The SOMAP.org

Open Information Security Risk Management Handbook

Version 1.0, September 2006

1 Table of Content

1 Table of Content....2
2 Introduction....4
2.1 Informations about this document....4
2.2 Intended audience....4
2.3 Preface....4
2.4 Feedback....5
2.5 Versions....5
3 Risk....6
3.1 What is Risk....6
3.2 Sources of Risk....6
3.3 Risk is changing over time....7
3.3.1 Changing habits....7
3.3.2 De-perimeterisation....7
3.3.3 Regulations....7
4 What is Risk Management....8
4.1 Risk Management is a process....8
4.2 Risk Management is daily business....8
4.3 Decision-making....8
4.4 Risk Treatment....8
Risk acceptance / retention....9
Risk mitigation....9
4.5 Residual Risk....9
4.6 Risk Mitigation strategies....9
4.6.1 Introduction....9
4.6.2 Risk transfer....10
4.6.3 Risk reduction / mitigation....10
4.6.4 Risk removal / avoidance....10
4.7 Limitations of Risk Management....10
4.8 Approaches to the Management of Risk....10
4.8.1 Proactive....10
4.8.2 Reactive....11
4.9 Risk Prioritisation....11
4.9.1 Qualitative Method....11
4.9.2 Quantitative Method....11
4.10 Why Risk Management is important....11
4.10.1 Value of Informations and New Challenges....11
Value....11
Theft....12
Unknown Threats....12
5 Information Security Management....13
5.1 Management Components....13
5.1.1 Ownership....13
Owner....13
Custodian....13
5.1.2 Risk analysis....14
5.1.3 Policy....14
5.1.4 Organisation....14
5.1.5 Guidelines....14
5.1.6 Due care....14
5.1.7 Procedures....14
5.1.8 Support....14
5.2 Keys to success....14
5.3 Internal Control....14

5.4 Documents....15
5.5 Standards....15
5.6 Organisational Context....15
6 The Information Security Risk Management Process....16
6.1 Risk Management is a life cycle....16
6.1.1 Identify Risk....16
Inventory....16
Identification of requirements....16
Asset Valuation....16
6.1.2 Plan Policies & Controls....16
Identification of already implemented Safeguards....16
Assessment of Threats and Vulnerabilities....17
Risk Identification and Calculation....17
Determine acceptable risk....17
6.1.3 Implement Safeguards....17
6.1.4 Monitor & Evaluate....17
6.2 Duties and responsibilities....17
6.3 Risk Review....18
6.3.1 Regular review....18
6.3.2 Risk register....18
6.4 Incident Management....18
6.5 Crisis Management....18
7 Appendix A: GNU Free Documentation License....19
7.1 PREAMBLE....19
7.2 APPLICABILITY AND DEFINITIONS....19
7.3 VERBATIM COPYING....20
7.4 COPYING IN QUANTITY....20
7.5 MODIFICATIONS....21
7.6 COMBINING DOCUMENTS....22
7.7 COLLECTIONS OF DOCUMENTS....23
7.8 AGGREGATION WITH INDEPENDENT WORKS....23
7.9 TRANSLATION....23
7.10 TERMINATION....23
7.11 FUTURE REVISIONS OF THIS LICENSE....24
8 Bibliography....25
9 Alphabetical Index....26

2 Introduction

2.1 Informations about this document

The SOMAP.org Open Information Security Risk Management Handbook (Handbook) is a handbook which contains descriptions and explanations on how to plan, implement and manage an information security risk strategy and ISMS (Information Security Management System) activities.

The SOMAP.org Open Information Security Risk Analysis Guide (Guide) is an integral part of this Handbook. The Guide describes the risk assessment and management process in detail. It discusses the different steps of the risk analysis process and contains the formulas to calculate risk and how to use them.

The Guide and the Handbook are both 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 Handbook for further informations concerning copying and changing parts or the whole of this document.

2.2 Intended audience

This 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 to follow standards is important and how this document can help in doing so.

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.

If you are interested to make your hands dirty or if you want to introduce (or maintain) a risk management process in a company or an organisation, then the SOMAP.org Open Information Security Risk Assessment Guide can help you to get all the informations needed for that.

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 of the gained profit, the health of the company as of 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 not only is 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 Handbook 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 handbook can always be found at the project website at http://www.somap.org/

Version	Information
June, 2006	Release of first public draft.
Version 1.0, September 2006	Release of first version.

3 Risk

3.1 What is Risk

According to [WPRISK], Risk is “the potential harm that may arise from some present process or from some future event”. [ISO73:2002] defines Risk as the “combination of the probability of an event and its consequence”. Which means we are talking about the probability of a negative event which can hurt your business.

We all know risk in one or the other way. We risk our health when driving a car, we risk a crash when flying with an aircraft and we risk our sanity when working with computers. We learned that all of our steps are risky and we learned to calculate and analyse that risk. We did not only learn to calculate risk, but we also learned how important something is for us and we instantly decide if something is worth the risk or not.

If you have a business, there are many risks which influence your business and which can directly or indirectly result in some of these problems:

- Loss of income.
- Loss of competitive advantage.
- Legal penalties.

If a factory burns down, we are not able to produce further goods and we risk a loss of income because of that. If the competition learns about our top secret recipe for our delicious chocolate cake, we risk the loss of competitive advantage.

3.2 Sources of Risk

There are many different sources which can have an impact on an asset and therefore can be a risk. Such a source is called threat. A threat can put one or multiple assets at risk. The following illustration shows how different kinds of risk can be grouped and that the endangering threats can be grouped as well.

When managing risk it does not really matter what kind of risk we want to protect our assets from. While the type of risk could make a difference in our decision if we do and how we do protect an asset it does not really make a difference in managing the risk per se. Although grouping threats can make us understand the situation better.

3.3 Risk is changing over time

3.3.1 Changing habits

The risk in the IT field is changing over time. A few years ago not many computers were connected to the Internet. Nowadays with the prices for broadband falling and households joining the Internet, things changed. The same within the companies. While email was not widely used, nowadays every company needs that form of communication in some form. With these changing habits, the risk is changing as well.

3.3.2 De-perimeterisation

Another trend is what is known as “de-perimeterisation”. While a few years ago every network needed to have a firewall and then everything was good, things changed here as well. Our society is based on a flow of information. That information is constantly moving around, leaving and entering networks around the world. Our main problem is, that this information can not be protected by a simple firewall, because that information will not stay in one place but “move around”. One could argue that we then should keep the informations in one place where we can protect them. But it looks as if our society needs that flow of information to further evolve.

3.3.3 Regulations

Regulations and law changes constantly. With changing regulations the requirements a company must fulfill are changing as well. Not meeting regulations can become a very big risk and can result in big problems for a company and especially its executive board.

4 What is Risk Management

4.1 Risk Management is a process

Risk management is a process we all do every day. We know that juggling with a chainsaw can be risky, especially for our hands. We assess the consequences and how important the juggling is for us. And we will then most probably decide against the juggling. We automatically manage risk.

We do basically the same within our business environment. How risky is it to spend some money on the development of a new software tool? How risky is it to start a new business unit? How risky is it to run our own web server? The whole risk management is about us wanting to do something and us thinking about the consequences this could have. If it is more risky to run our own web server than the gain we get from that server we will probably not install or run our own.

Risk management therefore is here to help us decide on what to do and what not to do. Since deciding on such a question is requiring the calculation of and thinking about many factors, there are strategies and formulas to help. Some of these strategies and formulas can be found in this Handbook. Details about them can be found within the SOMAP.org Guide document.

4.2 Risk Management is daily business

When implementing safeguards and controls based on a risk analysis it does not suffice to only implement those countermeasures. The implemented safeguards and controls also need to be checked regularly. Such maintenance activity includes (not a complete list):

- Analysis of log files.
- Reviewing the implementation of safeguards (and their effectiveness).
- Restarting a new risk analysis when an environment changes.

4.3 Decision-making

If during an assessment a risk is being detected, a decision needs to be made as of what to do with this risk. Depending on the situation and the environment, different strategies can help to manage risk. To help in deciding on what to do with risk, some factors should be analysed:

- The possible impact of an incident.
- The frequency of the incidents.

It is important to not only analyse the possible impact of a realised risk, but also to analyse the costs of the chosen risk mitigation strategy. Protecting a pen with a private armed guard will only be arguable if the pen is worth a kingdom.

Other factors to keep in mind are (in an unsorted list):

- Costs of countermeasures and their implementation.
- Politics and business culture.
- Priorities and available resources.

4.4 Risk Treatment

Risk treatment describes how a risk is handled. This process ends normally in writing a risk treatment plan. This plan contains all the informations of who is doing what and until when. To be able to formulate a risk treatment plan these information needs to be gathered (among others):

- Priorities of the company.
- Dependencies and limiting factors.
- Identification of key stakeholders.

It is also very important to have a clear review process established which controls the risk treatment process and checks that everything runs as planned. Risk treatment is no “fire and forget” process. Controls can introduce new risk which needs to be controlled as well.

For the treatment of the concrete risk there are several strategies. Those strategies can be grouped into two groups.

- Risk acceptance / retention.
- Risk mitigation.

Risk acceptance / retention

Basically risk acceptance means that everybody is happy with the risk and that no further actions are taken. This mostly will happen if the possible impact of a realised risk is too low or if the management of a company is risk hungry.

Risk mitigation

On the other hand there is the risk mitigation. The mitigation of the risk should reduce risk to an accepted level. Please see the risk mitigation chapter for further details on what kind of risk mitigation strategies there are.

4.5 Residual Risk

When managing risk it is the goal to remove or lower risk. Residual risk is the risk which could not be removed (or which was accepted). It is important to stress again that having residual risk is nothing bad but actually the basis of the risk management process. It normally is too cost intensive to minimise every risk and there is no need to mitigate risk which does not hurt a company.

Managing the residual risk is what the whole risk management process is about: Deciding on which risk to take, which to remove and what to do with the residual risk.

Whats very much important when talking about residual risk is to write down when and how the residual risk was accepted and to have the board sign that piece of paper so there exists some evidence when something bad happens.

4.6 Risk Mitigation strategies

4.6.1 Introduction

All these strategies can be applied alone or can be combined for a greater effect. It is important to always be aware that although it is the plan to address risk and to try to minimise risk, risk often can never be completely removed. And although safeguards are in place, these can often open new vulnerabilities and therefore result in new risk.

Just think about a safeguard protecting a web server. That safeguard is managed via a web interface on the web server itself. Although the safeguard is protecting all the web applications on the web server perfectly it opens up a new risk: A weak authentication mechanism to access the management interface located on the same machine as the web applications them selfs.

4.6.2 Risk transfer

When transferring risk we ask somebody else to take the risk for us (normally having us pay that somebody a huge amount of money). When doing a deal with an ISP to have him host our website, we transfer the risk of a defacement of our site to our ISP. Although we transferred the risk to our ISP, this does not mean that the risk is completely removed. Although the ISP now has to patch the web server software and secure the system there is still the potential for a defacement. And although everything is running on that ISP's system, our companies website will be defaced and our customers will see it. So although the risk of a defacement of our website was transferred to that ISP, our company will experience some negative effects as well.

4.6.3 Risk reduction / mitigation

Reducing risk can be done in choosing smaller solutions or installing safeguards and countermeasures. Only serving static websites instead of dynamic ones can reduce the risk of a client exploiting a vulnerability in our web servers code.

Installing a firewall on a computer can reduce the risk of being attacked. But the firewall could be wrongly configured and opening up new vulnerabilities which then could be exploited. Or the firewall – although correctly installed and configured – could not be running and therefor not protecting our asset at all.

It is important to always be aware that reducing risk does not mean that it has to go away and it is also important to always be aware that installing safeguards can open new vulnerabilities or not protect from the vulnerability in the first hand.

4.6.4 Risk removal / avoidance

When removing an asset completely (not running a web server, as example) we reduce the risk of being defaced. Sometimes this is a strategy which can be acceptable. And it is the safest strategy since there is no risk of an unknown vulnerability.

4.7 Limitations of Risk Management

So where does the risk management end, what can not be managed? The risk management can become quite time consuming (and therefor expensive) when it is the goal to remove every risk. Spending too much time on analyzing unlikely or small risk (which easily can be taken) can easily become very expensive.

Although risk management is about managing risk, it does not have a silver bullet on what risk to take and what risk to mitigate. While the management process offers some tools and helps it also requires to have some know-how and some experience. Therefor it is always a good idea to start the risk management process with some expert.

4.8 Approaches to the Management of Risk

There are two possible approaches to manage risk. A proactive and a reactive approach. Both are described in the next sections.

4.8.1 Proactive

Handling the risk pro actively means managing the risk “before something happens”. This is the “good” strategy. Risk Management should be done proactive because this means cost effectiveness and low risk.

4.8.2 Reactive

Managing the risk reactively means that there is only an reaction “after something happened”. This approach is also known as firefighting. Reacting on risk when an incident or attack happened means cost ineffectiveness and is a highly risky approach.

4.9 Risk Prioritisation

The analysis and calculation of risk can be done in two ways which are detailed in this chapter.

4.9.1 Qualitative Method

Qualitative risk management is done using estimations of cost, impact and likelihood. When doing a qualitative analysis real monetary values are never used.

The qualitative method is more common than the quantitative method. The reason for this is mostly that it is much easier to use estimations than real values and that the calculation mechanism is easier to be accomplished.

4.9.2 Quantitative Method

The quantitative method is based on real monetary values and tries to be as exact in its calculations as possible. This method is not as widely used as the qualitative method, mostly because of its complexity. With this method every incident needs to be estimated concerning the incidents monetary consequences which can become very complex.

4.10 Why Risk Management is important

Risk management is not only important because we could loose money or competitive advantage. Risk management is also important because of these reasons:

- Risk management is a way of justifying expenditions.
- The board is mandated to know about the risks.
- Security officers have to report to the management about the environment. At least in some countries and in some companies.
- Rely on Information Systems: Information Security is a management issue because the companies dependency of the IT is so high.

Besides those reasons, there are also other reasons like:

- Risk management can be used as evidence for an Information Security Management System (ISMS). Such a system can be a requirement by regulation (or when a disaster happens the insurance company could ask for an ISMS).
- Risk management has to be practiced when certifying a company.

There are of course many more reasons why Risk Management is important. These reasons will most probably change from situation to situation.

4.10.1 Value of Informations and New Challenges

Value

To define the value of information is a difficult thing. What is the value of an information system? What is the value of an asset? An asset can easily be valued. A server costs an amount of money to buy. But what is the data worth stored on the server? What does it cost when a mail server is not

available for a few hours? These questions are indeed very difficult to answer.

Theft

There is also a change in the way we used to think. What is information theft? Nothing is “away”, every bit is still available, the theft consists of a copy of the “stolen” data. The problem with that is that we can not detect theft of data as easily as theft of a physical object like a chair or a file cabinet. How can theft be detected, where (and what) is the evidence helping us find the thieve? These questions are very differently answered for different assets.

Unknown Threats

There are many threats which we today do not know about yet. Risk management helps in planning and preparing for unknown threats.

5 Information Security Management

It is a very important fact that security has to enable business and not hinder it. All security mechanisms must therefor not be hindering the daily business. Risk management means minimising risk and maximising the business opportunity. This has several reasons.

Security mechanisms which hinder somebody doing his job will some when be disabled (as more they hinder, as sooner they are disabled) or removed. Which will result in not having any security mechanism at all.

Hindering security mechanisms are highly unproductive which also means that the security officer has no deeper understanding of the daily business. The security officer should learn about the business and then work with the employees and not against them to implement cost effective and "transparent" security mechanisms.

To be able to implement cost effective and safe security mechanisms the security officer needs to manage several components as described in the next chapter.

5.1 Management Components

Information security management is an interaction between the following components:

All of these components are a requirement of the [ISO27001:2005] standard.

5.1.1 Ownership

Owner

Every asset has an owner. Even if you are not aware that this is true, every asset has somebody which is responsible for it. Or at least, somebody should be responsible. Only that owner can (and has to) decide on the worth of an asset.

A security officer never should be the owner of an asset. Even if this could look like a good idea, it is not. At the end the security officer would be responsible for all the assets which he obviously can not be.

Custodian

The owner can define a custodian. It is then the custodian which looks after the asset instead of the owner.

5.1.2 Risk analysis

Risk analysis is the process of assessing assets, threats, vulnerabilities and calculating the risk from those factors. The risk analysis is described later in this handbook and in detail within the SOMAP.org Guide.

5.1.3 Policy

Policies are not going into technical details but describe rules and approved technologies.

5.1.4 Organisation

The security officer has to learn and know about the overall business culture and environment. If he does not know about those he can not implement and validate effective security mechanisms.

5.1.5 Guidelines

Guidelines contain informations on how things should be done and what is accepted and what not.

5.1.6 Due care

IT Security is a management issue. The management has to learn and know about their assets and risk. And the board has to decide on what risk they agree to take.

5.1.7 Procedures

Procedures contain very detailed information on how things have to be done.

5.1.8 Support

There needs to be a documentation of who does what. There needs also to be a documentation on when who changed what and why. Only with this documentation it is possible to learn about the environment and what changes were applied.

5.2 Keys to success

For a successful security management there are several points to take care of:

- Executive sponsorship.
- Stakeholders (Roles & Responsibilities).

The security management is successful when all the involved persons know why they need a security management and when they are willing (and prepared) to invest in the security of their assets. Like that it is important that the management sponsors the security management. This sponsorship makes the security management an important part of the business of a company which is the first step (and a must) to success.

5.3 Internal Control

Internal Control is about checking the facts and figures of a company. It helps in avoiding misuse of any of a companies (financial) assets but the Internal Control can also be used as evidence in an external assessment or evaluation of the company.

The following list contains a few reasons why Information Security is a part of the Internal Control:

- Data Classification.
- Change Management.
- Document Management.

5.4 Documents

The requirements concerning Documents and the availability and management of them is quite similar among the more common standards like ISO/IEC 9001 and [ISO27001:2005]. All of these standards require that all the documentation is stored so that only authorised users have access and so that the documents are versioned and released according a defined procedure.

As a simple rule concerning documentation it can be said that every step and every decision needs to be written down and archived. These notes and documents can then later be used as evidence during an assessment or audit.

5.5 Standards

There exist many standards for information security management. The SOMAP.org project tries to be as compatible with the more common ones as possible. When starting with Information Security Management it is important to choose if it is a requirement to follow a standard and then to define to work toward achieving compliance with which one of them. While many of the standards are compatible with each other, some of them are quite different to the rest.

Please see the Bibliography at the end of this Handbook for further references to standards.

5.6 Organisational Context

The information security management needs to have a business case. This means that information security is not some component which just can be bought and added to the mix. A business needs a reason to add information security: There must be an asset at stake or a risk to be managed.

Therefor a business should define the scope of the information security management and the management should formulate a policy on how to life information security management. Once it becomes clear what's the goal of the information security management, somebody (typically a security officer) has to identify and adopt a systematic method and approach to information security management and the risk assessment.

6 The Information Security Risk Management Process

6.1 Risk Management is a life cycle

Risk Management is a continuous process as illustrated in the image below:

The risk management process starts with the assessment of risk and ends with monitoring and evaluating the implemented safeguards. It then restarts at the beginning to address changes which could have happened since the last assessment. This process is described in detail below.

6.1.1 Identify Risk

Inventory

First step is to create and maintain an inventory. The inventory contains the assets of an environment. An inventory can be built from scratch, generated from a questionnaire or imported from an already installed inventory management system.

It is important to not get lost in micro management when trying to manage an inventory. An inventory normally is not precise into every detail. It is a good idea to group similar assets together.

When creating an inventory, every asset should have an owner. It is important to identify an owner of every asset (which is not the CSO). Without an owner, there is no responsibility for the asset (and the implementation of possible safeguards).

Identification of requirements

Every company has to comply with business or legal requirements. These requirements must be identified and taken into considerations during the risk management process.

Asset Valuation

Every Asset has a value for the owner. According to Clause 7.2 of the ISO/IEC 17799:2005 standard it is the assets owner responsibility to define and review the classification of the asset.

6.1.2 Plan Policies & Controls

Identification of already implemented Safeguards

Before diving too much into the detail of the risk assessment it is important to identify already implemented Safeguards. This step is important because with this information it is possible to find out the effectiveness of an already installed safeguard.

Assessment of Threats and Vulnerabilities

In this steps Threats and Vulnerabilities are identified. Doing so can be very difficult, especially because it is the goal to assess all possible threats and vulnerabilities. This step is normally done with the help of a repository of threats and vulnerabilities. The idea of such a repository is it to assist in the process to identify possible threats and vulnerabilities which match with the assets from within the inventory.

One of the steps during the assessment of threats and vulnerabilities it the process to define the likelyhood and impact of a vulnerability. The value for the likelihood is best obtained from those directly involved with the business process or asset at risk.

Risk Identification and Calculation

When all factors are known, the risk can be calculated and visualised. During this step the Business Impact Assessment can help in finding the biggest risk. Please consult the SOMAP.org Guide for details in how to calculate which factors with what formulas.

Determine acceptable risk

When all the risks are known and it is clear which risk is the biggest, the security officer generates a risk assessment report. This report is the basis for the Board to determine the acceptable risk. Once it is clear which risks are accepted and which Safeguards and Controls are implemented a final risk assessment report is generated. This report has to be accepted by the Board.

With accepting the risk assessment report, the Board gives the security officer the task to implement the required safeguards.

6.1.3 Implement Safeguards

It is not the security officers job to manage the implementation of safeguards and controls. While he does manage the implementation, he does not implement the safeguards himself. This is the job of the asset owners or custodians. The asset owners have to implement the safeguard or at least give the order to do so to a third party.

6.1.4 Monitor & Evaluate

During the implementation of safeguards as well as afterwards the security officers controls and monitors the implemented safeguards and assets.

When an asset changes (added to the inventory or removed from) or when a safeguard changes, the risk management life cycle is started again from the beginning. Every change within an environment can introduce new risk or change the risk factor of already existing (and managed) risks.

6.2 Duties and responsibilities

The following table contains an overview of who is actually doing what during the Risk Management lifecycle. It is important to stress the fact that the risk management is only worth the effort when everybody active within the risk management lifecycle knows what she has to do and why.

Who	What
Executive Management	Determination of acceptable risk.
Infosec Department	The assessment, identification of requirements, implementation of Safeguards and restarting the lifecycle.
Operations	Implementation of safeguard requirements.
Stakeholders	Filling out questionnaires.
Owner	Defining classification and value of assets.

6.3 Risk Review

6.3.1 Regular review

Risk should be reviewed on a regular basis. The risk management life cycle should be restarted at least once a year to every 18 months. Factors in the decision how often to do a risk analysis are:

- Changing assets.
- Changing environment.
- Implementation of Safeguards.
- Status of Safeguards.
- External events (Exploits, disasters, trends, ...).

Based on these factors, the security officer should decide on a regular review cycle.

6.3.2 Risk register

A risk register is the backlog of all the informations gathered from every risk analysis done. Such a risk register helps in compiling reports on tendencies, implemented safeguards and the effectiveness of the whole risk management process in general.

The risk register builds the basis for risk communication between the security department and the rest of a company (and beyond).

6.4 Incident Management

The incident management is the process of planning and preparing for any unwanted occurrence. It is about what to do when a web site is defaced. The incident management prepares detailed instructions in how to proceed, secure evidence, get the intelligence how things happened and then return to the normal state.

6.5 Crisis Management

The crisis management is planning and managing the time between an event (it needs to be a huge event, sinking ship, peoples life threatened as example. Otherwise the incident management will suffice.) and the recovery. The crisis management is about analysis a crisis situation and deciding a response.

Risk management is **not** crisis management. But managing risk successfully means also to manage an incident or a crisis.

7 Appendix A: GNU Free Documentation License

Version 1.2, November 2002

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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 entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity 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.

7.6 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."

7.7 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.

7.8 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.

7.9 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.

7.10 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.

7.11 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

8 Bibliography

Where to find further informations

- [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*.
- [ISO27001:2005] ISO/IEC (2005), *Information technology. Security techniques. Information security management systems. Requirements*.
- [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.

9 Alphabetical Index

De-perimeterisation....7
Incident management....18
Internal Control....14
Lifecycle....16
Responsibilities....17
Risk acceptance / retention....9
Risk Mitigation strategies....9
Risk reduction / mitigation....10
Risk removal / avoidance....10
Risk transfer....9
Sources of Risk....6
Standards....15