The SOMAP.org
Open Information Security Risk Assessment Guide

Version 1.0

1 Table of Content

Table of Contents

2 Introduction

2.1 Informations about this document

The SOMAP.org Open Information Security Risk Assessment Guide (Guide) contains detailed information about security risk management. It discusses the management processes and explains formulas and how to use them. This Guide is an extension to the SOMAP.org Open Information Security Risk Management Handbook (Handbook) and describes the details of the Risk Assessment Workflow as introduced in the Handbook.

The Security Officers Best Friend (SOBF) tool is the reference implementation of this Guide. The SOBF tool is written in Java and should run on most platforms.

In the current version, the Guide describes two risk analysis methodologies. These are the qualitative and the quantitative methods. There are other methods and this Guide and the SOBF tool are both not restricted to only the current two methodologies. The SOMAP.org project is interested to learn more about other methodologies which could be explained in a later version of the Guide and implemented with the SOBF tool.

The Guide, the Handbook and the SOBF tool are projects developed by the Security Officers Management and Analysis Project (SOMAP.org). SOMAP.org is a swiss non-profit organisation with the main goal to run an open information security risk management project and to maintain free and open tools and documentations for security officers and other interested parties.

For further informations concerning SOMAP.org or any of the SOMAP.org projects please visit the projects website at http://www.somap.org/. SOMAP.org is work in progress and any contribution is welcome. If you are interested in helping out, then please contact the SOMAP.org project via email at contact@somap.org.

Please have a look at the license at the end of this Guide for further informations concerning copying and changing parts or the whole of this document.

2.2 Intended audience

The SOMAP.org Handbook contains high level informations and is intended for the upper management as for the security officer to get an overview of the topic. The Handbook contains an introduction to risk management. You can learn about what risk is and what risk management is, why the management of risk is important and what can be done to have a risk management system in place. The Handbook discusses why it is important to follow standards and how this document can help you in doing so.

This Guide contains informations about the risk analysis process, the methods for the analysis and details about calculations and the mechanics of the calculations. It is possible to follow the Guide step-by-step. Either “manually” or using the SOBF Tool. Or you can only pick the parts which are relevant to you.

The SOBF tool has the feature to create Reports based on the calculations and formulas which are described in this Guide. The possible Reports and their description and explanation will be covered by the Reports subproject. Please see the SOMAP.org website for details.

2.3 Preface

Nowadays the environment is changing quickly, so are the requirements, the threat profiles, the regulations and other risk influencing factors. These changes can have a direct impact on the gained profit, the health of the company as on the employees and how the company is looked at from the outside. To act on these changes it is inevitable to manage security and to be able to show (proof) how and what is managed and done.

The proof of security management is not only needed for a potential certification but also to show your customers your companies efforts (gained trust), to show the stakeholders the companies worth and any legislation that the company is following the legal obligations.

Understanding the company, guarding the assets and showing everybody that the company is strong. That is what Risk Management is all about.

2.4 Feedback

If you are having comments or suggestions in how to make this Guide better or what should be added or changed, then please drop us a note and tell us about your ideas. You can reach the SOMAP.org project via email at contact@somap.org.

2.5 Versions

The newest version of this guide can always be found at the project website at http://www.somap.org/

Version	Information
June, 2006	Initial release.
September, 2006	Some updates to be more standards compliant.
1.0	February, 2007. Release of first official version.

3 Terms, Definitions and Relations

3.1 Overview

This Guide tries to be as compliant with the definitions from the ISO 7498-2 and ISO 27001/27005 standards as possible.

3.2 Elements

Elements are objects (physical items, virtual things) which are in a relationship with each other. An asset is an element, a threat is an element. A threat and and asset have a relationship and form one or multiple vulnerabilities.

Every element can have one or more factors.

3.3 Factors

There is an old saying which goes like this: “What can't be measured can't be managed”. Factors are there to allow to measure and to help decide on the management part.

A factor is a numerical information of an element. The likelihood that a vulnerability is exploited is a factor of a vulnerability.

Factors can either be an integer ranging from 0 up to some maximum value or it can be a floating point value ranging from 0 to 1 (where 1 is the equivalent of 100% and 0 means 0%).

Factors are (mostly) specific to a risk analysis methodology and therefore they are described within the respective methodologies chapter.

Calculations and Formulas

This version of the Guide uses the classic risk calculation formula. Some of these are enhanced to better suite the needs of the SOBF tool or the general work flow analysis

It is planned to evaluate the implementation of the Common Vulnerability Scoring System [CVSS] for the algorithms and formulas in a later version of this Guide and the SOBF tool.

3.4 Methodologies

The current version of the SOMAP.org Guide describes two methodologies to analyse risk: The qualitative methodology and the quantitative methodology. Depending on the goals which should be achieved when doing the Risk Assessment the one method is better suited than the other. So the decision which method to use should be evaluated in front of the Risk Assessment. Please see the Handbook for further details concerning these two methodologies.

3.5 Common Elements

A common element consists of data which can be shared with other security officers. The SOMAP.org project runs a sub-project maintaining and enhancing a set of common elements. That sub-project is called Repository and is a community effort to create and maintain an open source information security repository.

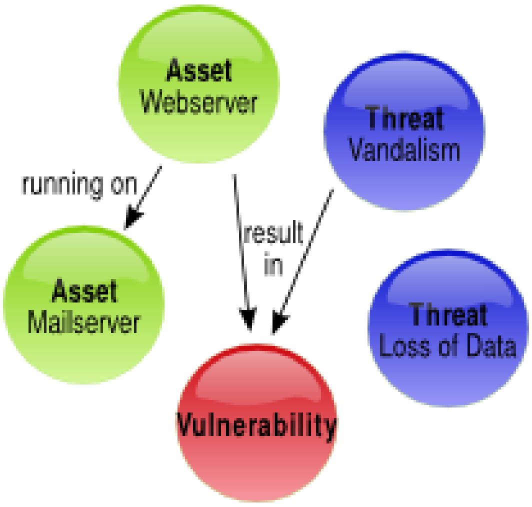
Asset
Webserver
Threat
Vandalism
Asset
Mailserver
Threat
Loss of Data
Vulnerability

Common element means, that this is an element which is defined within the Repository and which is used exactly the same by everybody. As an example, every Inventory Item is referring an Asset from the Repository. All factors from the Asset are inherited to the Inventory Item. The Asset works as a template for the creation of the Inventory Item and the Assets factors are only meant as a guide and therefore can be overwritten on the personalised element.

Other common elements are used for classification and grouping of personalised elements.

3.6 Relationship

All the common elements within the Repository are put into a relation with each other. These relations or links describe relationships between the common elements.

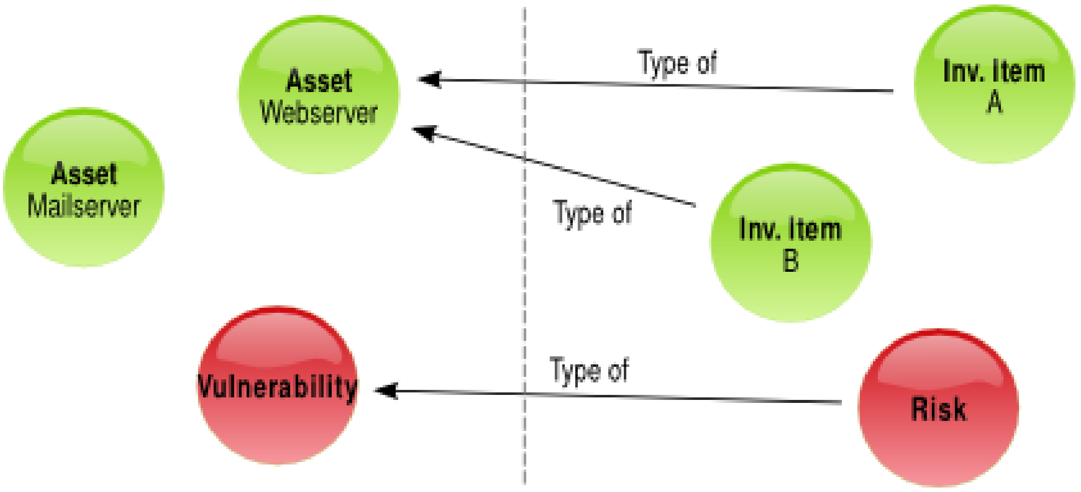


With such links it is possible to model relationships between multiple Assets and it becomes possible to build some kind of tree or network made out of Assets. A structure like that offers the possibility and flexibility to inherit informations from one Asset to the next. An Asset "file cabinet" with a very high protection level can therefor inform the Asset "CEO office" that it should have the same high protection level because the file cabinet is located in the CEO office. See the chapter on inheritance for further details.

3.7 Personalised Elements

Personalised means that this is an element which is different from environment to environment. The personalised elements are user and environment specific and these elements are normally not shared with others. One of the main reasons for not sharing is that this data is most probably highly confidential.

Some of the personalised elements are in a "type-of" relationship with a common element. This relationship gives detailed information about a personalised element.

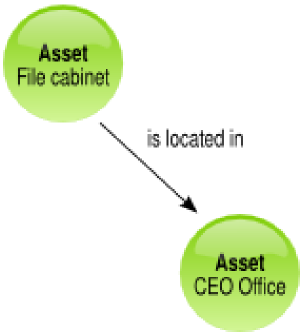


Values of personalised elements are used to fine tune calculations to a concrete environment. While the common value for the likelihood of a vulnerability gives some guidance of what to expect, this value will not be valid for everybody. This is where the concept of personalised values is used so everybody can fine tune predefined common values.

3.8 Future plans

3.8.1 Inheritance

The diagram below shows an inheritance between two assets. When modelling relationships between elements – using the topic map technology – it is possible to analyse inherited risk automatically.



It is also possible to have one asset influence the other asset. Like that one asset can influence the level of protection needed of another asset.

3.8.2 Checklists

Checklists are lists which are owned by a Custodian or Owner of an Inventory Item and which contains tasks which need to be done. Such a task most probably consists of implementing or maintaining a Safeguard or Control measure.

3.8.3 Questionnaires

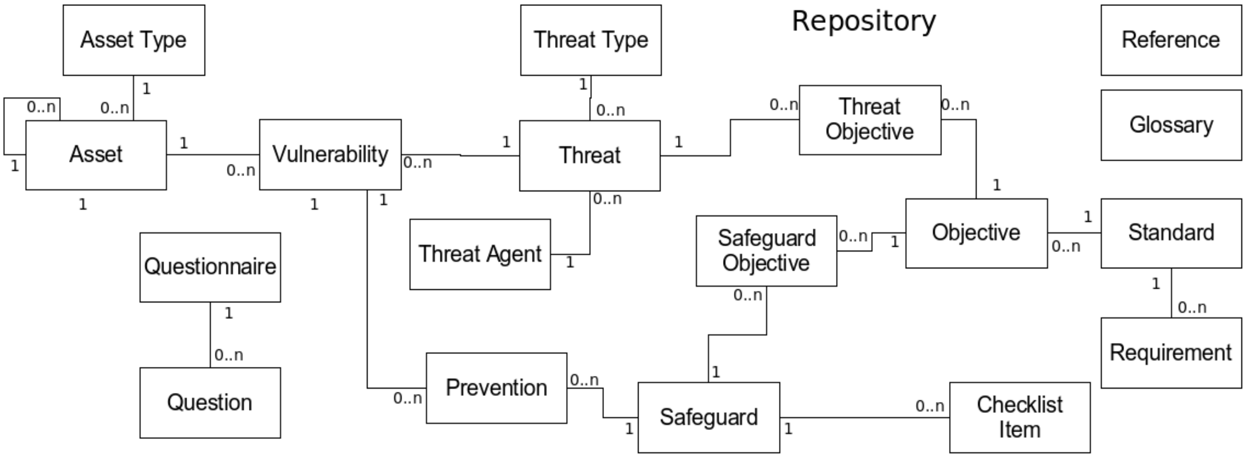
A Questionnaire is a convenient method to find out about an environment. Having Questionnaires is planned for the SOBF tool to allow for a convenient method to start with an environment. A finished Questionnaire could automatically create an environment with Inventory Items based on the informations from the Questionnaire.

4 Risk Assessment Elements

4.1 Common Elements

The Guide diverges from some of the element definitions and naming of different standards. This is mostly because the Guide is based on a data model for easy calculation of risk.

The following illustration shows the common elements and how they are linked with each other.



4.1.1 Asset

An Asset is something that has a value or utility for an organisation. An Asset is used for business operations and it's continuity and availability are important for the organisation. An asset within this Guide is a description of a theoretical Object/Subject which could be required to protect. See the description of Inventory Item for details on how an Asset is linked with an Inventory item.

Assets can be linked with each other to build a hierarchical tree.

4.1.2 Asset Type

The Asset Type is used to croup Assets into logical groups of similar Assets.

4.1.3 Threat

ISO 7498-2 describes a threat as “a potential violation of security”. The SOMAP Methodology knows a Threat as a description of a theoretical violation of security. That violation can either come from a person, a thing, it can be an event or an idea which poses a danger to an asset.

Every Threat can potentially be conducted by a Threat Agent.

Attack

If a Threat becomes reality and is occurring the Threat is then known as an Attack. An Attack can then either be successful or unsuccessful, mostly depending on the installed controls.

4.1.4 Threat Type

Threat Classification and Grouping

Threats can be classified (accidental, intentional) and sorted (active, passive) according the following groups.

Accidental

This threat was not planned by a threat agent and happens as an accident. Such threats can be system malfunctions or nature disasters.

Intentional

An intentional threat was planned by a threat agent.

Active

An active threat – if becoming a successful attack – will change data.

Passive

A passive threat – if becoming a successful attack – will never change data.

4.1.5 Threat Agent

The Threat Agent is used as a category or classification of Threats and represents an element which could exploit one or multiple threats for an Attack. A Threat Agent does not have to be a human being but can also be a natural force or something else.

Threat Agent Motives (COMIC)

A Threat Agent can have a motivation out of the following list:

- Commercially
  The Threat Agent is motivated in commercial gains. To gain an advantage market position over the competition as an example.
- Opportunistic
  The Threat Agent uses his chance. Changes makes thieves, as an old saying goes.
- Monetary
  The Threat Agent is motivated by financial gains or other money motivated reasons.
- Idealistic
  The Threat Agent is fighting for a/his cause. This is mostly politically motivated.
- Can do
  The Threat Agent is attacking a system because he can do so. There is no special gain for him.

Threat Agent Motivation Rating

This is a rating describing the motivation level of the different Threat Agents. While some Threat Agents will try to get at the low hanging fruits only, others will have more patience.

4.1.6 Vulnerability

A Vulnerability is a description of a flaw or a weakness in or on an Asset. (A Threat and an Asset are linked together to describe a Vulnerability.) A Vulnerability can also be a weakness in a Safeguard or an absence of a Safeguard.

4.1.7 Objective

Objectives describe the goals of a Standard. What should/could be achieved. Objectives are grouped by Standards and the SOBF tool typically only contains Objectives of chosen Standards.

4.1.8 Standard

A Standard is what it says it is: A Standard like ISO 17799 or ISO 27001. A Standard can be used to filter Objectives and other elements based on an environments requirements. If an environment should be assessed against as example ISO 17799, then this specific Standard should be integrated in the SOBF tool.

4.1.9 Requirement

Requirements are part of a Standard. Requirements describe a must of a Standard.

4.1.10 Safeguard

A Safeguard is a possible (and theoretical) protection mechanism which protects an Asset from one or multiple Vulnerabilities.

Implementation

When implemented, a Safeguard becomes a Control.

4.1.11 Checklist and Checklist Items

A Checklist consists of questions in the form of Checklist Items. These questions are answered with the goal to find out which Safeguards already are implemented in the form of Controls and which ones are in planning. A Checklist can be a convenient method to manage Controls and their respective status.

Checklists will be described in a later version of the Guide.

4.1.12 Questionnaire and Questionnaire Items

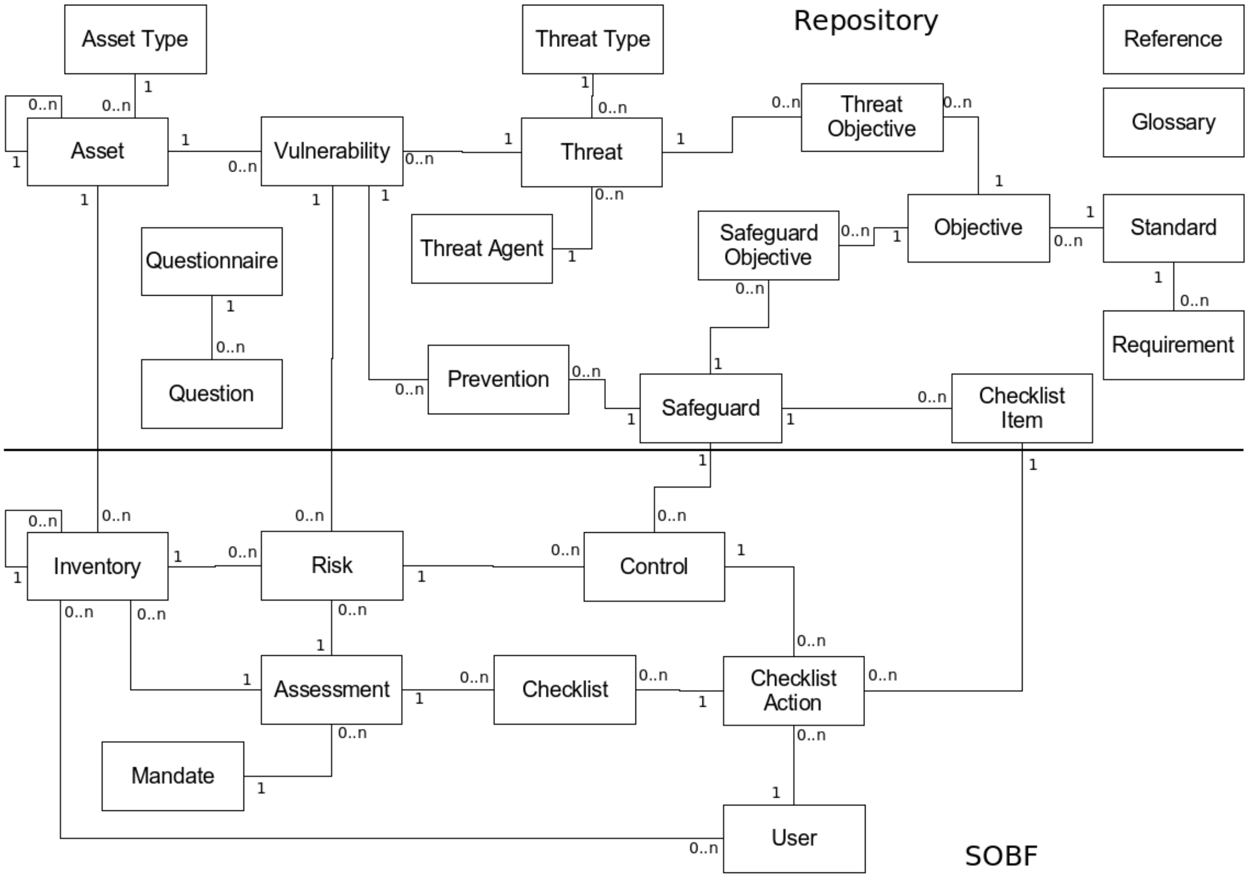
A Questionnaire is also list of questions but with an other intention than the Checklist. Filling out a Questionnaire will result in a list of active Assets (Assets which are within an environment), possible Threats and implemented Controls. A Questionnaire can be a quick start to begin a risk analysis.

Questionnaires will be described in a later version of the Guide.

4.2 Personalised Elements

4.2.1 Overview

The illustration below shows the personalised elements and how they are linked to the common elements.



4.2.2 Assessment

An Assessment keeps all the info of an Assessment together. The Assessment consists of one turn of the risk analysis workflow. Findings from earlier assessments can be used in later assessments as a basis.

4.2.3 Inventory Item

An Inventory Item is an instance of an Asset. Which means it is a physical representation of an Asset in real life. Every Inventory Item is linked to an Asset. The Asset describes the type of an Inventory Item. If a file cabinet is an Asset then the file cabinet in the CEOs office is an Inventory Item. If cabling is an Asset then the cabling through your underground parking is an Inventory Item.

Level of Detail

It is the security officers decision to decide on the level of detail needed during the risk analysis. While it can be OK in some scenarios to group Inventory Items to logical groups and then analyse those groups only, other scenarios can require to have every Inventory Item analysed on its own.

The level of detail will influence the size and detail of the resulting analysis of risk. It could be a good strategy to first start small and refine the level of detail in further iterations of the risk assessment workflow.

4.2.4 Owner and Custodian (User)

Every inventory item needs an owner or custodian as described in the Handbook. An owner is an individual or element with approved management responsibilities for controlling the production, development, maintenance, use and security of an inventory item.

The Custodian of an Inventory Item is used as the default user for Checklist Items. This means that the Custodian of an Inventory Item has the responsibility to implement mitigation strategies on his own Inventory Items (at least per default. This can be changed by the security officer).

4.2.5 Environment

The Environment consists of all the Inventory Items of a user. It is the base of all to be protected Inventory Items.

4.2.6 Control

A Control is an instance of a Safeguard which means that this Control is an installation or planned installation of a Safeguard. The Control is linked with a Risk and influences the probability and the damage a Risk can cause.

Even when there is a Control in place, an Attack can still occur and can still be successful. Although the Attack has then perhaps a reduced efficiency.

When multiple Controls are used to guard from a Vulnerability, the effectiveness of this protection is calculated with the Control Effectiveness formula described in the respective methodology.

Installed Controls can also introduced new Vulnerabilities to an Inventory Item.

4.2.7 Risk

The Risk is what the Risk Analysis is all about. The Risk results from an Inventory Item, the threats against that item, the implemented Controls and some formula mixing this all together. The Risk Values of all Inventory Items in an Environment are evaluated and result in a top ten report of the ten highest risks of an environment.

It is the objective of the risk management to reduce risk to an acceptable level. Do so with one of the methods described in the handbook.

When done multiple times, the Risk Analysis produces a history of the risks which can be used to follow the costs and efficiency of the implemented Controls.

4.2.8 Checklist

Checklists will be described in a later version of the Guide.

4.2.9 Checklist Action

Checklist Actions will be described in a later version of the Guide.

4.3 Information Propagation

When creating a personalised element this element can have a direct connection with one or multiple common element. A common element then acts as the template for the newly created element. This has the effect that a personalised element inherits some of the common elements information like the effectiveness of a safeguard and information like that.

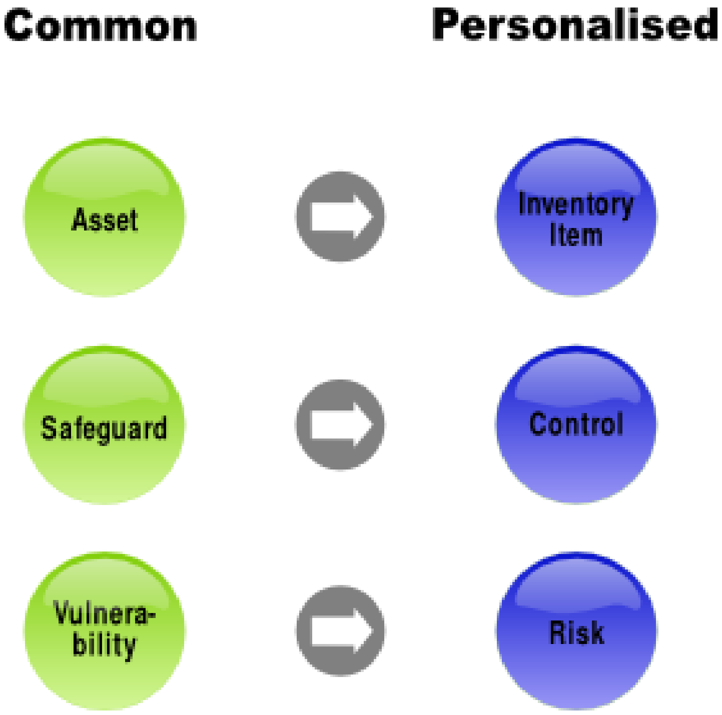
This section contains all the information concerning which element can inherit what value and how this inheritance works.

4.3.1 Propagation Procedure

Generally all factors are copied as long as they are not overwritten with personalised values.

4.3.2 Propagating Parties

These are the elements which currently propagate their factors:

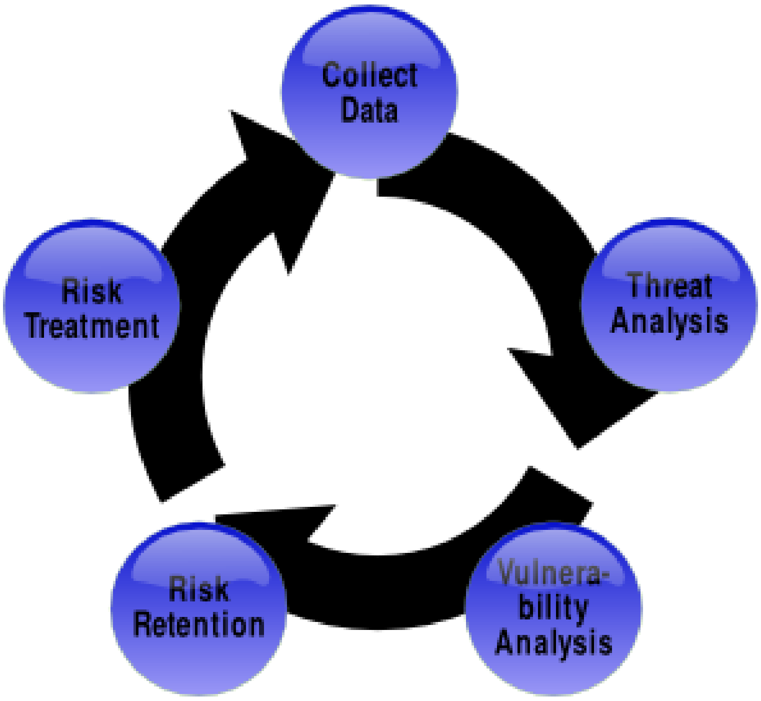


5 The Risk Assessment Workflow

5.1 The Workflow

The upcoming ISO 27005 standard is talking about a risk assessment process. The Guide does not use the same naming for two reasons. First, the Guides Workflow consist of more steps than the risk assessment process. And second, the word “workflow” describes the idea of a recurring flow of activities much better.

The Risk Assessment Workflow helps in completing a structured risk assessment and analysis. The Workflow leads the security officer through 5 phases. Every such phase consists of multiple activities which sometimes can be done in parallel, sometimes need to be done sequentially. The activities are small pieces of work which can either be done by the security officer or which can be delegated. Depending on the activity in question, multiple persons need to give their input in order to finish an activity.



One turn of the Risk Assessment Workflow corresponds one assessment within the SOBF tool. The phases “Collect Data”, “Threat Analysis” and “Vulnerability Analysis” are also known as the super phase “Context establishment”.

SOMAP.org runs a Reports sub-project which designs and maintains a set of reports based on this Risk Assessment Workflow. Please see the Reports project for a detailed description of every report. Please see the Handbook for further details about when to do this Workflow in the overall security management process.

5.2 Collect Data

At the beginning of a Risk Assessment Workflow, the security officers starts a new assessment. If there was already an assessment, it is possible to use the old assessment as a template for the new assessment. Inventory items – as example – can be imported from the old assessment into the new assessment. Like that it is possible to create an analysis based on the current protection status and achievements from earlier assessments.

5.2.1 Inventory

The Inventory is everything. The Inventory contains all the information of an environment. With the Inventory it is possible to decide which Inventory Items should be protected and which are not that important to a company.

There are two possible ways to collect data about an inventory. One way is to fill out a questionnaire. The SOBF tool will then create an inventory based on the informations from the questionnaire. Another way is to import or model an inventory based on concrete data. It does not matter which way is chosen, the idea of the inventory is always the same: The inventory is used to understand an environment and its needs.

Which way is best to build an inventory depends mostly on the requirements, the available resources, the required result and what the security officer likes best.

Rapid Risk Assessment (Questionnaire)

A questionnaire is normally used when details in the inventory are not required. The result of a questionnaire are groups of assets which can then be used to analyse the situation on a higher level. In such a scenario the Inventory will not contain every single web server in use but contain a single inventory item “web server” which represents all the different web servers in use. It is easier and quicker to analyse such a high level Inventory than a detailed Inventory.

Build and Import Inventory

When there is already a management system containing an existing inventory (or when building a detailed inventory) this results in a very detailed risk analysis where every single inventory item is analysed.

When building an inventory, the security officer is free to model the inventory in whatever detail it is needed.

5.2.2 Inventory Item Valuation (Classification)

Every Inventory Item needs to be classified. This activity helps in deciding which Inventory Items are more important to a company than others. The inventory items owner has to decide how important the inventory item is and whats the cost of that inventory item.

5.2.3 Inventory Report

At the end of this phase, the security officer creates a report showing the inventory and which items/assets are the most important and costly in an environment.

5.3 Threat Analysis

In this step the security officer defines (or activates) threats which are relevant within the environment which is currently analysed. This step is a very important step for the security officer has to analyse the situation and decide on the right threats.

Result of this phase is a threat analysis report which shows which threats are active and who the threat agents are.

5.4 Vulnerability Analysis

Based on the result from the threat analysis, the security officer gets a list of possible vulnerabilities. In this phase the security officer does the same with the possible vulnerabilities as with the threats during the threat analysis: he decides on which vulnerabilities are relevant and which are not. He takes the list of vulnerabilities and actives the relevant ones.

The result from this phase is a vulnerability analysis report which is basically a list of activated vulnerabilities. These vulnerabilities are used directly to generate possible risk values.

5.5 Risk Retention

There are several activities within this phase. The most important activity is to define which risks are the biggest, to decide what to do about those risks and then to accept the residual risk.

5.5.1 Risk identification

The first activity is to update the information on implemented or planned Controls, based on the vulnerability analysis report from the previous phase. Controls are there to protect from Risks and it is very important to learn about already installed or planned Controls since these influence the risk calculation process.

5.5.2 Risk estimation

The second activity consists of linking all information together and in producing a risk analysis report. The report contains mostly the calculations described within the Risk Analysis calculation chapter.

5.5.3 Risk evaluation

The next activity is about deciding what to do about the known risks. Depending on the strategy, the security officer can decide on implementing further Countermeasures and Controls. Therefore this activity and the second activity will be mostly executed in iterative steps until everybody is happy with the situation.

5.5.4 Risk financing

The second last activity in the risk acceptance phase is to produce the final risk assessment report. The idea of this report is to have a paper containing all the relevant information concerning the inventory, the threat, the risk of an environment and which Controls either already are implemented or are planned to be installed.

The last activity in this phase will be the security officer showing the risk assessment report to the upper management and have this paper signed by somebody of the upper management. Like that the security officer not only has a mandate to do whats written in the risk assessment report but he also has proof of his findings and analysis.

5.6 Risk Treatment

The last phase in the Risk Assessment Workflow is about implementing and supervising the implementation and maintenance of the defined Controls.

5.6.1 Risk communication

One of the possible activities in this phase is to produce a controls report. This report contains a list of defined Controls, their implementation status, owner and other informations. Such a report can be used to communicate risk to decision makers and stakeholders.

5.6.2 Risk monitoring and review

Another activity is to produce checklists for owners and custodians of Inventory Items. These checklists are used to manage the implementation and maintenance of the Controls. Based on this data the security officer has complete control over the status of the environment.

6 Qualitative Risk Analysis

6.1 Risk Calculation Factors

While both - common elements as well as personalised elements - can have factors, the risk analysis process only makes use of the personalised elements factors. The reason for this is that only the personalised elements factors are correct for the environment which is analysed.

The rest of this chapter therefore only contains the personalised elements values.

elements can have qualitative values. Those values are a part of the formulas of the qualitative risk analysis. This chapter contains all the values needed for a qualitative Risk Analysis.

6.1.1 Inventory Item

Asset Value (AV)

The Asset Value describes that assets theoretical value. This value is not meant to be a monetary information but can be understood as how much worth or how important that asset is. To calculate the qualitative asset value one can use a simple calculated using the values of Confidentiality, Integrity and Availability, Auditability and Accountability. While the classical calculation of qualitative asset value (also known as the CIA Triad) does not make use of the informations concerning auditability and accountability this information is quite important and therefore a component of the SOMAP.org risk calculation formula.

Confidentiality (C)

Confidentiality ensures that information is only accessible to the ones with the proper authorisation. The Confidentiality value describes how important it is that this asset or the assets data stays confidential.

Confidentiality Values

Value	Description
0	not applicable
1	not confidential
2	not very confidential
3	confidential
4	very confidential
5	highly confidential

Integrity (I)

Integrity means that the information stays the same and is not changed. Neither actively nor passively. The Integrity value describes how important it is that the Assets integrity is protected.

Integrity Values

Value	Description
0	not applicable
1	very low
2	low
3	medium
4	high
5	very high

Availability (A)

Availability has the meaning that an asset is there at your service and can be by the users. The availability value describes how important it is that this asset is available.

Availability Values

Value	Description
0	not applicable
1	not important
2	not very important
3	important
4	very important
5	extremely important

Accountability (Ac)

Accountability is also known as responsibility and describes the mechanism to identify who did what. The accountability value describes how important it is to be able to have the possibility to find out about who did what with an asset.

Accountability Values

Value	Description
0	not applicable
1	very low
2	low
3	medium
4	high
5	very high

Auditability (Au)

Auditability describes that an asset can have an audit trail containing a complete logging history. Such an audit trail can be used to analyse an incident. The auditability value is used to describe how important it is for an asset to have an audit trail.

Auditability Values

Value	Description
0	not applicable
1	very low
2	low
3	medium
4	important
5	very important

6.1.2 Control

Control Effectiveness (CE)

This factor describes how effective a Control is when it is implemented.

When implementing multiple Controls on one Vulnerability the values are calculated according the Control Effectiveness formula.

It is also very important to know that implemented Controls can open up new Vulnerabilities. It is possible to analyse the influence of a control on another control.

Cost of Control (PC)

Every Control has its price. This factors tells you how costly a control is.

Status of implementation (SI)

This factor describes the status of the implementation of the control.

Value	Description
0	not applicable
1	under investigation
2	installation planned
3	installing
4	installed
5	tested

6.1.3 Risk

Risk Value (R)

The Risk value is the risk which is taken when no (further) Safeguards are applied. This value is calculated from the Likelihood and the Impact.

Likelihood (L)

Likelihood describes how likely it is that a vulnerability will be exploited.

Likelihood Values

Value	Description
0	not applicable
1	very unlikely
2	unlikely
3	possible
4	likely
5	very likely

Impact (I)

The Impact describes how bad the unavailability of the asset as a result of an exploited vulnerability will be

Impact Values

Value	Meaning
0	not applicable
1	very low impact
2	low impact
3	medium impact
4	high impact
5	very high impact

6.2 Risk Calculation Formulas

6.2.1 Qualitative Asset Value (QualAV)

AV = C + I + A
or
AV = C * I * A * Au * Ac

6.2.2 Risk Value (RV)

Likelihood (L)
Impact (I)
RV = L * I * AV
or Risk value for every QualAV value.

7 Quantitative Risk Analysis

7.1 Risk Calculation Factors

An element can have quantitative values. These values are used – exactly like the qualitative values – for calculations in the quantitative risk analysis.

7.1.1 Inventory Item

Asset Value (AV)

This is the monetary value of an Inventory Item.

```
Homepage Server (Web server) = 7'000 CHF
```

Asset Loss Expectancy (ALE)

This is the estimated monetary loss per day if that Inventory Item is damaged stolen or not available anymore.

```
ALE = Loss / Day
```

Recovery Time (RT)

This is the time needed to recover from an incident.

Please see the chapter on crisis management in the SOMAP.org handbook for informations concerning recovery and resumption time.

7.1.2 Control

Control Effectiveness (CE)

This formula results in a factor which defines how effective all the chosen Controls will be.

```
CEn = CEn-1 * (1 - SEn)
CE0 = 1
```

Control Prioritisation

Not all the Controls are equally effective. Some Controls can protect from multiple Vulnerabilities. It is therefor important to formulate a strategy to prioritise Controls to implement the most cost effective solution. A tool can only supply basic decision helps but it can not decide on itself.

Cost of Control (PC)

Every Control has its price.

Status of Implementation (SI)

The status of implementation describes if a Control needs implementation and if so whats the current level of the implementation.

Value	Description
0	not applicable
1	under investigation
2	installation planned
3	installing
4	installed

5	tested

7.1.3 Risk

Annualized Rate of Occurrence (ARO)

This factor describes how many times an incident happens in a year.

Annual Cost of Safeguard (ACS)

This factor describes how expensive a safeguards implementation is in a year. Please note that this is not the cost to buy the safeguard but the concrete cost of possible incidents and everything.

Exposure Factor

Used to classify the type of exposure. It describes how much an incident will destroy of an asset:

Value	Description
0	not applicable
1	intranet
2	extranet
3	internet

7.2 Risk Calculation Formulas

The Quantitative method uses monetary values for assets and calculates estimated monetary loss and uses these values to calculate Risk.

7.2.1 Incidental Damage (ID)

This is the monetary value of a damage if a Vulnerability gets exploited.

```
Asset Value (AV)
Exposure Factor (EF)
ID = AV * EF
```

7.2.2 Timely Damage (TD)

How expensive is a recovery. Every day will be counted.

```
Asset Loss Expectancy (ALE)
Recovery Time (RT)

TD = ALE * RT
```

7.2.3 Single Incident Damage (SID)

This is the damage in monetary terms taken from a single incident.

```
Exposure Factor (EF)
Timely Damage (TD)
SID = EF + TD
```

7.2.4 Single Loss Expectancy (SLE)

This is the damage in monetary terms taken from a single incident when taking the implemented Controls into account.

```
Control Effectiveness (CE)
```

```
SLE = SID * (1 - CEn)
```

7.2.5 Annualized Loss Expectancy (ALE)

This is the estimated monetary damage taken in one year.

```
Annual Rate of Occurrence (ARO)
Single Loss Expectancy (SLE)

ALE = ARO * SLE
```

7.2.6 Cost Benefit Analysis (CBA)

Monetary value describing if the implemented Controls do cost more than they protect or how effective they are in protecting an Asset.

```
Annual Cost of Safeguard (ACS)
Annualized Loss Expectancy (ALE)

CBA = ALE(Without Control) - ALE(With Control) – ACS
```

8 Risk Treatment

Risk Treatment is about the selection and implementation of controls to modify risk. Part of the Risk Treatment is it to define the baseline security requirements. While this is a part of the workflow, the current version of the Guide does not discuss this topic in detail.

Please refer to the Handbook and the ISO 13335 (and the upcoming ISO 27005) standard for further details. At least for now.

9 Reports

9.1 Overview

Reports are not part of this Guide. They are described by the Reports sub-project of SOMAP.org. This chapter only contains a list of Reports which are based on calculations from the risk analysis methodologies as described in this Guide.

Please see the Report sub-project's website for further details.

9.2 Short list of Reports

Trends

The trends report contains historical data and compares these informations with the current situation. This can be used to try to find trends in the threat profile.

Top Ten Risks

This is a report containing the current top ten risks. This is mostly a report which the upper management wants to see.

Operational Risk Management Matrix

This matrix is very useful to visualise the impact and dependence of cost and protection level.

Cost Benefit Analysis

The cost benefit analysis helps in finding out about how much money should be spent on which Control to have the best protection for the best monetary value with the lowest risk.

10 Appendix A: GNU Free Documentation License

Version 1.2, November 2002

10.1 PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

10.2 APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover

Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgments", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

10.3 VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

10.4 COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

10.5 MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and

publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgments" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgments and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one element. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same element you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

10.6 COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgments", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

10.7 COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

10.8 AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

10.9 TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 3. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgments", "Dedications", or "History", the requirement (section 3) to Preserve its Title (section 0) will typically require changing the actual title.

10.10 TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10.11 FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation

11 Bibliography

Where to find further informations (in no specific order):

- [Handbook] The Security Officers Management and Analysis Project (SOMAP.org). *Open Information Security Risk Management Handbook*. Version 1.0, September 2006.
- [HHS2003] United States Department of Health & Human Services. *Information Security Program, Risk Assessment Guide*. October 24, 2003.
- [SRMG2006] Microsoft Solutions for Security and Compliance (2006). *The Security Risk Management Guide*.
- [NIC2002] Arthur Nichols (2002). *A Perspective on Threat in the Risk Analysis Process*.
- [CAN1999] Government of Canada, Communications Security Establishment (1999). *Threat and Risk Assesssment Working Guide*.
- [NWGRFC2828] Network Working Group (May 2000). *Request For Comment 2828, Internet Security Glossary*.
- [NISTRM2002] NIST Special Publication 800-30 (Juli 2002). *Risk Management Guide for Information Technology Systems.*
- [OCTAVE] Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation). http://www.cert.org/octave/
- [WPRISK] Wikipedia article about Risk. http://en.wikipedia.org/wiki/Risk
- [ISO73:2002] ISO/IEC (2002), *Risk management. Vocabulary. Guidelines for use in standards*.
- [ISO13335-1:2004] ISO/IEC (2004), *Information technology – Security techniques – Management of information communication technology security*.
- [ISO27001:2005] ISO/IEC (2005), *Information technology. Security techniques. Information security management systems. Requirements*.
- [ISO27005] Draft: ISO/IEC (2006), *Information technology – Security techniques – Information security risk management*.
- [ISO17799:2005] ISO/IEC (2005), *Information Technology. Security Techniques. Code of Practice for Information Security Management*.
- [GSHB] Bundesamt für Sicherheit in der Informationstechnik (2004). *IT-Grundschutz Manual*.
- [DMS1997] Dorfman, Mark S. (1997). *Introduction to Risk Management and Insurance (6th ed.)*, Prentice Hall. ISBN 0137521065.
- [SRM2003] Stulz, René M. (2003). *Risk Management & Derivatives (1st ed.)*, Mason, Ohio: Thomson South-Western. ISBN 0-538-86101-0.
- [AA2004] Alijoyo, Antonius (2004). *Focused Enterprise Risk Management (1st ed.)*, PT Ray Indonesia, Jakarta. ISBN 979-9891818-1-7.
- [CAES2004] Alexander, Carol and Sheedy, Elizabeth (2004). *The Professional Risk Managers' Handbook: A Comprehensive Guide to Current Theory and Best Practices (1st ed.)*, Wilmington, DE: PRMIA Publications. ISBN 0-9766097-0-3.
- [CVSS] *Common Vulnerability Scoring System*. http://www.first.org/cvss/

12 Alphabetical Index