualitative way using following table:

Absolute threat risk	
(12; 16>	Extreme
(8; 12>	High
(4; 8>	Medium
(0; 4>	Low

Figure 10.7: Absolute threat risk

Threat name	Threat probability	Asset name	Asset importance	Threat impact	Impact score (Asset importance * Threat impact)
Fire	0,7	Collection	4	4	16
		Employee data	3	1	3
		Building	2	3	6
		SUM (Impact score)			25
		Relative threat risk (SUM (Impact score) * Threat probability			**17,5**
		MAX (Impact score)			16
		Absolute threat risk (MAX (Impact score) * Threat probability			**11,2**

Threat name	Threat probability	Asset name	Asset importance	Threat impact	Impact score
Flood	0,1	Collection	4	3	12
		Building	2	2	2
		SUM (Impact score)			14
		Relative threat risk (SUM (Impact score) * Threat probability			**1,4**
		MAX (Impact score)			12
		Absolute threat risk (MAX (Impact score) * Threat probability			**1,2**

Figure 10.8: Example of a Threat risk calculation table

In this example we calculated that risk of fire is relatively higher than risk of flood. In absolute measure risk of fire is high and risk of flood is low.

10.3 Risk per asset calculation

In order to calculate a total risk for one asset we have to consider all threats that can affect this asset. For each threat the threat score is calculated by multiplying threat impact with threat probability.

If we summarize the threat scores and multiply the result with the importance of the asset, we obtain a Relative asset risk value. It can be used to find assets with higher and lower protection needs.

If we choose the maximum threat score and multiply it with the importance of the asset, we obtain an Absolute asset risk value. It is a real number in the interval $<0; 16>$. It can also be represented in qualitative way using the following table:

Absolute asset risk	
(12; 16>	Extreme
(8; 12>	High
(4; 8>	Medium
(0; 4>	Low

Figure 10.9: Absolute asset risk

Asset name	Asset importance	Threat name	Threat impact	Threat probability	Threat score (Threat impact * Threat probability)
Collection	4	Fire	4	0,7	2,8
		Flood	3	0,1	0,3
		SUM (Threat score)			3,1
		Relative asset risk (SUM (Threat score) * Asset importance)			**12,4**
		MAX (Threat score)			2,8
		Absolute asset risk (MAX (Threat score) * Asset importance)			**11,2**

Asset name	Asset importance	Threat name	Threat impact	Threat probability	Threat score
Building	2	Fire	3	0,7	2,1
		Flood	2	0,1	0,2
		SUM (Threat score)			2,3
		Relative asset risk (SUM (Threat score) * Asset importance)			**4,6**
		MAX (Threat score)			2,1
		Absolute asset risk (MAX (Threat score) * Asset importance)			**4,2**

Figure 10.10: Example of an Asset risk calculation table

In this example we calculated that risk for collection is relatively higher than risk for building. In absolute measure risk for collection is high and risk for building is medium.

10.4 Output

Using described methodology it is possible to obtain four different inputs:

Relative risk of threat : It is a table of threats ordered by their relative risk score. The threats with high score should be given high priority in mitigation.

Absolute risk of threat : In this table each threat is assigned an absolute qualitative value. It can be used to determine if there are some critical threats for the security of the system.

Relative risk for asset : Assets are ordered by their relative risk score. The assets with high score should be given high priority in securisation of the system.

Absolute risk for asset : Each asset is assigned an absolute qualitative value, which can be used for determination of protection needs of assets.

Threat	Relative risk	Absolute risk
Fire	17,5	High
Flood	1,4	Low

Asset	Relative risk	Absolute risk
Collection	12,4	High
Building	4,6	Medium

Figure 10.11: Example of output tables

Chapter 11

Conclusion

We have studied the risk functions of four models. Most of the approaches are qualitative. There are two families of risk functions. NIST, MEHARI and Octave Allegro are calculating the risk of threats while Security Pattern calculates the risk for assets.

There are different degrees of classification. NIST goes from 3 to 5 level, MEHARI and Octave Allegro have 4 levels, and Security Pattern has 6.

We have identified a common core between NIST, MEHARI and Octave Allegro, which reveals the similarities between these risk functions.

Eventually we propose a new abstract model for all methods (NAMIAM), which allows to calculate both: risk per threat and risk per asset, using qualitative and quantitative inputs. This can later be used for prioritization of security needs as well as for evaluation of overall system security.

List of Figures

Bibliography

[1] Jean-Claude Asselborn. Management of information systems security, 2007 - 2008. The course material of MICS - 3rd Semester.

[2] CLUSIF. MEHARI* V3: Risk Analysis Guide. October 2004.

[3] Alice Goguen Gray Stonebumer and Alexis Feringa. NIST : Risk Management Guide for Information Technology System. Special Publication 800-30. National Institute Of Standards and Technology, 2002.

[4] Duane Hybertson Frank Buschmann Markus Schumacher, Eduardo Fernandez-Buglioni and Peter Sommerlad. Security Patterns: Integrating Security and Systems Engineering. Software Design Patterns. WILEY, 2005.

[5] Lisa R. Young Richard A. Caralli, James F. Stevens and William R. Wilson. Introducing OCTAVE Allegro : Improvement the Information Security Risk Assesment Process. Carnegie Mellon University, May 2007. Technical Report CMU/SEI-2007-TR-012, ESC-TR-2007-012.