UNIVERSITY OF OSLO
Department of Informatics

Model Driven Availability Risk Analysis (MODA)

Mihail Korabelnikov

Cand Scient Thesis

30th of January 2004

Foreword

This thesis is submitted for the *Cand. Scient*. degree in Informatics at the Department of Informatics, University of Oslo (UIO). The thesis has been written at SINTEF under supervision by Chief Scientist Ketil Stølen.

I would like to thank my wife Irina for her support, my daughter Nicole for crying during the nights and son Alexander for taking care of his little sister.

Especially, I would like to thank my adviser, Ketil Stølen for his inspiration and guidance throughout the work on this thesis.

Abstract

The availability of data systems is one of the greatest challenges companies face today. Keeping a high level of availability is not a trivial task:

Security technology may be deployed incorrectly and does not give a company an effective protection against security threats. Security measures must be incorporated and assessed to protect data systems and company infrastructures against a massive range of threats and vulnerabilities that affect availability of data systems.
Businesses today must be responsive and change very rapidly. Their supporting software systems must change equally rapidly. The change in the system architecture may lead to change in system availability. This should be addressed quickly.
The threats and vulnerabilities are not standardised, but are situation dependant. This is why organisations and companies have to assess risks to the availability of a data system regularly. A regular availability risk assessment may be very costly for a company.

This thesis presents Model Driven Availability Risk Analysis (MODA), a methodology for identifying, assessing and treating risks to availability of data systems. MODA aims to take one step in the direction of addressing the challenges sketched above and aims for improved time efficiency, cost effectiveness, and usability.

To successfully analyse system availability, we need to know all the key areas of risk to system availability. We identify these key areas and define four sub classes of availability, the so-called availability aspects: Network availability, Software availability, Hardware availability, and Human availability. Further, we decompose each availability aspect into more basic entities, define the relationship of each aspect to other availability aspects and identify the assets that can be affected by its denial.

The risk assessment community makes use of a structured approach to address risks – the so-called Risk management process. The MODA risk management process is based on AS/NZS 4360:1999 Risk Management [6] and CORAS [5] and we decompose it into sub-processes for context identification, risk identification, risk assessment, risk evaluation and risk treatment. We present MODA in an example-driven manner in the form of a small case study. Further, to evaluate the suitability of MODA we conduct a larger case study using MODA to assess the availability of a chat service.

Table of Contents

List of Figures

List of Tables

1 Introduction

> *"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts."*
>
> Eugene H.Spafford

1.1 Characterisation of the problem

Progress has given to humanity many useful things, but the same progress has given people a lot of problems. It is hard to imagine a modern company that runs business without computers. An active use of the Internet is now one of the most important factors that contribute to the business success. The number of computer systems that process different kinds of information is increasing every year. These data systems are made to perform information services. If an information can not be accessed by service consumers, the result can be the reduction of competitive ability and reputation of service provider as well as financial losses for both service provider and service consumer. Many companies now are realizing that their prosperity, new markets penetration and customers satisfaction are very much dependent on the availability of services that these companies offer to their clients. In many industrial countries people can choose among tens or hundreds of companies that offer services based on the 24X7 concept. This means that a service is available 24 hours per day, 7 days per week.

Business has opened thousand doors inviting employees and clients to either complete a business process or place online orders. But this openness has its cost. Today, information security is the one of the greatest challenges companies face in the world of e-commerce and growing use of Internet for business needs. Their infrastructures are exposed to a massive new range of threats and vulnerabilities that affects availability of data systems. The number of financial losses that are caused by computer crimes, and number of hacker attacks on data systems are growing every year. As a result of this, companies use more and more money on security and the number of security technologies applied by companies is steadily increasing every year. In spite of this fact, the press release of American Computer Security Institute [1] shows that the number of companies that detected computer security breaches, increased 5 % from the year 2001 to the year 2002. This fact shows that security technology does not necessarily give a company an effective protection from security threats. One major reason for this phenomenon is the fact that ***security technology is often deployed incorrectly.***

The importance of availability can be exemplified by a management system that optimizes production on a factory or controls parameters of important components of an airplane. Vladimir Galatenko and Igor Doroshin note in their article "Availability as an element of information security" [2] that an operator on a chemical factory is able to perceive less than 1% of the information of the technology process. The denial of availability of this kind of data system can have very serious consequences. Less serious, but also very unpleasant – both materially and morally – may be the result of long-term unavailability of a data system offering services used by many people. While the denial of availability of the data system of an Internet bank or travel agency can affect tens or hundreds of thousands of people, the denial of availability of the data system of a national bank can affect the national security of a country.

People can be divided in two categories: those who use computers at work or at home and those who don't. While the number of people in the last category is reducing every year, the number of people in the first category is steadily increasing together with user demands to their "cybernetic friends". We all want to have the fastest Internet connection, immediate response from application programs and 100 percent uptime of the system. But our wishes brutally collide with reality. Today we live in the world where terrorist attacks are happening in countries that were hard to imagine as terrorist targets ten years ago. The heart of the modern computer world – the Silicon Valley in California, experiences planned power blackouts and the most popular operating system is famous for something called The Blue Screen of Death. The modern world is also characterized by uncompromising competition among companies. The new software is expected to have more features and as result this increased complexity.

IT systems are getting more and more complex and this fact is itself a serious threat. Many data systems are so tightly integrated that it is almost "impossible" to keep an overview of their structure – which is an obvious precondition to obtain a highly available data system. Liberalisation and demonopolisation of infrastructures further increased information exchange with the help of the Internet between private persons and between organisations and companies. This fact in turn brings on to the necessity of integration of data systems that were physically separated. After the integration or development of a data system, developers can discover new security breaches that need complicated, expensive and time-consuming solutions. One way to reduce development costs can be the assessment of consequences of system changes in the design phase. It is much cheaper to make changes in the design of a system then to make changes in a developed system. Many companies know this rule, but are still faced with additional work after development of the system. One of the problems is that ***availability is often considered first after integration or development*** of the system.

It is also very important to have a good balance between the level of security and the accessibility and user friendliness of the data systems. What we have here is a paradox. On the one hand, we as computer users, expect more functionality and availability from software products, and on the other hand, software producers provide lower and lower levels of availability as their products increase in complexity, and delivery times gets shorter and shorter. The case of deployment of the VISA SET [3] standard for secure use of credit cards for net shopping shows that millions of dollars were spent to develop the system which was not widely accepted. The system software was too "heavy" and complicated, and maybe too secure. Now, VISA is concerned with just being "secure enough", and has announced the new pay solution for Internet - 3D Secure. This fact shows that ***too much security can make the system impossible to use*** or in other words – too much security can negatively affect availability of the system.

Unreliable software is not the only reason for the reduction of availability of a data system. A serious threat to availability of a data system is the so-called Denial of Service Attack (DoS) – an attack that breaks the functionality of a data system by sending much more requests than the data system is able to process. For example, as a result of DoS attack [4] in february 2002, the normal work of Internet service providers (ISP) in U.S.A like ShiffOut, TheDotComplete, The DogmaGroup and Firenet, was affected. The DoS attack SYN Flood [4] in December 1996 had the effect that the web server of the American Internet provider Web Communications LLC, could not give internet access for more than 40 hours to more than 2200 corporate clients.

Reduced availability of a data system also can be caused by application software that is attacked by computer virus. For example, after the epidemic of the computer virus Code Red in August 2001, the American ISP Qwest DSL [4] had to pay a lot of money to its customers as compensation for lost Internet connection caused by functionality problems of company equipment affected by the virus. Along with hacker attacks and problems with software, the availability of a data system also depends on the proper functioning of hardware. It is not hard to imagine how effective an air traffic operator can be if the monitor of his computer does not work.

We as system developers cannot consider a technological system separate from its users and the company in which it is supposed to work. System developers have to carefully study the environment of the system's deployment, the system's future functionality, and the external and internal infrastructures of the organisation in which the system is to be deployed. Hence, ***availability cannot be handled by analysing technology alone***. The most advance and secured data systems can not function effectively without people updating its software and hardware. Incompetent and irresponsible employees also can cause a lot of damages to data systems and company businesses. The use of Internet for personal purposes is now a serious problem faced by many companies. An army of clerks and managers equipped with keyboard and mouse is surfing on the Internet waves day-by-day and week-by-week. During the work time, people send personal email, read anecdotes, play games, download music, films and unauthorised software, and chat with friends. All these inappropriate user actions directly affect the productivity of employees and the availability of services that a company offers to its clients. Aleksei Lukatski in his book "Attacks identification" [4] shows that every company loses about 825 dollars per year as a result of use of Internet of one employee for his or her personal purposes.

Software developing companies use different methods and techniques to support availability risk assessment. Their ability to understand and manage these methods and techniques will be crucial to protecting brand image, developing customer confidence and achieving long term success. Keeping availability of a data system at a high level costs a lot of money. It is not enough to have firewall, update software and hardware regularly or use powerful antivirus software. Personnel have to regularly attend courses to keep their knowledge updated and the company has to test all data system components regularly. Today, the threats and vulnerabilities are not standardised, but are situation dependant. That's why organisations and companies have to assess availability risks regularly. But ***availability risk assessment is costly,*** and many companies do everyday exercises in balancing cost against the threats.

1.2 Model Driven Availability Risk Analysis

The problems that we have highlighted so far show that we need risk and availability assessment methodology that will be effective, sufficiently cheap, and easy to use by the risk assessment practitioners in the early stages of the development process. This methodology should support people participating in the availability risk assessment in gaining a better understanding of the system environment and assists their communication by presenting information in an understandable manner. The objective of this thesis is to take one step in this direction by proposing an availability risk assessment methodology called MODA (Model Driven Availability Analysis).

The MODA methodology can be seen as a specialization of the CORAS model based security risk assessment (MBRA) methodology [5] targeting availability. CORAS builds on the concept of applying systems modelling when specifying and describing the systems to be assessed as an integrated part of the risk assessment. The practical use of models in the risk assessment is motivated by several factors:

- Risk assessment requires proper descriptions of the assessed system, its context and all security features. The modelling technology improves the precision of such descriptions. Improved precision is expected to improve the quality of risk assessment results.
- Graphical models further the presentation of information in an unambiguous way to participants of the risk assessment. This is expected to improve the quality of results, and also speed up the risk analysis process since the danger of wasting time and resources on misconceptions is reduced.
- The modelling technology facilitates a more precise documentation of risk assessment results and the assumptions on which their validity depend. This is expected to assist to the reduction of maintenance costs.
- The modelling technology provides a solid basis for the integration of assessment methods that should improve the effectiveness of the assessment process.
- The modelling technology is supported by a rich set of tools from which the risk analysis may benefit. This may improve quality, reduce costs and further productivity of risk assessment.
- The modelling technology provides a basis for tighter integration of risk management in the system development process. This may considerably reduce development costs and ensure that the specified security level is achieved.

1.3 Report structure

This report is divided into eight chapters and four appendices as specified below:

- Chapter 1: **Introduction**
  Provides the motivation for the development of MODA, presents the main rational behind MODA and gives the overview of the report structure.
- Chapter 2: **Background**
  Gives an overview of the CORAS methodology, provides definitions relevant for availability, explains risk assessment with a little example, and clarifies the use of UML for the availability assessment.

- Chapter 3: **Problem analysis**
  Motivates and presents the MODA success criteria, and discusses research strategies that can be used for the validation of MODA success criteria.
- Chapter 4: **Availability decomposed**
  Decomposes availability into 4 availability aspects: network availability, software availability, hardware availability, and human availability; defines the relationships between availability aspects and between availability aspects and assets.
- Chapter 5: **Model Driven Availability Risk Analysis (MODA)**
  Provides the description of MODA and exemplifies its usage in a small case study of availability risk assessment.
- Chapter 6: **Using MODA to assess a Chat Service**
  Demonstrates MODA in a major case study.
- Chapter 7: **Discussion**
  Discusses MODA and shows what could be done different.
- Chapter 8: **Conclusion**
  Provides the main conclusions of the report, shows how MODA meets the success criteria, and discusses relevant and future work.
- **References**
  Provides references.
- **Appendix A**
  The first part provides consequence and frequency tables for the availability risk analysis; the second part provides questionnaires for assets identification.
- **Appendix B**
  Provides templates for the MODA risk treatment sub-process.
- **Appendix C**
  Provides risk treatment tables and risk treatment priority tables for the case study of Chapter 6.
- **Appendix D**
  Provides documentation for the case study of Chapter 6.

Figure 1.1 gives a description of the report structure. The arrows show alternative sequences in which the chapters and appendices may be read.

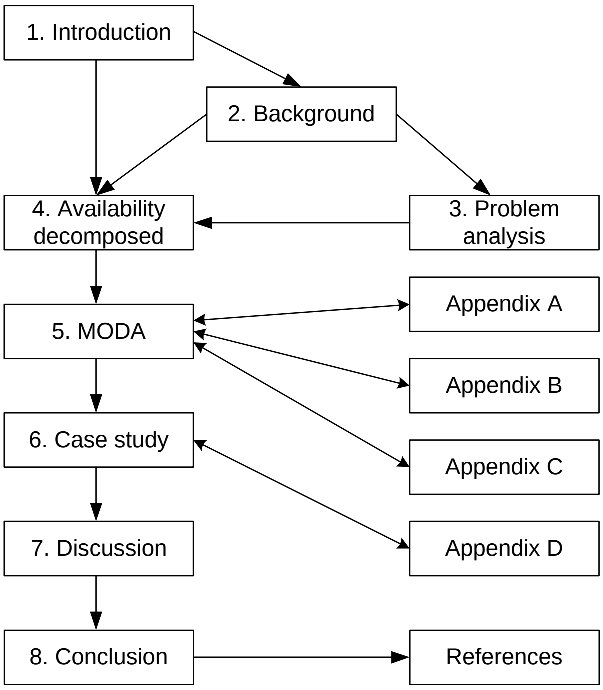


Figure 1.1: Reading guide to the report

If the reader is familiar with the background information in chapter 2, it is possible to go directly from chapter 1 Introduction to chapter 4 Availability decomposed. If the reader is not interested in the MODA success criteria, he may skip chapter 3 Problem analysis. The arrows with two pointers indicate that the reader should use the information from appendices A, B and C when he reads chapter 5 and the information from appendix D when he reads chapter 6.

2 Background

In this chapter we provide necessary background information. The chapter is structured into four sections. Section 2.1 presents and explains risk assessment with the help of a little example. Section 2.2 gives an overview of the CORAS methodology for model-based risk assessment that has been an important source of inspiration. Section 2.3 gives the definition of availability, security and other important notions. An important part of MODA is the practical use of UML to support availability risk assessment. Section 2.4 motivates and explains the use of UML for the risk assessment.

2.1 Risk assessment

Risk is a part of everyone's life, and people would like to have control over the risks they face on a daily basis. The Australian Standard for Risk Management [6] defines risk as " The chance of something happening that will have an impact upon objectives." The same standard defines the risk management process as "The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk". By doing risk assessment, you can identify threats in advance and treat them before they will harm you, your plans, business or project. It can be much cheaper to address the identified risk by avoiding it or minimizing its effects than be unprepared and spend time and money on recovery.

The Risk assessment community uses different approaches and methods for the risk assessment. For example, while Sommerville [7] decomposes the risk management process into four stages for risk identification, risk analysis, risk planning, and risk monitoring, AS/NZS 4360 [6] provides a sequencing of the risk management process into sub-processes for context identification, risk identification, risk assessment, risk evaluation, and risk treatment. In addition, the latter operates with two supporting sub-processes that help project leaders to have an overview of the fist five processes.

We base our risk management process on AS/NZS 4360. In the following we illustrate the risk assessment with a little example.

Context identification

The goal of this sub-activity is to establish the objectives, strategies, scope and parameters of the system, including the specification of the risk assessment resources required and the risk assessment records to be kept. By defining the target of evaluation, we specify what we are going to analyze – the whole system or some parts of this system. By specifying objectives and parameters of the target system we get a clear understanding of the system usage and its role in the surrounding environment.
Imaging you are going to travel with your car in the winter across Scandinavia. You can define that the target of evaluation is a car that should drive in the winter across Scandinavia. By specifying parameters of the target system – the car, you will define components such as motor, chassis, clutch, wheels that contribute to the system functionality and which will be the valuable information for the risk identification sub-process.

Risk identification

If you are going to travel with your car in the winter across Scandinavia, you can face several threats that can make your journey less pleasant than anticipated. For example, the tires of your car can be punctured, your car can stop because of lack of fuel or you will not be able to drive your car because of ice-crusted road.

The objective of risk identification is to define threats that are relevant for your target of evaluation. In our case we can define that the most serious threats for our car trip will be tire puncturing and ice-crusted road.

Risk analysis

Now when we know the possible risks to our car trip, we have to analyse them and ask ourselves what are the consequences of these risks (unwanted incidents) and how big is the probability that these risks will actually happen. The consequence and probability of risk can be assigned quantitative values or qualitative values like: *Nil*, *Very Low*, *Low*, *Medium*, *High* and *Very High* [8]. If you don't have an additional tire, the consequence of tire puncturing will be inability to drive the car and maybe you will have to wait quite long for technical help. If you don't have winter tires, the consequence of ice-crusted road can again be your inability to drive the car. By defining the probability of identified unwanted incidents, you have to take into account circumstances that are relevant for your case. For example, the probability that you will puncture the tire will be higher on the dirt road then on the main road. In our car trip case, we decided that the tire puncturing will have the same consequence as ice-crusted road, but ice-crusted road will have higher probability than tire puncturing.

Risk evaluation

The objective of risk evaluation is to define priorities of the identified risks for further treatment. By comparing the consequence and probability of risks, you get an estimate for risk level or its severity. Simplistically, you compare consequences and probabilities of different risks to decide which of them should be treated first. If a risk has a very small consequence or its probability is near 0, then its treatment can be postponed or it may be removed from the list of your risks. In our car trip example, the risk level of ice-crusted road will be higher than the risk level of tire puncturing and we decided to treat first the risk of ice-crusted road.

Risk treatment

The objective of the risk treatment is to define treatment approaches for each identified risk. For each risk, we can consider one or several of the following treatment approaches [6]:

- Risk avoidance
- Reduction of likelihood
- Reduction of consequence
- Risk transfer
- Risk retention

For example, we can reduce the likelihood of tire puncturing if we choose only main roads for our car trip. We can reduce the consequence of tire puncturing if we bring along additional tires. To reduce the likelihood of ice-crusted road, we can choose to use winter tires and drive only in the daytime. To reduce its consequence, we may have some additional equipment in the car (e.g. special chains for tires) that we can use in case of difficult road conditions.

2.2 CORAS

CORAS [9] is a EU-funded research and technological development project under the Information Society Technologies (IST) Programme that was completed in October 2003. Its main objectives were:

- To develop a practical framework exploiting methods for risk analysis developed within the safety domain, semiformal description methods (in particular, methods for object- oriented modelling), and computerised tools (for the above mentioned methods), for a precise, unambiguous, and efficient risk analysis of security critical systems.
- To apply the framework in security critical application domains.
- To assess the applicability, usability, and efficiency of the framework.
- To promote the exploitation potential of the CORAS framework.

CORAS adapted, refined, and combined methods for risk analysis, semi-formal description methods – in particular, methods for object-oriented modelling, and computerised tools, to build a specialised RM-ODP [10] inspired framework targeting risk analysis of security critical systems.

The main deliverable of the CORAS project is the CORAS framework that is characterised by:

- A careful integration of techniques and features from partly complementary risk analysis methods like HazOP [11], FTA [12], FMECA [13], CRAMM [14] and Markov analysis [15].
- Patterns and methodology for UML oriented modelling targeting the different risk assessment methods.
- A risk documentation framework based on RM-ODP [10].
- An integrated risk management and system development process based on UP [16].
- A platform for tool-inclusion based on XML [17].

The CORAS risk management process is based on the standards

- AS/NZS 4360:1999 Risk Management [6].
- ISO/IEC 17799-1:1999 Code of Practice for Information Security Management [18].

and complemented by

- ISO/IEC 13335: Information Technology – Security Techniques – Guidelines for the Management of IT-Security [19].
- IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related (E/E/PE) Systems [20].

The CORAS risk management process is decomposed into five sub-processes for context identification, risk identification, risk analysis, risk evaluation and risk treatment that are in turn decomposed into activities as described in Figure 2.1. The main concepts in the CORAS risk management process are presented in Figure 2.2 [5].

CORAS sub-processes				
Sub-process 1 *Identify Context*	Sub-process 2 *Identify Risks*	Sub-process 3 *Analyse Risks*	Sub-process 4 *Risk Evaluation*	Sub-process 5 *Risk Treatment*
▪ Identify areas of relevance ▪ Identify and value assets ▪ Identify policies and evaluation criteria ▪ Approval	▪ Identify threats to assets ▪ Identify vulnerabilities of assets ▪ Document unwanted incidents	▪ Consequence evaluation ▪ Frequency evaluation	▪ Determine level of risk ▪ Prioritise risks ▪ Categorise risks ▪ Determine interrelationships among risk themes ▪ Prioritise the resulting risk themes and risks	▪ Identify treatment options ▪ Assess alternative treatment approaches

Figure 2.1: The sub-processes and activities of the CORAS risk management process

- **Risk management:** The culture, processes and structures that are directed towards effective management of potential opportunities and adverse effects.
- **Risk management process:** The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
- **Risk identification:** The process of determining what can happen, why and how.
- **Risk assessment:** The overall process of risk analysis and risk evaluation.
- **Risk analysis:** A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
- **Risk evaluation:** The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
- **Risk treatment:** Selection and implementation of appropriate options for dealing with risk.

Figure 2.2: Main concepts in the CORAS risk management process

2.3 Security aspects

Keeping the availability of a data system on a high level is not a trivial task. Security measures must be incorporated into computer systems whenever they are potential targets for malicious or mischievous attacks. Availability cannot be considered separately from security and this fact brings on the need to understand availability in the perspective of security domain. What we need is a clear definition of availability, security and the concepts that are relevant for them.

Computer systems do not always fail in the same way. Some security threats may affect system availability while others may not. **Threat** is defined by [21] as “a potential cause of an unwanted event, which may results in harm to a system or organisation and its assets”Security threats may also affect other system attributes such as *system service*, *system function* (system functionality), and *system dependability*. In the article “Fundamental Concepts of Dependability” [22] Avizienis, Laprie and Randell define these system attributes in the following way: “**Dependability** of a computing system is the ability to deliver service that can justifiable be trusted. The **service** delivered by a system is its behaviour as it is perceived by its user(s); a **user** is another system (physical, human) that interacts with the former at the service interface. The **function** of a system is what the system is intended for, and is described by the system specification”.

What is IT security? ISO/IEC TR 13335-1:20001: Information technology – Guidelines for the management of IT Security – Part 1: gives the following definition of IT security:
IT security includes all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of IT systems [23].

This is in agreement with other definitions of security, which also view it as a composite notion. For example, [22] defines security as follows:
Security is the concurrent existence of a) availability for authorized users only, b) confidentiality, and c) integrity.

Figure 2.3 shows the definition of IT security terminology [19] on which this thesis will be based:

- **Accountability:** The property that ensures that the actions of an entity may be traced uniquely to the entity.
- **Authenticity:** The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
- **Availability:** The property of being accessible and usable upon demand by an authorised entity.
- **Confidentiality:** The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
- **Data Integrity:** The property that data has not been altered or destroyed in an unauthorised manner.
- **Integrity:** See data integrity and system integrity.
- **Non-repudiation:** The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later.
- **Reliability:** The property of consistent intended behaviour and results.
- **System Integrity:** The property that a system performs its intended functions in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system.

Figure 2.3: The definition of IT security terminology

2.4 UML

To make a proper risk assessment, it is not sufficient to consider only technical system documentation; a clear understanding of system usage and its role in the surrounding organisation is just as important. Stakeholders participating in an availability analysis *need a correct description of the target of evaluation at the right level of abstraction,* and are defined by [6] as “people and organisations that may affect, be affected by, or perceive themselves to be affected by, a decision or activity”.

Another challenge is that the availability risk analysis is costly and time consuming and should not be initiated from scratch each time we analyse a new or modified system. Hence, *we need means to support the documentation as well as reuse of risk assessment results.*

The risk assessment team consists of "those who perform all sub-processes and deliver the risk assessment report to the client" [5]. The members of a risk assessment team are required to communicate in order to capture and analyse the functionality and characteristics of the system in question. They *need effective means that can help them to establish a common understanding of aspects relevant for the risk assessment.*

The UML [24] – Unified Modeling Language is today the leading specification language in software engineering. UML is graphical and helps to address above challenges in the following sense:

- UML models allow documenting the various aspects of the target of evaluation in a uniform manner. For instance, UML graphical models can be used to explain important details of the target of evaluation to domain experts.
- Documenting availability assessment with help of UML graphical models supports reuse of analysis documentation, both for systems that undergo maintenance and for new systems, if similar systems have been analyzed earlier. For example, the availability assessment team can reuse UML graphical models from previous availability assessment to describe aspects that are relevant for the current availability assessment.
- UML diagrams abstract the essential details of the underlying problem and in this way support the communication and interaction among stakeholders with different background involved in a risk assessment. For instance, technical personnel can use UML graphical models to express their ideas in a way that can be understood by people without technical background.

The Object Management Group (OMG) owns the UML trademark and manages its evolution. UML defines twelve types of diagrams: four are used to describe the static structure of a system, five describe dynamic aspects, and three are used to represent ways to organize and manage application modules. Today, UML tools are available from a number of vendors and software developers can combine different UML tools to tailor their development environments. For example, to facilitate modelling of a net bank system, a software development team can combine one vendor's UML framework for modelling security aspects of a data system with another vendor's UML framework for modelling of financial systems. For more information about UML, we refer to [25].

3 Problem analysis

This chapter is structured into two sections. Section 3.1 motivates and presents the success criteria for MODA. Section 3.2 presents research strategies and defines the ones we will use for the evaluation of the MODA success criteria.

3.1 MODA success criteria

In the following section we present a set of statements about what MODA should be and motivate why these aspects are important for the final product. When evaluating the final methodology, we will evaluate it against these criteria.

As we mentioned in chapter 1, information security is one of the greatest challenges companies face today. Security measures must be incorporated to protect data systems and company infrastructures against a massive range of threats and vulnerabilities that affect availability of data systems. These security threats cannot be ignored during the availability risk assessment. Hence we need availability risk assessment methodology that *addresses availability in a security context.*

Success criterion 1	**MODA should target availability in a security context**

Figure 3.1: Success criterion 1 for MODA

Businesses today must be responsive and change very rapidly. Their supporting software systems must change equally rapidly. Time is money - everyone knows this by-word. Time too is very important for companies and their employees. The company project managers as well as other members of the risk assessment team are not interested in spending a lot of time on availability risk assessment. Hence we need availability risk assessment methodology that is *time efficient*.

Success criterion 2	**MODA should be time efficient**

Figure 3.2: Success criterion 2 for MODA

Many factors contribute to changes in data systems and systems availability. For example, it can be need for integration with another system, changes in user requirements or the availability of new technology on the market. This and the fact that threats and vulnerabilities are often situation dependent, force organisations and companies to regular assessment of risks that can affect the availability of a data system. But regular availability risk assessment may very soon "blow up" the financial budget of a software company. Hence we need availability risk assessment methodology that is *cost effective*. One way to achieve this is to extract experiences from using the methodology for reuse in later availability assessments.

Success criterion 3	**MODA should be cost effective from a reusability perspective**

Figure 3.3: Success criterion 3 for MODA

Project managers and risk analysts have many responsibilities and the effectiveness of their work depends very much on the tools that they have available. The availability risk assessment methodology that we are developing must support their work, be fit for its intended use, and be perceived as an added value. *User friendliness* is an often-used term that is important to any user of risk assessment methodology. Project managers and risk analysts should be able to use MODA without difficulties and be assisted by the set of guidelines, templates and checklists.

Success criterion 4	**MODA should be user friendly assisting its users by providing guidelines, templates and checklists**

Figure 3.4: Success criterion 4 for MODA

3.2 Validation of success criteria

Validation of our success criteria will be concerned with showing that the requirements listed in the previous section are fulfilled. That MODA satisfies these success criteria may be viewed as our overall research hypothesis. There are many strategies for the validation of research hypothesis, each one suitable for different research settings. The most common of them are shown in Figure 3.5 and their definitions accordingly to Joseph E. McGrath [26] are given below.

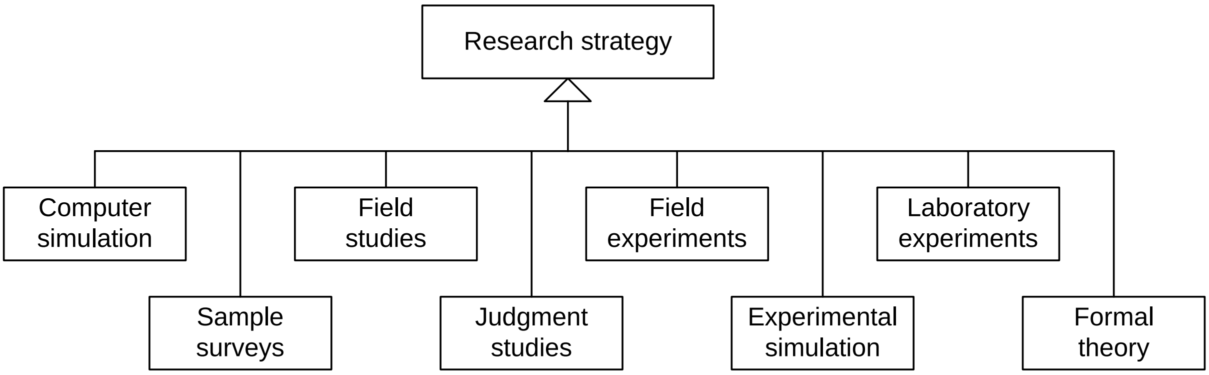


Figure 3.5: Research strategies

Field studies - direct observations of “natural”, ongoing systems, while disturbing and intruding on those systems as little as possible. By *field study* we mean the practical use of availability risk assessment methodology. In our thesis we refer to this interpretation of field study as *Case study*.

Field experiments are field studies with one major intervention and manipulation of some system’s features. An interesting experiment could be to see if a change in a format of tables used in MODA would make a difference for the risk analysts who use the availability risk assessment methodology. We will not conduct a field experiment due to time and resource limitations.

Laboratory experiments are attempts to create the "essence" of some general class of systems in a context in which the researcher can control features of the situation. A possible laboratory experiment could be to test how changes in templates and the order of guidelines used in MODA will affect their understanding by the users of MODA. If there are possibilities for misunderstandings, using the guideline or template could lead to faulty results, and this may be determined. Because of the time and resource limitations we will not conduct a laboratory experiment in our thesis.

Experimental simulations are laboratory studies in which an effort is made to create a system that is like some class of naturally occurring systems, but is artificial in that it is created by the researchers for study, and people perform in it for research purposes rather than for purposes stemming from their own live. An experimental simulation could be used to monitor how participants of the risk assessment employ MODA and understand the risk assessment methods like HazOp or FTA. Again, it will be difficult to make experimental simulations due to time and resource limitations.

Sample surveys are efforts to get information from a broad sample of actors (system developers), usually in the form of verbal responses to a relatively small set of questions. In sample surveys we could ask a broad sample of risk assessment practitioners (20 – 100 people) to assess the methodology accordingly to its requirements. Since this strategy requires a broad sample of actors, we need to postpone a sample survey about MODA until it hopefully gets a larger user-base.

Judgment studies are efforts to get responses from very small and somewhat casually selected sample of "judges". In judgment studies we could ask the rather small group of persons with knowledge about risk assessment to assess our methodology. This is not a trivial task because the available risk assessment practitioners can be busy and the reading of methodology can take time – this can collide with the time constrain of our thesis.

Formal theory denotes set of general theories that are used to support researchers.
Computer simulation refers to attempts to model a specific real life system or class of systems. These two topics will not be investigated further in our thesis.

As explained above we will use Field study (Case study) to argue the fulfilment of the success criteria. We do not consider field experiments, laboratory experiments, experimental simulations, sample surveys, judgment studies, formal theory and computer simulations as appropriate given the scope and resources available for our work.

Figure 3.6 summarises the MODA success criteria and the strategies used for their validation.

Success criterion 1: **MODA should target availability in a security context**
Validation: This will be verified by use of Field Studies (Case Studies). The case studies will show to what extent MODA templates can be used for the identification and treatment of security risks.

Success criterion 2: **MODA should be time efficient**
Validation: This will be verified by use of Field Studies (Case Studies). The case studies will show whether MODA has templates, tables or guidelines required to facilitate quick availability assessment.

Success criterion 3: **MODA should be cost effective from a reusability perspective**
Validation: This will be verified by use of Field Studies (Case Studies). The case studies will show whether MODA has elements that can be reused.

Success criterion 4: **MODA should be user friendly assisting its users by providing guidelines, templates and checklists**
Validation: This will be verified by use of Field Studies (Case Studies). The case studies will show whether MODA has guidelines, templates and checklists that assist users in the availability risk assessment.

Figure 3.6: MODA success criteria and the strategies for their validation

4 Availability decomposed

The availability of information system depends on the correct functioning of every element in the computing infrastructure including the environment in which the system resides. In order to analyse successfully the system availability, we need to know all the key areas of risk to system availability. In this chapter we identify these key areas and define how they can affect system assets.

This chapter is structured into seven sections. Section 4.1 defines four sub classes of availability, the so-called availability aspects, and explains concepts that are relevant for them. Section 4.2 describes hardware components and gives definitions that characterise the difference between internal, external and basic hardware components. Section 4.3 considers the first availability aspect, namely network availability. It starts by defining network components. Further it provides a decomposition of network availability and network components into more basic entities. The relationship of network availability to other availability aspects is considered in sub-section 4.3.1. Assets that can be affected by the reduction of network availability are considered in sub-section 4.3.2. Section 4.4 considers the second availability aspect, namely software availability. The relationship of software availability to other availability aspects is considered in sub-section 4.4.1. How reduction of software availability affects assets is considered in sub-section 4.4.2. Section 4.5 describes human availability – the third availability aspect. Sub-section 4.5.1 describes relationship of human availability to other availability aspects. Assets, which can be affected by the reduction of human availability, are described in sub-section 4.5.2. Section 4.6 considers the last availability aspect known as hardware availability. The relationship of hardware availability to other availability aspects is considered in sub-section 4.6.1. Sub-section 4.6.2 describes assets that can be affected by the reduction of hardware availability. Based on the information provided in sections 4.1 – 4.6, section 4.7 presents templates for availability analysis.

4.1 Availability aspects

An effective function of a data system depends very much on the effective function of data system components that in turn depend on the effective functioning of software, hardware and the network of links that connects these system components.

If the *network* is congested, it cannot deliver packets to the destination host. If you have an unstable operating system (*software*), probably you can have difficulties in use of application programs that support your work. If the internal modem (*internal hardware*) in your computer does not function, you cannot receive or send email, or be available for a teleconference with your colleagues. If your printer or scanner (*external hardware*) does not function, you cannot print or scan documents. The *human* factor is also very important to the availability of data systems. People configure networks, install new computers, update software and hardware. If network or system administrator makes a mistake during router or server configuration, this fail can cause a collapse of the whole network.

In order to have a possibility to do the risk assessment on the very detailed level and at the same time make it easy and effective, we consider availability as a super class that is decomposed in the following four sub classes (availability aspects):

- Network availability
- Software availability
- Human availability
- Hardware availability

We define these four sub classes of system availability as follows:

Network availability is the property of network to be accessible and usable upon demand by an authorized entity.
Software availability is the property of software to be accessible and usable upon demand by an authorized entity.
Human availability is the property of human to be accessible and usable upon demand by an authorized entity.
Hardware availability is the property of hardware to be accessible and usable upon demand by an authorized entity.

These categories are different in a sense that they can affect different assets and each of them may need the use of different assessment methods. To successfully assess the availability of information systems, we have to clarify the following issues:

- Dependencies between availabilities. To what extend do one kind of availability depend on other kinds of availability?
- What assets can be affected by the reduction of each availability?

Figure 4.1 specifies the decomposition of availability into availability aspects.

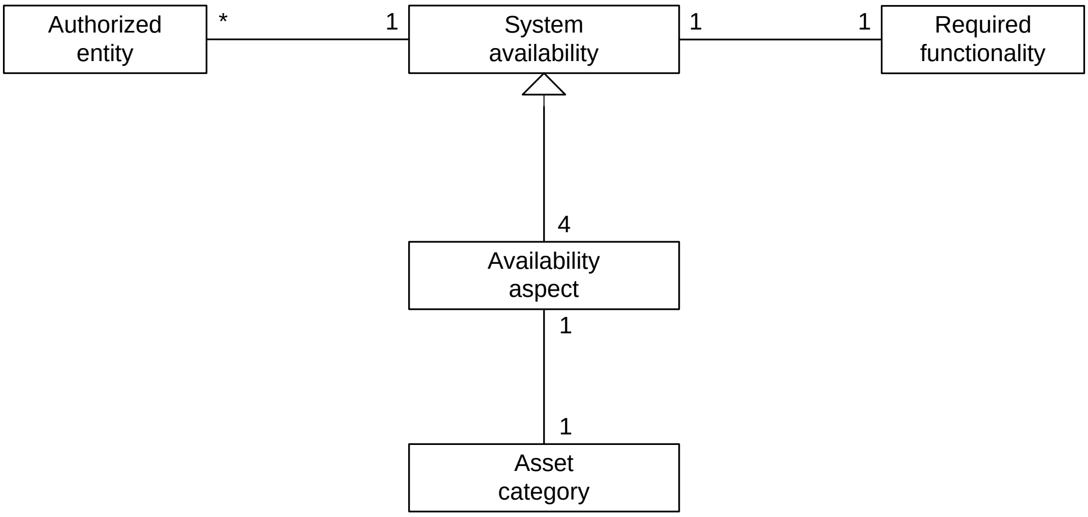


Figure 4.1: Decomposition of system availability

The concepts of Figure 4.1 can be given the following definitions:

- **System availability** is the property of system to be accessible and usable upon demand by an authorized entity.
- **Availability aspect** is a sub-class of system availability (we define four availability aspects: network, software, hardware, and human availability).
- **Authorized entity** is a system component and/or user that is authorised to access/use the service provided by the system.
- **Asset category** is a categorisation of similar assets. We categorise assets in the following categories: software assets, physical assets, information assets, human assets, organisational assets, law and regulation assets [5].
- **Required functionality** is what the system (component) is intended for, and is described by the system (component) specification.

We can see from Figure 4.1 that system availability is decomposed into 4 availability aspects. Each availability aspect is related to one corresponding asset category (e.g. Human availability has one corresponding asset category – Human assets). Each system (component) has required functionality and can be accessed/used by more than one authorised entity.

4.2 System hardware components

Computer systems can have many different hardware components and very often people use different words to describe the same hardware elements. For example, Irv Englander [27] in his book “The Architecture of Computer Hardware and Systems Software” describes display and printer as “*hardware components*” while Webopedia [28] - Internet online encyclopaedia dedicated to computer technology, describes printer and monitor as “*external peripheral devices* ” that are in contrast to “*internal devices*” such as a CD-ROM drive or an internal Zip drive. However, the same Webopedia uses printers, screens and disc drives as examples of hardware and defines hardware as: ”objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips”. All these different definitions of the same hardware components can be quite confusing. That’s why it is important to know what kind of hardware components we can have in the assessed system.

As we will see in the next section, system components communicate and coordinate their actions through the network. Networks of computers are constructed from links and two types of nodes: host nodes (connect users/servers to the network) and network nodes (forward messages from one link to another). Both host and network nodes may contain hardware components that are housed within them or attached to them externally. The following definitions characterise this difference more clearly:

- **External hardware -** any machine or component that is directly connected to the host/network node (e.g. keyboard, mouse, printer, scanner, web camera, monitor, external modem, external CD burner, external network interface card).
- **Internal hardware** - physical object that is housed within the main container of the host/network node (e.g. memory, processor, graphic card, sound card, network interface card, hard disc, CD-ROM drive, internal Zip- drive).
- **Basic hardware component** - physical object that is housed within the main container of the external/internal hardware (e.g. external hardware – monitor, contains basic hardware components such as chip, circuit, power supply).

The components related to the system hardware are shown in Figure 4.2.

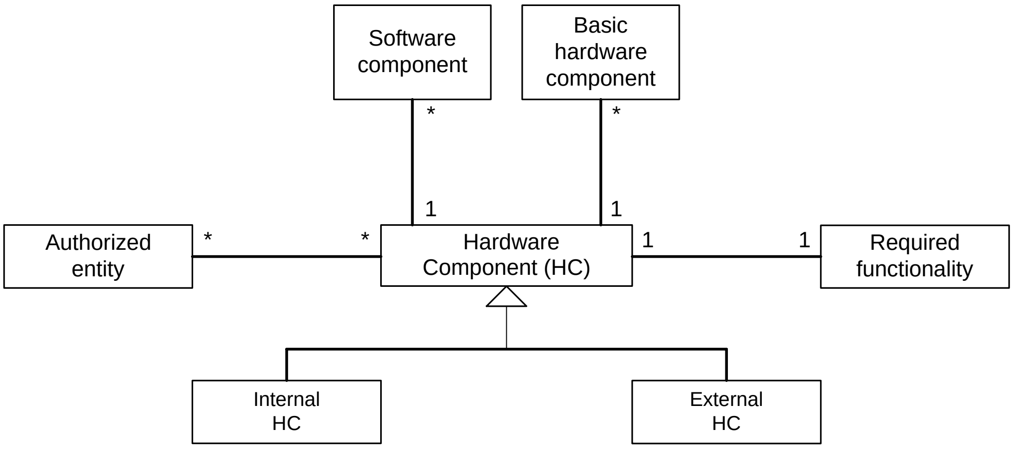


Figure 4.2: System hardware components

Figure 4.2 shows that a hardware component can be either internal or external and may contain more than one basic hardware component. Both internal and external hardware components may require more than one software component that converts general commands from an application into specific commands that the hardware component understands.

4.3 Network availability

The network availability is the main concern when we analyse telecommunication systems. It is concerned with the exchange of information between components and between components and the system's environment. That's why it is important to figure out what building blocks constitute the network. Computer networks must provide robust and effective connectivity among a large number of computers, and are constructed from two classes of hardware building blocks: nodes and links.

We divide nodes in two categories: the host nodes that connect users or servers to the network and the network nodes that are responsible for forwarding of messages from one link to another. The host nodes can be dedicated servers (e.g. database server), general-purpose computers like desktop workstations or PDA's that users use to run application programs on. The network nodes can be implemented on general-purpose devices (general-purpose computers) or by special-purpose devices (e.g. switch, router).
Network links are the links that connect network nodes to each other. They can be implemented on different physical media like coaxial cable, optical fiber or space (the radio waves propagate through space).

When we analyse availability of information systems, we have to keep in mind the fact, that networks may not remain fixed and may evolve to accommodate changes to both the underlying technologies as well as changes in application programs demands. Some nodes of the network can be connected by radio links while others can be connected by a cable.

To analyse network availability, we analyse the availability of components that contribute to the network connectivity: network nodes and links. Nodes and links can in turn be analysed by analysing components and factors that contribute to their functionality: software, hardware and people. Decomposition of the network availability is shown in Figure 4.3.

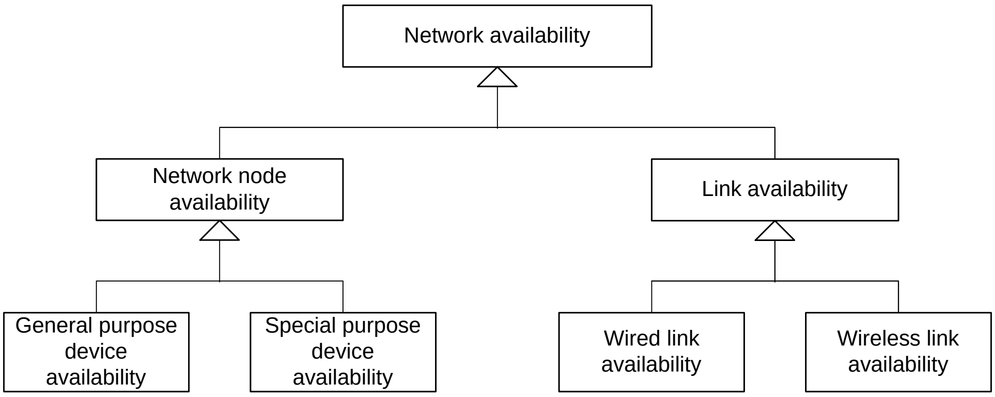

Network availability
Network node availability
Link availability
General purpose device availability
Special purpose device availability
Wired link availability
Wireless link availability

Figure 4.3: Decomposition of the network availability

Figure 4.4 shows that a network can consist of two or more nodes connected by one or more links. Each node in the network is either host node or network node and each link is either wired link or wireless link.

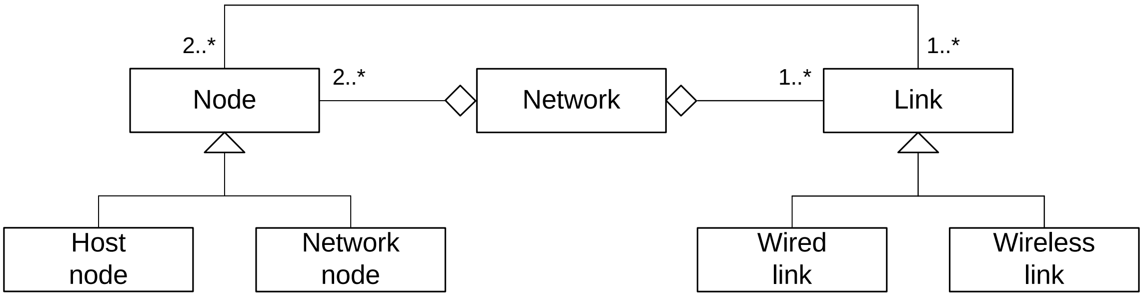


Figure 4.4: Network components

4.3.1 Relationship to other availability aspects

As we said, network availability depends on the availability of the network building blocks: nodes and links that in turn have components and factors that contribute to their fail free function: software, hardware and people. First we will describe the components supporting functionality of host and network nodes, and then we will define the relationship of network availability to other availability aspects.

Figure 4.5 shows decomposition of a host node and its relation to other elements in the system. Each host node can be accessed/used by more than one authorized entity, while one authorized entity can access/use more than one host node. The required functionality of host node can be supported by more than one internal or external hardware component as well as by more than one software component that is either system software component (e.g. operating system) or application software (e.g. Microsoft Word).

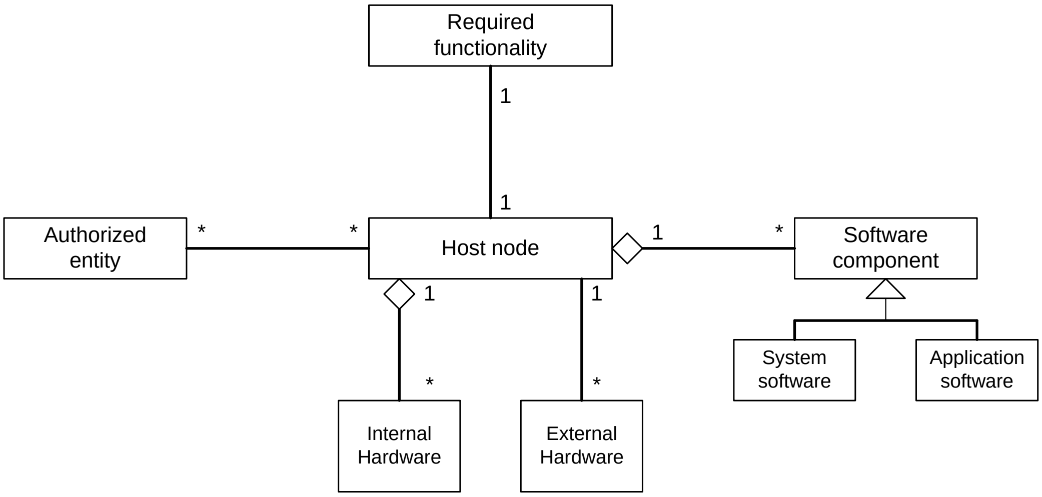


Figure 4.5: Decomposition of host node

Figure 4.6 shows decomposition of a network node and its relation to other elements in the system. As we said, each network node can be implemented on a general-purpose device or on a special-purpose device. If a network node is implemented on a general-purpose device, its required functionality can be supported by the same set of hardware and software components that can support the functionality of a host node. If a network node is implemented on a special-purpose device, its required functionality can be supported by several internal hardware components (e.g. network adaptor) and software components (e.g. software that supports update of routing table).

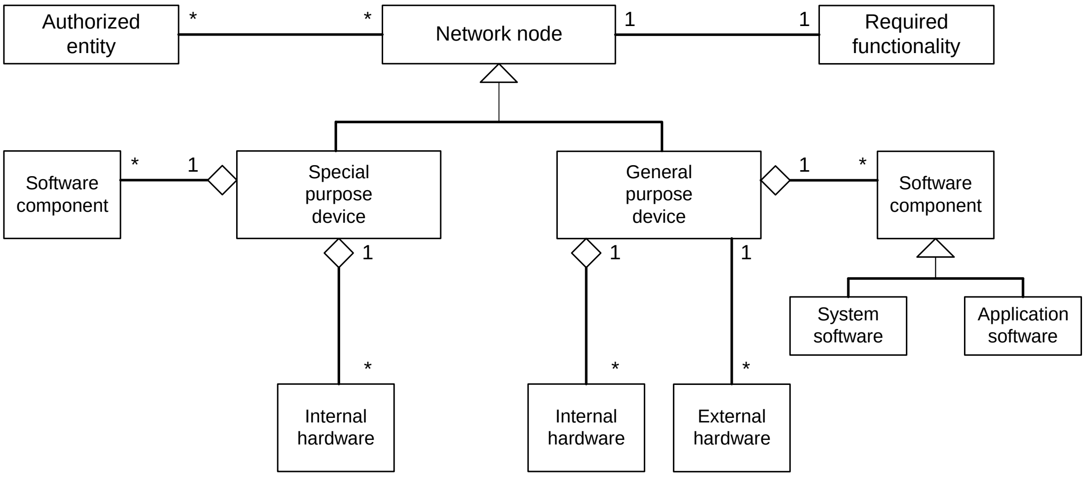


Figure 4.6: Decomposition of network node

As we can see from Figures 4.5 and 4.6, both host and network nodes depend on effective functioning of hardware and software components as well as proper behavior of authorized entities that can be either authorized users or other system components. Along with hardware and software components, authorized users may directly affect network availability – people can update, configure, install or maintain network links as well as network nodes hardware and software components. Figure 4.7 shows decomposition of dependability of network availability.

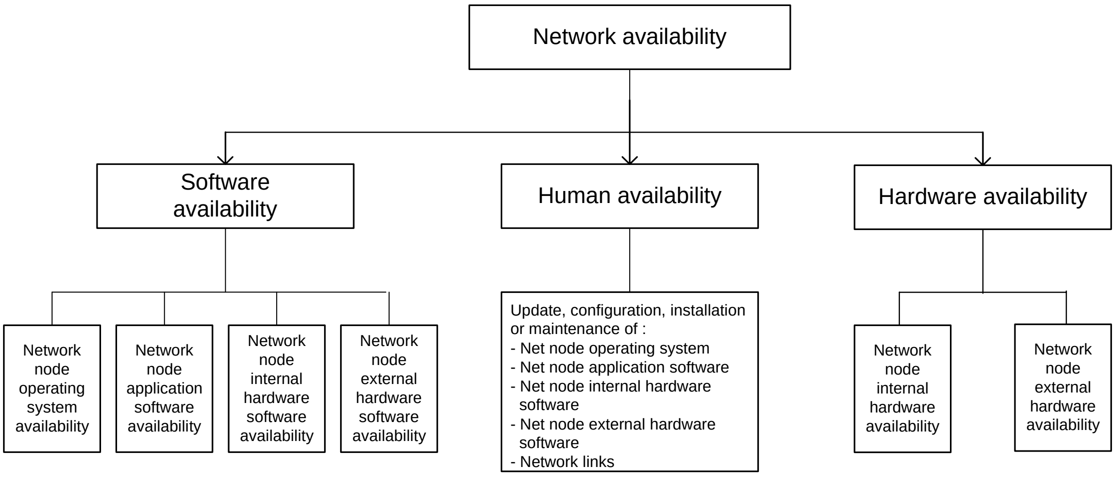

Network availability
Software availability
Human availability
Hardware availability
Network node operating system availability
Network node application software availability
Network node internal hardware software availability
Network node external hardware software availability
Update, configuration, installation or maintenance of :
- Net node operating system
- Net node application software
- Net node internal hardware software
- Net node external hardware software
- Network links
Network node internal hardware availability
Network node external hardware availability

Figure 4.7: Decomposition of dependability of network availability

Network availability depends on:

***Software availability*:**

Network node operating system availability
- if the functionality of a network node is supported by an operating system.

Network node application software availability
- if the functionality of a network node is supported by application software.

Network node internal hardware software availability
- if the functionality of a network node internal hardware depends on software.

Network node external hardware availability
- if the functionality of a network node external hardware depends on software.

***Hardware availability*:**

Network node internal hardware availability
- if the functionality of a network node is supported by a internal hardware.

Network node external hardware availability
- if the functionality of a network node is supported by a external hardware.

***Human availability*:**
- if authorized personnel update, configure or install an operating system supporting the functionality of a network node.
- if authorized personnel update, configure or install application software supporting the functionality of a network node.

- if authorized personnel update, configure or install software supporting the functionality of a network node internal hardware.
- if authorized personnel update, configure or install software supporting the functionality of a network node external hardware.
- if authorized personnel install or maintain network links.

4.3.2 How reduction of network availability affects assets

Reduction of network availability may affect assets in the following sense:

- Human assets
  - *human asset* A: if A delivers a service through the network to the service's consumers (e.g. in the telemedicine service, because of a network problem a specialist is unable to give a consultation to a doctor or patient).
  - *human asset* A: if A receives a service through the network from the service provider (e.g. a stock broker cannot make a deal without network access to online stock information).
- Information assets
  - *information asset* A: if A is transmitted or accessed through the network (e.g. network problems can cause the loss of A or difficulty in delivery or update of A).
- Software assets
  - *software asset* A: if A is transmitted or accessed through the network (e.g. network problems can cause the loss of A or difficulty in delivery or update of A).
- Physical assets
  - *physical asset* A: if A is responsible for execution of service that is accessible by other system components through the network (e.g. surveillance video camera or printer that are accessible through the network).
- Organisational assets
  - *organisational asset* A: if A can be directly affected by the change of network availability.
- Low and regulation assets
  - *low and regulation asset* A: if A is accessed through the network.

4.4 Software availability

The effective functioning of software installed in system components is one of the main conditions for effective work of the system. Both internal and external hardware can be supplied with its own coordinated software to help make the computer more accessible and productive to the user. Application software supports our work in different ways. For example, you can use application software to write and translate documents, listen music or browse web pages. The operating system has other purposes: it controls and operates hardware and provides the user and application programs a variety of facilities and services. Software availability can be decomposed into the availability of host node software and network node software. Both host node and network node software availability can be further decomposed into operating system availability, application software availability, internal hardware software availability, and external hardware software availability. Decomposition of the software availability is shown in Figure 4.8.

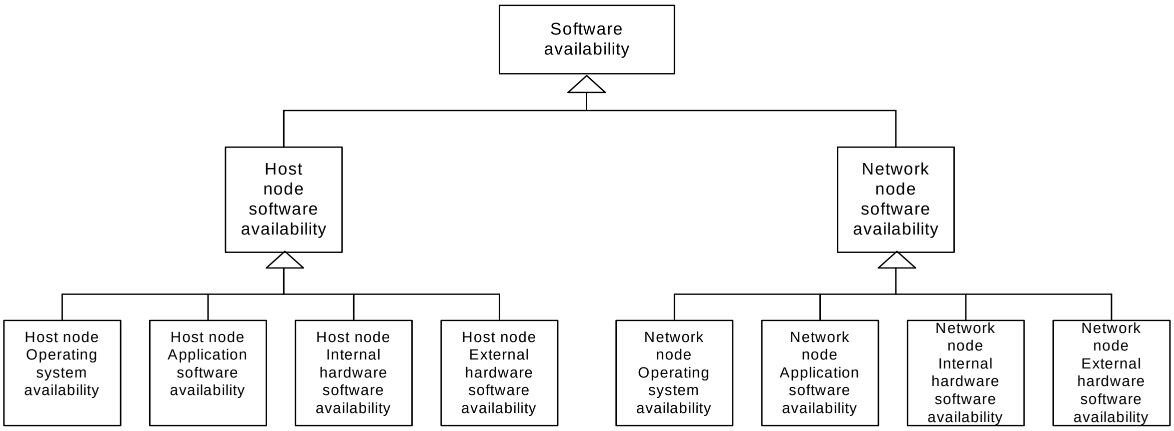

Software availability
Host node software availability
Network node software availability
Host node Operating system availability
Host node Application software availability
Host node Internal hardware software availability
Host node External hardware software availability
Network node Operating system availability
Network node Application software availability
Network node Internal hardware software availability
Network node External hardware software availability

Figure 4.8: Decomposition of the software availability

4.4.1 Relationship to other availability aspects

The system administrator has to update software in time and install new software components correctly. The operating system installed on a hard disc cannot function if the hard disc does not function. The software that supports the functionality of internal and external hardware components depends on proper behaviour of the operating system and hard disc. In this section we describe the relationship of software availability to other availability aspects. The section is divided into two sub-sections. In sub-section 4.4.1.1 we consider software of host node and software of network node implemented on a general-purpose device. In sub-section 4.4.1.2 we consider software of network node implemented on a special purpose device.

4.4.1.1 Relationship of host/network node software availability

The availability of host/network node software can be decomposed into the availability of node application software, availability of node operating system and availability of software that supports functionality of host/network node internal and external hardware.
Figure 4.9 shows decomposition of host/network node software availability and dependability of software components on other availability aspects.

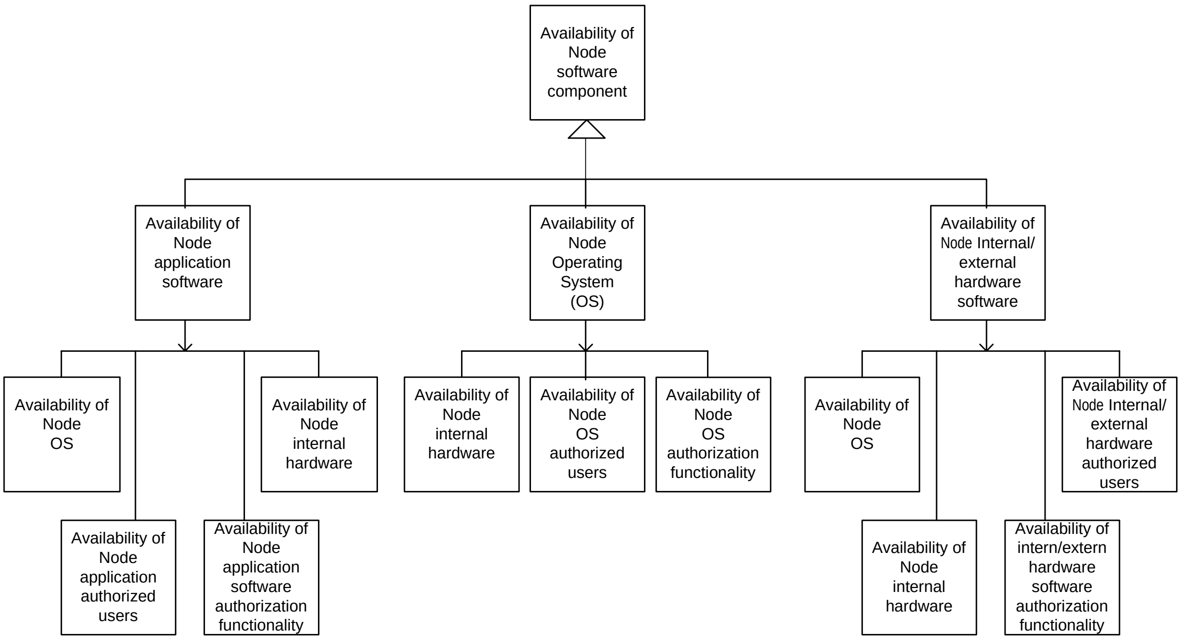

Availability of Node software component
Availability of Node application software
Availability of Node Operating System (OS)
Availability of Node Internal/ external hardware software
Availability of Node OS
Availability of Node internal hardware
Availability of Node application authorized users
Availability of Node application software authorization functionality
Availability of Node internal hardware
Availability of Node OS authorized users
Availability of Node OS authorization functionality
Availability of Node OS
Availability of Node Internal/ external hardware authorized users
Availability of Node internal hardware
Availability of intern/extern hardware software authorization functionality

Figure 4.9: Decomposition of dependability of host/network node software availability

Host/Network node operating system depends on:

- Node internal hardware availability (e.g. hard disc, disc drive, power supply).
- Availability of authorized users of node OS (e.g. correct installation, update, use).
- Availability of node OS authorization functionality.

Host/Network node application software depends on:

- Node operating system availability.
- Node internal hardware availability.
- Availability of authorized users of node application software.
- Availability of node application software authorization functionality.

Host/Network node internal/external hardware software depends on:

- Node operating system availability.
- Node internal hardware availability.
- Availability of authorized users of node internal/external hardware.
- Availability of node internal/external hardware software authorization functionality.

4.4.1.2 Relationship of network node software availability

Recall that if a network node is implemented on a special-purpose device, its required functionality can be supported by several internal hardware components and software components. These software and hardware components in turn can be installed, configured or updated by authorized personnel. Figure 4.10 shows dependability of network node software on other availability aspects.

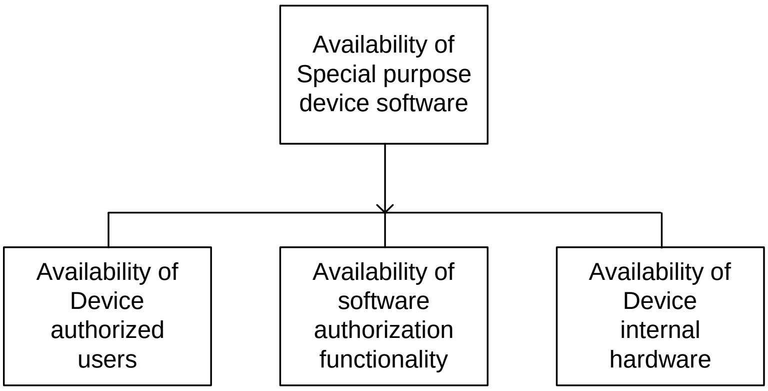

Availability of Special purpose device software
Availability of Device authorized users
Availability of software authorization functionality
Availability of Device internal hardware

Figure 4.10: Dependability of network node (special purpose device) software

The information depicted in Figure 4.10 can be interpreted in the following sense:

If the functionality of special purpose device depends on software (e.g. device can be programmable), availability of device software depends on:

- Availability of device authorized users (correct use, installation, update or configuration of device software).
- Availability of device software authorization functionality (device software needs a protection against unauthorized access).
- Availability of device internal hardware (device software may access device memory).

4.4.2 How reduction of software availability affects assets

This section is divided into two sub-sections. In sub-section 4.4.2.1 we consider software of host node and software of network node implemented on a general-purpose device. In sub-section 4.4.2.2 we consider software of network node implemented on a special purpose device.

4.4.2.1 Reduction of host/network node software availability

Reduction of host/network node software availability can be analysed by analysing reduction of node operating system availability, reduction of node application software availability and reduction of node internal/external hardware software availability.

Reduction of host/network node operating system availability

Reduction of host/network node operating system availability may affect assets in the following sense:

- Human assets
  - *human asset* A: if host/network node operating system runs application programs that support A in the execution of A's tasks.

  - *human asset* A: if A can be directly affected by the change of functionality of application software running under host/network node OS (e.g. application program that monitors patient's health during operation).
  - *human asset* A: if the reputation of A or relationship of A with other people can be affected by the change of functionality of application software running under host/network node OS.
- Information assets
  - *information asset* A: if host/network node operating system runs application programs that store, process or transmit A in the system.
- Software assets
  - *software asset* A: if host/network node operating system runs application programs that store, process or transmit A in the system.
- Physical assets
  - *physical asset* A: if host/network node operating system runs application programs that control the function of A.
- Organisational assets
  - *organisational asset* A: if A can be directly affected by the change of functionality of host/network node operating system.
- Low and regulation assets
  - *low and regulation asset* A: if host/network node operating system runs application programs that control the access to A.

Reduction of host/network node application software availability

Reduction of host/network node application software availability may affect assets in the following sense:

- Human assets
  - *human asset* A: if host/network node application software supports A in the execution of A's tasks.
  - *human asset* A: if A can be directly affected by the change of functionality of host/network node application software.
  - *human asset* A: if the reputation of A or relationship of A with other people can be affected by the change of functionality of host/network node application software.
- Information assets
  - *information asset* A: if host/network node application software is used for storing, processing or transmission of A in the system.
- Software assets
  - *software asset* A: if host/network node application software is used for storing, processing or transmission of A in the system.
- Physical assets
  - *physical asset* A: if host/network node application software is used to control the function of A.
- Organisational assets
  - *organisational asset* A: if A can be directly affected by the change of functionality of host/network node application software.
- Low and regulation assets

  - *low and regulation asset* A: if host/network node application software controls the access to A.

Reduction of host/network node internal/external hardware software availability

If the functionality of host/network node internal/external hardware depends on software, the reduction of host/network node internal/external hardware software availability may affect assets in the following sense:

- Human assets
  - *human asset* A: if host/network node internal/external hardware supports A in the execution of A’s tasks.
  - *human asset* A: if A can be directly affected by the change of functionality of host/network node internal/external hardware.
  - *human asset* A: if the reputation of A or relationship of A with other people can be affected by the change of functionality of host/network node internal/external hardware.
- Information assets
  - *information asset* A: if host/network node internal/external hardware is used for storing, processing or transmission of A in the system.
- Software assets
  - *software asset* A: if host/network node internal/external hardware is used for storing, processing or transmission of A in the system.
- Physical assets
  - *physical asset* A: if A is unusable without host/network node internal/external hardware software that supports functionality of A (e.g. physical asset - CD-burner is unusable without software that supports its functionality).
- Organisational assets
  - *organisational asset* A: if A can be directly affected by the change of functionality of host/network node internal/external hardware.
- Low and regulation assets
  - *low and regulation asset* A: if host/network node internal/external hardware controls the access to A.

4.4.2.2 Reduction of network node software availability

Reduction of Network node software availability may affect assets in the following sense:

- Human assets
  - *human asset* A: if Network node software supports A in the execution of A’s tasks.
  - *human asset* A: if A can be directly affected by the change of functionality of Network node software.
  - *human asset* A: if the reputation of A or relationship of A with other people can be affected by the change of functionality of Network node software.
- Information assets
  - *information asset* A: if Network node software stores, processes or transmits A in the system.

- Software assets
  - *software asset* A: if Network node software stores, processes or transmits A in the system.
- Physical assets
  - *physical asset* A: if A is unusable without Network node software that supports the functionality of A (e.g. there are some routers – physical assets, that are unusable without software that supports their functionality).
- Organisational assets
  - *organisational asset* A: if A can be directly affected by the change of functionality of Network node software.
- Low and regulation assets
  - *low and regulation asset* A: if Network node software controls the access to A.

4.5 Human availability

Employees and users interact with the system and it is very important to know how this interaction is executed and what consequences for people and the system change in this interaction may have. Human errors, negligence and greed may be responsible for many thefts, frauds or misuse of facilities. For example at nuclear power plant, one mistake in the work routines may lead to the health damage of personnel, while a mistake in the work routines in a hospital can lead to the damage of patient's health.

We categorize human services in three categories:

- people who use a data system to perform services (e.g. booking personnel, medical personnel). We refer to this category of human services as *human service providers*.
- people who update, configure or install system or system infrastructure (e.g. system developers, system/network administrators). We refer to this category of human services as *system personnel*.
- people who give technical or information support for system or system infrastructure (e.g. software troubleshooting service or reparation of scanners, printers). We refer to this category of human services as *system technicians*.

Figure 4.11 shows the decomposition of human availability.

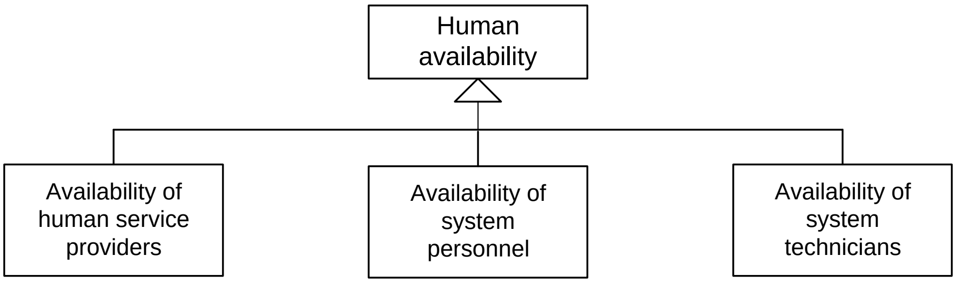

Human availability
Availability of human service providers
Availability of system personnel
Availability of system technicians

Figure 4.11: Decomposition of human availability

4.5.1 Relationship to other availability aspects

Human service providers may deliver a service through the network to the service consumers (e.g. medical personnel may give online consultation service). System personnel may update or configure software components through the network or use software and hardware components to accomplish their tasks. System technicians may depend on the proper functionality of software and hardware components that support them in service execution. In this section we describe the relationship of each category of human services to other availability aspects. The section is divided into three sub-sections. In sub-section 4.5.1.1 we consider human service providers. Sub-section 4.5.1.2 describes system personnel. In sub-section 4.5.1.3 we consider system technicians.

4.5.1.1 Relationship of human service providers availability

Availability of human service providers depends on:

***Network availability*:**

- if human service providers deliver service through the network to the service consumers.
- if the human service providers provision of service depends on the network availability.
- if the functionality of software components used by human service providers to perform service, depends on the network availability (e.g. You can not use Outlook to send email if your computer is connected to the network that can not deliver packets to the destination host).
- if the functionality of hardware components used by human service providers to perform service, depends on the network availability.

***Software availability*:**

Host/Network node operating system availability

- if host/network node operating system runs application programs that support human service providers in the execution of service.

Host/Network node application software availability

- if host/network node application software supports human service providers in the execution of service.

Host/Network node internal hardware software availability

- if host/network node internal hardware supports human service providers in the execution of service.

Host/Network node external hardware software availability

- if host/network node external hardware supports human service providers in the execution of service.

***Hardware availability*:**

Host/Network node internal hardware availability

- if host/network node internal hardware supports human service providers in the execution of service.

Host/Network node external hardware availability

- if host/network node external hardware supports human service providers in the execution of service.

4.5.1.2 Relationship of system personnel availability

Availability of system personnel depends on:

***Network availability*:**

- if system personnel deliver service through the network to the service consumers.
- if the system personnel provision of service depends on the network availability.
- if the functionality of software components used by system personnel to perform service, depends on the network availability.
- if the functionality of hardware components used by system personnel to perform service, depends on the network availability.

***Software availability*:**

Host/Network node operating system availability

- if host/network node operating system runs application programs that support system personnel in the execution of service.

Host/Network node application software availability

- if host/network node application software supports system personnel in the execution of service.

Host/Network node internal hardware software availability

- if host/network node internal hardware supports system personnel in the execution of service.

Host/Network node external hardware software availability

- if host/network node external hardware supports system personnel in the execution of service.

***Hardware availability*:**

Host/Network node internal hardware availability

- if host/network node internal hardware supports system personnel in the execution of service.

Host/Network node external hardware availability

- if host/network node external hardware supports system personnel in the execution of service.

4.5.1.3 Relationship of system technicians availability

Availability of system technicians depends on:

***Network availability*:**

- if system technicians deliver service through the network to the service consumers.
- if the system technicians provision of service depends on the network availability.
- if the functionality of software components used by system technicians to perform service, depends on the network availability.

- if the functionality of hardware components used by system technicians to perform service, depends on the network availability.

***Software availability*:**

Host/Network node operating system availability

- if host/network node operating system runs application programs that support system technicians in the execution of service.

Host/Network node application software availability

- if host/network node application software supports system technicians in the execution of service.

Host/Network node internal hardware software availability

- if host/network node internal hardware supports system technicians in the execution of service.

Host/Network node external hardware software availability

- if host/network node external hardware supports system technicians in the execution of service.

***Hardware availability*:**

Host/Network node internal hardware availability

- if host/network node internal hardware supports system technicians in the execution of service.

Host/Network node external hardware availability

- if host/network node external hardware supports system technicians in the execution of service.

Figure 4.12 summarizes the dependability of human availability on other availability aspects.

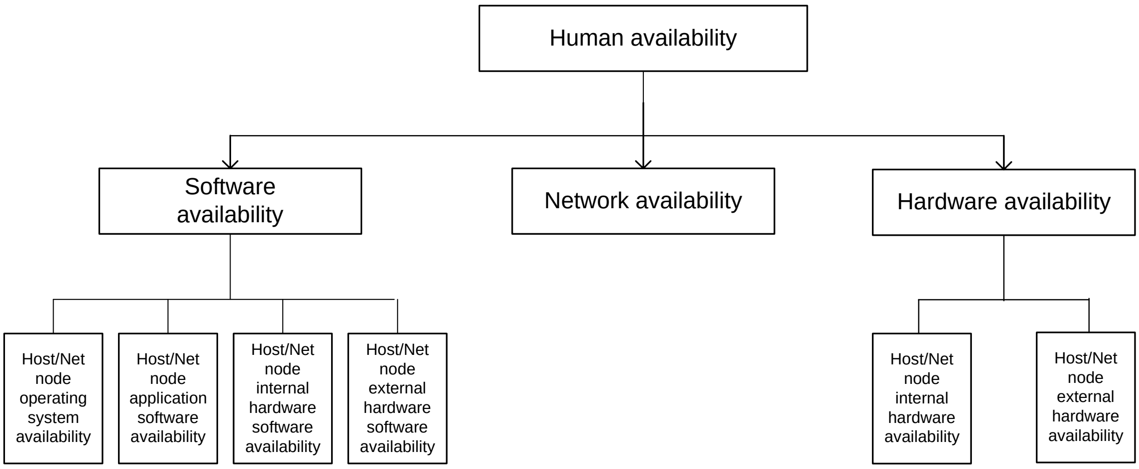

Human availability
Software availability
Network availability
Hardware availability
Host/Net node operating system availability
Host/Net node application software availability
Host/Net node internal hardware software availability
Host/Net node external hardware software availability
Host/Net node internal hardware availability
Host/Net node external hardware availability

Figure 4.12: Decomposition of dependability of human availability

4.5.2 How reduction of human availability affects assets

This section is divided into three sub-sections. In sub-section 4.5.2.1 we consider human service providers. Sub-section 4.5.2.2 describes system personnel. In sub-section 4.5.2.3 we consider system technicians.

4.5.2.1 Reduction of human service providers availability

Reduction of human service providers availability may affect assets in the following sense:

- Human assets
  - *human asset* A: if A uses the service provided by human service providers.
  - *human asset* A: if actions taken by human service providers affect A's health or ability of A to perform its duties.
- Information assets
  - *information asset* A: if actions taken by human service providers affect storing, processing or transmission of A in the system.
- Software assets
  - *software asset* A: if actions taken by human service providers affect storing, processing, transmission or function of A in the system.
- Physical assets
  - *physical asset* A: if human service providers control the function of A. (e.g. fail in work routines in an air traffic control can lead to the loss of plane – physical asset and people's lives – human assets).
  - *physical asset* A: if actions taken by human service providers affect the functionality of A.
- Organisational assets
  - *organisational asset* A: if A can be directly affected by the change of availability of service provided by human service providers.
- Low and regulation assets
  - *low and regulation asset* A: if human service providers provide the access to A.

4.5.2.2 Reduction of system personnel availability

Reduction of system personnel availability may affect assets in the following sense:

- Human assets
  - *human asset* A: if A uses the service provided by system personnel.
  - *human asset* A: if actions taken by system personnel affect A's health or ability of A to perform its duties.
- Information assets
  - *information asset* A: if actions taken by system personnel affect storing, processing or transmission of A in the system.
- Software assets
  - *software asset* A: if actions taken by system personnel affect storing, processing, transmission or function of A in the system.
- Physical assets

  - *physical asset* A: if system personnel control the function of A.
  - *physical asset* A: if actions taken by system personnel affect A's functionality.
- Organisational assets
  - *organisational asset* A: if A can be directly affected by the change of availability of service provided by system personnel.
- Low and regulation assets
  - *low and regulation asset* A: if system personnel provide the access to A.

4.5.2.3 Reduction of system technicians availability

Reduction of system technicians availability may affect assets in the following sense:

- Human assets
  - *human asset* A: if A uses the service provided by system technicians.
  - *human asset* A: if actions taken by system technicians affect A's health or ability of A to perform he/her duties.
- Information assets
  - *information asset* A: if actions taken by system technicians affect storing, processing or transmission of A in the system.
- Software assets
  - *software asset* A: if actions taken by system technicians affect storing, processing, transmission or function of A in the system.
- Physical assets
  - *physical asset* A: if system technicians control the function of A.
  - *physical asset* A: if actions taken by system technicians affect A's functionality.
- Organisational assets
  - *organisational asset* A: if A can be directly affected by the change of availability of service provided by system technicians.
- Low and regulation assets
  - *low and regulation asset* A: if system technicians provide the access to A.

4.6 Hardware availability

The effective functioning of hardware components installed in the data system is also one of the conditions for effective work of the system. Hardware components constitute the most visible part of the computer system and provide "the physical mechanisms to input and output data, for manipulating data, and for electronically controlling the various input, output, and storage components" [27]. As we defined, both host and network nodes may contain components that are housed within them or attached to them externally. Hardware availability can be decomposed into the availability of host node hardware and network node hardware. Both host node and network node hardware availability can be further decomposed into host node internal and external hardware availability and network node internal and external hardware availability. Decomposition of hardware availability is shown in Figure 4.13.

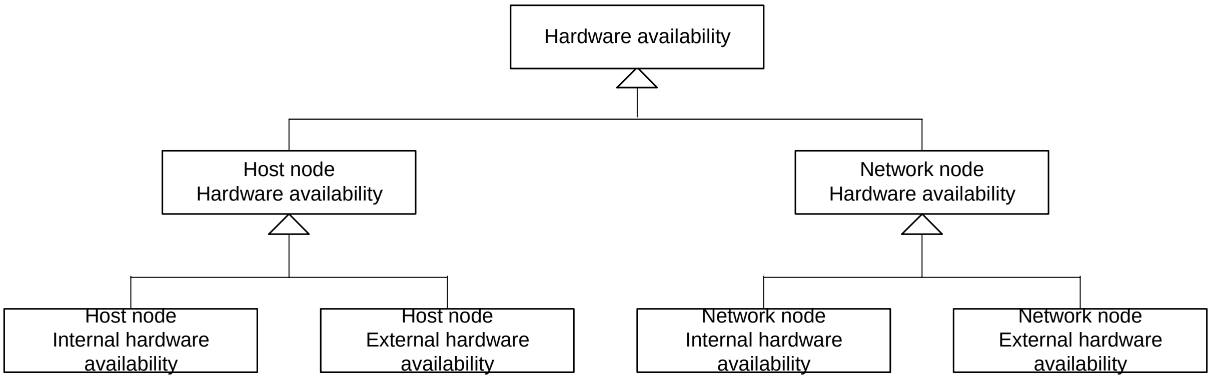

Hardware availability
Host node Hardware availability
Network node Hardware availability
Host node Internal hardware availability
Host node External hardware availability
Network node Internal hardware availability
Network node External hardware availability

Figure 4.13: Decomposition of hardware availability

4.6.1 Relationship to other availability aspects

The availability of system hardware can be considered from the two perspectives: availability of internal hardware and availability of external hardware. Both internal and external hardware components have components and factors that contribute to their effective functioning. The functionality of hardware components may depend on the software that converts commands from applications and makes them understandable for the hardware. Host external/internal hardware also depends on the functionality of basic hardware components that is housed within the main container of external/internal hardware. Availability of some hardware components may also depend on the availability of other hardware components (e.g. availability of monitor depends on the availability of graphic card). People can be responsible for use, update and maintenance of internal and external hardware components. In this section we describe the relationship of hardware availability to other availability aspects. The section is divided into two sub-sections. In sub-section 4.6.1.1 we consider host/network node internal hardware. In sub-section 4.6.1.2 we consider host/network node external hardware and summarize the dependability of host/network node external/internal hardware on other availability aspects.

4.6.1.1 Relationship of host/network node internal hardware availability

Host/Network node internal hardware depends on:

- Host/Network node internal hardware software availability, if functionality of host/network node internal hardware depends on software (e.g. functionality of power supply does not depend on software, but scanner and printer require software that supports their functionality).
- Availability of authorized users of host/network node internal hardware.
- Availability of basic hardware components of host/network node internal hardware.
- Availability of other host/network node hardware components, if these components support functionality of host/network node internal hardware.

4.6.1.2 Relationship of host/network node external hardware availability

Host/Network node external hardware depends on:

- Host/Network node external hardware software availability, if functionality of host/network node external hardware depends on software.
- Availability of authorized users of host/network node external hardware.
- Availability of basic hardware components of host/network node external hardware.
- Availability of other host/network node hardware components, if these components support functionality of host/network node external hardware.

Both external and internal hardware also depend on the availability of hardware authorization functionality – how well the hardware is secured against possible threats to be stolen or accessed by a not authorized person. Figure 4.14 below summarizes the dependability of host/network node external/internal hardware on other availability aspects.

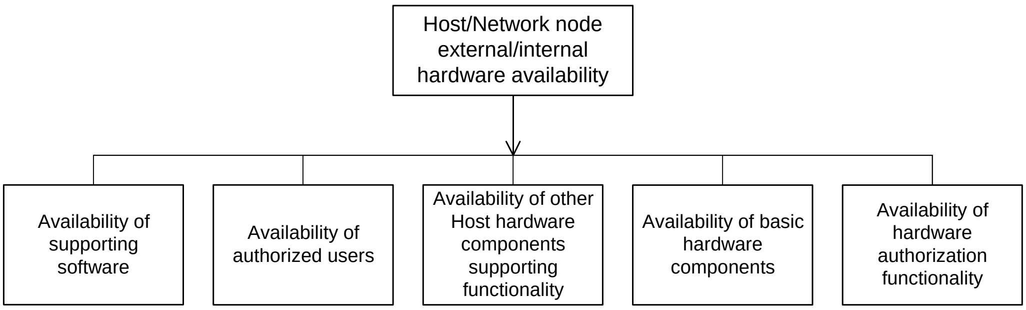

Host/Network node external/internal hardware availability
Availability of supporting software
Availability of authorized users
Availability of other Host hardware components supporting functionality
Availability of basic hardware components
Availability of hardware authorization functionality

Figure 4.14: Decomposition of hardware dependability

4.6.2 How reduction of hardware availability affects assets

This section is divided into two sub-sections. In sub-section 4.6.2.1 we consider host/network node internal hardware. In sub-section 4.6.2.2 we consider host/network node external hardware.

4.6.2.1 Reduction of host/network node internal hardware availability

Reduction of host/network node internal hardware availability may affect assets in the following sense:

- Human assets
  - *human asset* A: if internal hardware supports A in the execution of A’s tasks (e.g. internal modem connects user to the Internet).
- Information assets
  - *information asset* A: if internal hardware is used for storing, processing or transmission of A in the system (e.g. important information is often stored in files on a hard disc).
- Software assets
  - *software asset* A: if internal hardware is used for storing, processing or transmission of A in the system.
- Physical assets

  - *physical asset* A: if internal hardware supports the function of A (e.g. the internal modem can get functionality problems if the cable connecting it to other internal hardware components is broken).
- Organisational assets
  - *organisational asset* A: if A can be directly affected by the change of functionality of host/network node internal hardware.
- Low and regulation assets
  - *low and regulation asset* A: if host/network node internal hardware controls the access to A.

4.6.2.2 Reduction of host/network node external hardware availability

Reduction of host/network node external hardware availability may affect assets in the following sense:

- Human assets
  - *human asset* A: if external hardware supports A in the execution of A's tasks (e.g. external modem connects user to the Internet).
- Information assets
  - *information asset* A: if external hardware is used for storing, processing or transmission of A in the system (e.g. important information can be stored on an external hard disc).
- Software assets
  - *software asset* A: if external hardware is used for storing, processing or transmission of A in the system.
- Physical assets
  - *physical asset* A: if external hardware supports the function of A (e.g. some scanners and printers need power supply cable).
- Organisational assets
  - *organisational asset* A: if A can be directly affected by the change of functionality of host/network node external hardware.
- Low and regulation assets
  - *low and regulation asset* A: if host/network node external hardware controls the access to A.

4.7 Templates for the availability risk analysis

As we said, the resources and time available for a risk analysis are limited. The identification of availability risks is not a trivial process and can take quite long time. Based on the information provided in the previous sections, we define templates that can support the identification of availability risks. Our templates are so-called fault trees which are based on the Fault Tree Analysis (FTA) that is "a system engineering method for representing the logical combinations of various system states and possible causes which can contribute to specified event (called top event)" [6]. The presented templates can be used to support the construction of fault trees showing unwanted incidents that can cause the availability risks. After the construction of a fault tree, one can calculate the probability of occurrence of the top event from the probability of occurrence of the basic events. We will talk about this topic in the next chapter.

FTA uses Boolean logic to describe the combinations of individual faults that can constitute a hazardous event. Each level in the tree "lists the more basic events that are necessary and sufficient to cause the problem shown in the level above it" [12]. In fault trees presented in this section, we use "OR", "XOR", and "AND" ports to connect events on the lower level to the event on the higher level. We use the "OR" port to denote that any of events on the lower level is sufficient to cause the undesired top event (event on the higher level in fault tree). The "XOR" port denotes that only one event on the lower level can occur before the undesired event on the higher level can happen. The "AND" port denotes that all events on the lower level have to occur before the top event can occur.
This section is structured into five sub-sections. Sub-section 4.7.1 presents the template for the assessment of host node availability. The template for the assessment of host application software availability is presented in sub-section 4.7.2. Sub-section 4.7.3 describes the template for the assessment of host operating system availability. The template for the assessment of host hardware availability is presented in sub-section 4.7.4. Sub-section 4.7.5 describes the template for the assessment of host security service availability.

4.7.1 Template for the assessment of host node availability

As we can see from Figure 4.5, the host node has four components that can affect its availability: system software (operating system), application software, internal hardware, and external hardware. Figure 4.7, presents the decomposition of dependability of host node software components. Figure 4.7 shows that the functionality of all host software components depends on the availability of host internal hardware – host storage device (hard disc). We also see from Figure 4.7 that host application software and host internal/external hardware software depend on the availability of host operating system. This means that during the availability analysis of host node, we always have to consider the availability of host operating system and the availability of host storage device (hard disc). The host storage device can be internal or external, and its risks are considered under unwanted incident *Denial of host hardware availability*. The denial of host operating system is considered under unwanted incident *Denial of host software availability*. The assessment of host application software and host internal/external hardware is performed for those application and hardware components that are relevant for the particular availability assessment. Every computer needs the power, and this means that the availability of host node also depends on the availability of power supply service. We also have to consider how well the access to the host node is secured. Under unwanted incident *Denial of host authorization availability* we consider the probability that the denial of host availability can be caused by the reduction of host authorisation availability (e.g. the probability that computer can be stolen or accessed by an unauthorized person). Under unwanted incident *Denial of host security service availability* we consider the probability that the denial of host availability can be caused by the reduction of host security service availability (e.g. an attack from the Internet (Network) or by computer virus; see Figure 4.19). Figure 4.15 shows the template for the assessment of host node availability. The additional availability risks that can be important for the host node availability can be added to the relevant level of this fault tree.

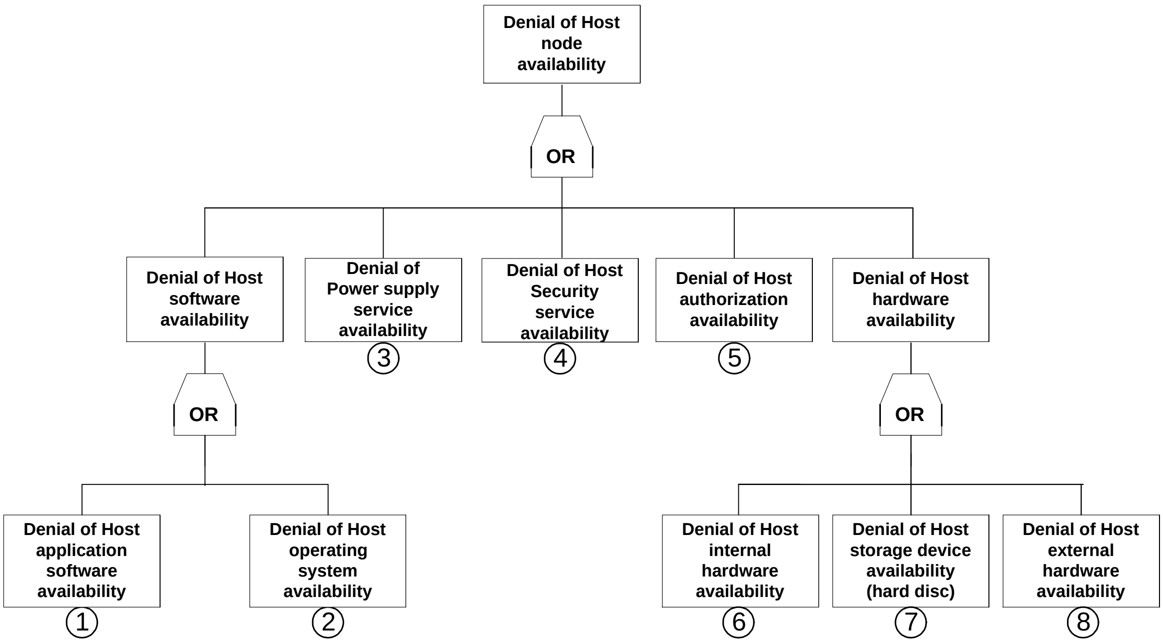

Denial of Host node availability
OR
Denial of Host software availability
Denial of Power supply service availability
Denial of Host Security service availability
Denial of Host authorization availability
Denial of Host hardware availability
3
4
5
OR
OR
Denial of Host application software availability
Denial of Host operating system availability
Denial of Host internal hardware availability
Denial of Host storage device availability (hard disc)
Denial of Host external hardware availability
1
2
6
7
8

Figure 4.15: Template for the assessment of host node availability

4.7.2 Template for the assessment of host application software availability

The template for the assessment of host application software availability is shown in Figure 4.16 below. Denial of host application software availability may be caused by unwanted incidents *Denial of software functionality*, *Incorrect installation and use by user*, and *Denial of software authorization functionality*. Under *Denial of software functionality* we consider the probability that software will not function or will malfunction. Under *Incorrect installation and use by user* we consider the probability that the denial of host application software may be caused by user actions. Under *Denial of software authorization functionality* we consider the probability that an unauthorized access to the host application software may cause its denial of functionality.

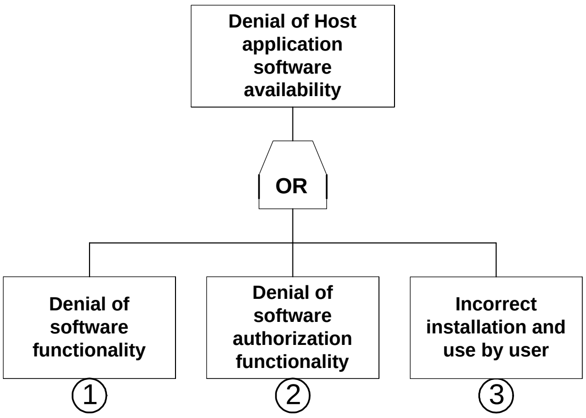

Denial of Host application software availability
OR
Denial of software functionality
Denial of software authorization functionality
Incorrect installation and use by user
1
2
3

Figure 4.16: Template for the assessment of host application software availability

4.7.3 Template for the assessment of host operating system availability

The template for the assessment of host operating system availability is shown in Figure 4.17 below. Denial of host operating system availability may be caused by unwanted incidents *Denial of operating system functionality*, *Incorrect installation and use by user*, and *Denial of operating system authorization functionality*. Under *Denial of operating system functionality* we consider the probability that operating system will not function or will malfunction. Under *Incorrect installation and use of OS by user* we consider the probability that the denial of host operating system may be caused by user actions. Under *Denial of operating system authorization functionality* we consider the probability that an unauthorized access to the host operating system may cause its denial of functionality.

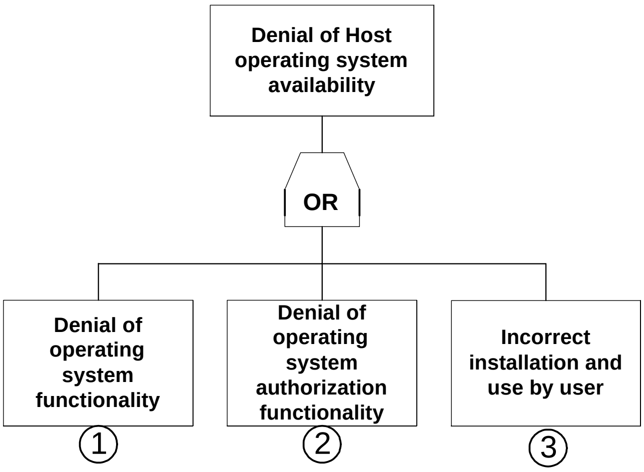

Denial of Host operating system availability
OR
Denial of operating system functionality
1
Denial of operating system authorization functionality
2
Incorrect installation and use by user
3

Figure 4.17: Template for the assessment of host operating system availability

4.7.4 Template for the assessment of host hardware availability

The template for the assessment of host hardware availability is shown in Figure 4.18. This template can be used for the assessment of both internal and external host hardware components. Denial of host hardware availability may be caused by unwanted incidents *Denial of functionality of hardware software*, *Denial of functionality of basic hardware components*, *Denial of functionality of other host hardware components*, *Incorrect installation and use by user*, and *Denial of authorization functionality of host hardware*. Under *Denial of functionality of hardware software* we consider the probability that software which supports hardware functionality, will not function or will malfunction. Under *Denial of functionality of basic hardware components* we consider the probability that basic hardware components will not function or will malfunction. Under *Denial of functionality of other host hardware components* we consider the probability that other host hardware components that support the hardware functionality, will not function or will malfunction. Under *Incorrect installation and use by user* we consider the probability that the denial of host hardware may be caused by user actions. Under *Denial of authorization functionality of host hardware* we consider the probability that an unauthorized access to the host hardware may happen and cause its denial of functionality (e.g. the probability that the host hardware can be stolen or accessed by an unauthorized person). The events with numbers 1 and 3 in the template are optional because there can be hardware components which do not depend on the functionality of software or other hardware components. For example, an external hardware – monitor depends on the functionality of software that supports its functionality and the functionality of graphic card, while an internal hardware – power supply does not depend on the functionality of software and other hardware components.

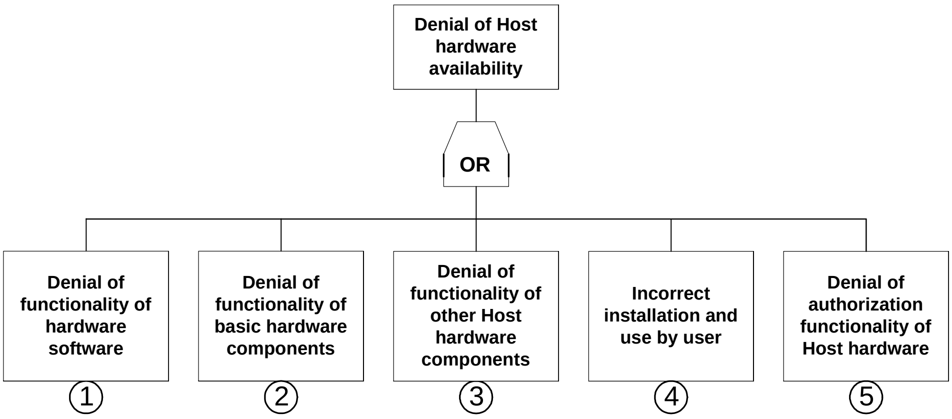

Denial of Host hardware availability
OR
Denial of functionality of hardware software
Denial of functionality of basic hardware components
Denial of functionality of other Host hardware components
Incorrect installation and use by user
Denial of authorization functionality of Host hardware
1
2
3
4
5

Figure 4.18: Template for the assessment of host hardware availability

4.7.5 Template for the assessment of host security service availability

The template for the assessment of host security service availability is shown in Figure 4.19. In this template we consider those software and special equipment components that contribute to the better protection of host node from security threats. We call this protection as host security service availability because antivirus software and special equipment such as firewall provide the host node with security service that protects it from the threats (network attacks and software viruses) that may affect its availability. The template shows that the protection of host node from the security threats can be done with the help of firewall and antivirus software.

Under *Lack of firewall* we consider the probability that due to the lack of firewall, the network threats (e.g. network attack) may cause the denial of host availability. Under *Denial of firewall functionality* we consider the probability that the firewall will not protect against threats that may cause the denial of host availability. These two threats are mutually excluding each other. This means that only one of these threats may occur before the unwanted incident *Denial of availability due to firewall problems* can happen. That is why we use the XOR port to connect these two threats to the risk *Denial of availability due to firewall problems*. In the same time, the denial of firewall functionality may have consequences for the host node availability if the firewall does not function and simultaneously the host node is attacked from the network. These two unwanted incidents have to happen in the same time, and that is why we use the AND port to connect them to the risk *Denial of firewall functionality*.

Under *Lack of antivirus software* we consider the probability that due to the lack of antivirus software, the malicious program or virus may cause the denial of host availability. Under

Denial of antivirus software functionality we consider the probability that antivirus software will not protect against threats (malicious program or virus) that may cause the denial of host availability. We use the XOR port to connect these two threats to the risk *Denial of availability due to antivirus software problems* because only one of these threats may occur before the unwanted incident on the higher level can happen. We use the AND port to connect the unwanted incidents *Virus attack*, and *Antivirus software does not function* to the risk *Denial of antivirus software functionality* because these two unwanted incidents have to occur simultaneously before the risk *Denial of antivirus software functionality* can happen.

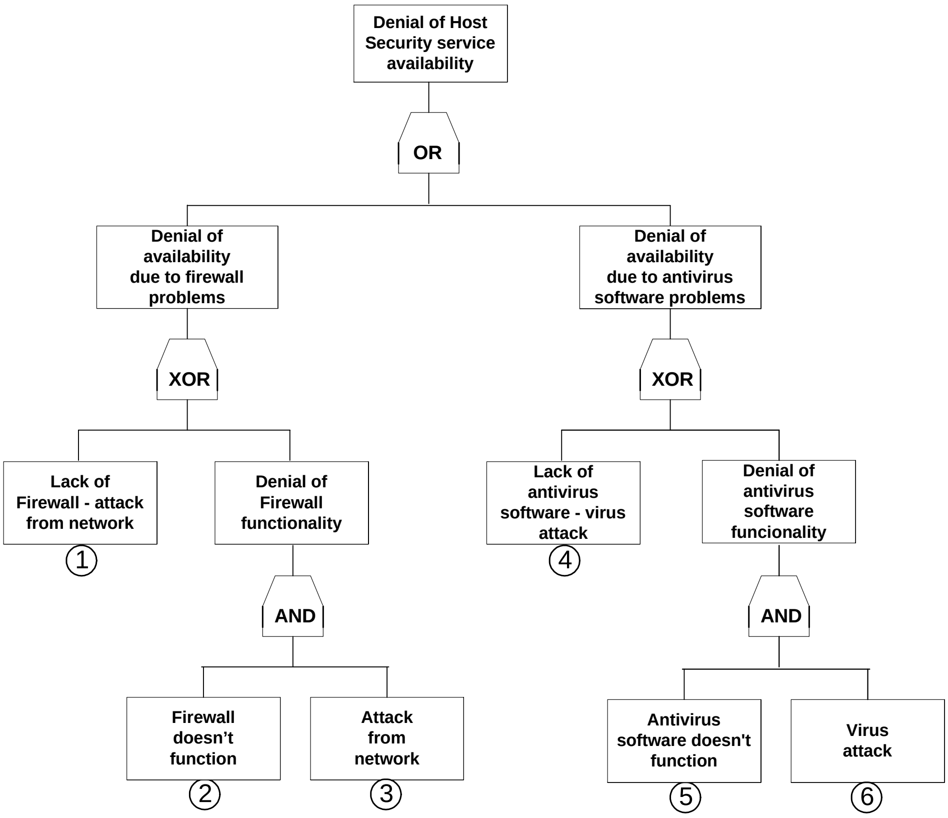

Denial of Host Security service availability
OR
Denial of availability due to firewall problems
Denial of availability due to antivirus software problems
XOR
XOR
Lack of Firewall - attack from network
1
Denial of Firewall functionality
Lack of antivirus software - virus attack
4
Denial of antivirus software funcionality
AND
AND
Firewall doesn't function
2
Attack from network
3
Antivirus software doesn't function
5
Virus attack
6

Figure 4.19: Template for the assessment of host security service availability

5 Model Driven Availability Risk Analysis (MODA)

As we mentioned earlier, the risk assessment community makes use of a structured approach to address risks – the so-called Risk management process. Recall that we defined this process in chapter 2 as the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk. MODA is a means within the risk management process to address availability risks. In this chapter we present MODA in an example-driven manner.

The chapter is structured into six sections. Section 5.1 gives the overview of the Risk management process on which MODA is based. MODA may be understood as a specialisation of the five risk management sub-processes specialised towards availability risk analysis. In the following we refer to this specialisation as the MODA risk management process. The first sub-process of the MODA Risk management process – Context Identification is presented in section 5.2. Section 5.3 describes the second sub-process, namely Risk Identification. The Risk Analysis is the third sub-process. It is presented in section 5.4. Section 5.5 presents Risk Evaluation – the fourth sub-process. Section 5.6 considers the last sub-process, namely Risk Treatment. All sections are further decomposed into sub-sections that present activities of sub-processes and demonstrate their practical use with the help of case study.

5.1 MODA Risk management process

The MODA risk management process is based on AS/NZS 4360:1999 Risk Management [6] and CORAS [5]. AS/NZS 4360 decomposes the risk management process into sub-processes for context identification, risk identification, risk assessment, risk evaluation and risk treatment. It also defines two sub-processes that run in parallel with the first five: communication and consultation, monitor and review. (Figure 5.1)

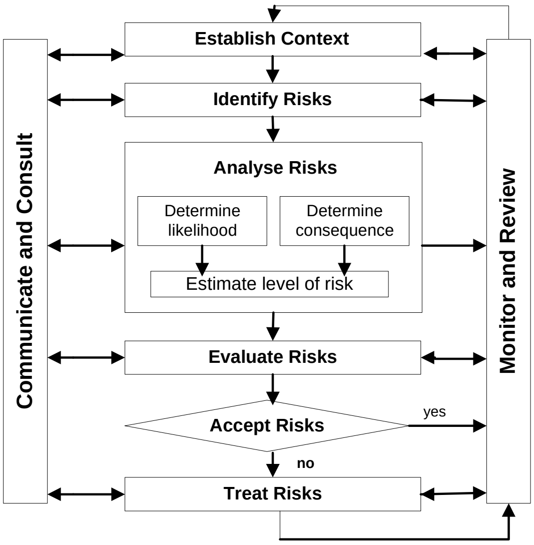


Figure 5.1: AS/NZS 4360 Risk management process

While the main source of inspiration for the definition of the MODA risk management process was AS/NZS 4360, the activities of the sub-processes of the CORAS risk management process provided valuable input for the definition of activities of sub-processes of the MODA risk management process.

MODA decomposes the risk management process into five sub-processes for context identification, risk identification, risk analysis, risk evaluation and risk treatment. These sub-processes are further decomposed into activities as described in Figure 5.2. The flow of information in the MODA risk management process is described in Table 5.1. The columns and rows represent the sub-processes of the MODA risk management process. The text in the shaded areas denotes the key activities within each sub-process. In the upper, right hand side of the shaded diagonal we describe how a sub-process provides information or results to be used in a later sub-process. For example, the “Risk identification” sub-process provides risks to availability aspects for the “Risk analysis” sub-process. In the lower, left hand side of the diagonal we describe how a sub-process depends on results or information from an earlier sub-process.

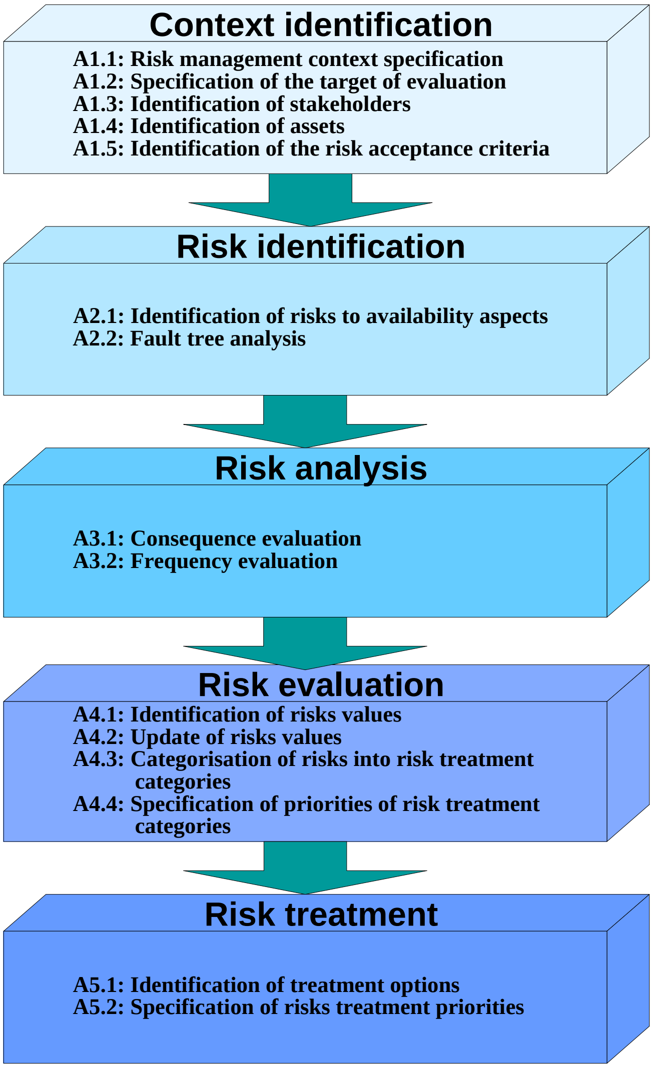

Context identification
A1.1: Risk management context specification
A1.2: Specification of the target of evaluation
A1.3: Identification of stakeholders
A1.4: Identification of assets
A1.5: Identification of the risk acceptance criteria
Risk identification
A2.1: Identification of risks to availability aspects
A2.2: Fault tree analysis
Risk analysis
A3.1: Consequence evaluation
A3.2: Frequency evaluation
Risk evaluation
A4.1: Identification of risks values
A4.2: Update of risks values
A4.3: Categorisation of risks into risk treatment categories
A4.4: Specification of priorities of risk treatment categories
Risk treatment
A5.1: Identification of treatment options
A5.2: Specification of risks treatment priorities

Figure 5.2: MODA risk management sub-processes along with activities (A)

Table 5.1: The flow of information in the MODA risk management process

	Context identification	Risk identification	Risk analysis	Risk evaluation	Risk treatment
Context identification	A1.1 Risk management context specification A1.2 Specification of the target of evaluation A 1.3 Identification of stakeholders A1.4 Identification of assets A 1.5 Identification of the risk acceptance criteria	- Provides target of evaluation (TOE) - Provides assets owners - Provides assets - Provides assets values	- Provides areas of relevance (context)	- Provides asset value domains - Provides risk evaluation criteria	- Provides areas of relevance (context)
Risk identification	- Depends on TOE - Depends on assets - Depends on assets values	A2.1 Identification of risks to availability aspects A2.2 Fault tree analysis	- Provides risks to availability aspects - Provides unwanted incidents		
Risk analysis		- Depends on risks to availability aspects - Depends on unwanted incidents	A 3.1 Consequence evaluation A 3.2 Frequency evaluation	- Provides consequence evaluation - Provides frequency evaluation	
Risk evaluation			- Depends on consequence evaluation - Depends on frequency evaluation	A 4.1 Identification of risks values A 4.2 Update of risks values A 4.3 Categorization of risks into risk treatment categories A 4.4 Specification of priorities of risk treatment categories	- Provides risks levels - Provides risk treatment categories - Provides risk treatment category priority
Risk treatment				- Depends on risks levels - Depends on risk treatment categories - Depends on risk treatment category priority	A 5.1 Identification of treatment options A 5.2 Specification of risks treatment priorities

5.2 Context identification

The objective of context identification sub-process is to define the scope of availability assessment, stakeholders along with assets, and risk evaluation criteria for each stakeholder. The context identification consists of five activities where the first activity may run in parallel with the other four and the latter four will typically be carried out in a sequential order:

- Risk management context specification
- Specification of the target of evaluation
- Identification of stakeholders
- Identification of assets
- Identification of the risk acceptance criteria

5.2.1 Activity 1.1: Risk management context specification

The objective of this activity is to establish the risk assessment objectives and identify needed risk assessment processes, activities and resources as well as risk assessment records to be kept. These tasks are decomposed into four sub-activities to get an overview of needed actions and make accomplishment of this activity more flexible and traceable.
The risk management context specification activity consists of four sub-activities that will typically be carried out in iterative manner:

- Specification of risk assessment objectives and needed studies
- Identification of relevant roles for a risk assessment
- Specification of risk assessment plan
- Identification of applied value categories

5.2.1.1 Specification of risk assessment objectives and needed studies

The objective of this sub-activity is to describe why the risk assessment is undertaken and define the risk management processes and activities that should be applied during the risk assessment, their scope and the resources required.

As a first step in this sub-activity, goals and objectives of the risk assessment should be defined and documented in the Assessment objectives table shown in Table 5.2. One should also document management/client decisions that depend on the assessment results. This can help the risk analysis leader to plan the work and ensure that the risk analysis is focused on management/client interests.

As a second step in this sub-activity, the risk assessment team and stakeholders should agree upon to which detail the risk management process will be applied. The needed studies along with required resources should be documented in the Assessment methods table [5] shown in Table 5.3. The descriptions of needed studies should be sufficiently detailed so that stakeholders who have not been the part of the risk management process can understand the conclusions and evaluate the process. The needed resources for selected studies should be specified as computational or human where the human resources may also include the need for specific expertise.

Table 5.2: Assessment objectives table

Risk assessment goals and objectives	<Description>

Table 5.3: Assessment methods table

Reference	Method Name	Description	Applied for Task	Resources Needed
<Pointer to where the method is further described>	<Method name>	<Description>	<List of tasks taken from assessment plan>	<Description of resources needed>

Assumptions that restrict the risk management process should be described and documented in the Assessment restrictions table [5] shown in Table 5.4.

Table 5.4: Assessment restrictions table

Reference	Restriction	Description	Applied for Activity
< Pointer to where the restriction is further described >	<Restriction>	<Description>	<List of activities>

5.2.1.2 Identification of relevant roles for a risk assessment

The objective of this sub-activity is to define the relevant roles of participants of the risk assessment. The Assessment roles table [5] shown in Table 5.5 should be filled in to document the roles of members of risk assessment team as well as names and background of team members. It should be specified who represents the client or a stakeholder and who belongs to the RA-team – those who will perform all the sub-processes and deliver the risk assessment report to the client. All roles are optional, except the project leader, the RA leader and the target owner (the client) roles that should be filled.

Table 5.5: Assessment roles table

Role	Name	Organisation	Background/Expertise
Project leader	<Name>	<Organisation>	<Text>
RA leader	<Name>	<Organisation>	<Text>
RA secretary	<Name>	<Organisation>	<Text>
Target owner	<Name>	<Organisation>	<Text>
Target developer	<Name>	<Organisation>	<Text>
…			
Field expert	<Name>	<Organisation>	<Text>
…			
RA expert	<Name>	<Organisation>	<Text>
…			
Other	<Name>	<Organisation>	<Text>
…			

5.2.1.3 Specification of risk assessment plan

The objective of this sub-activity is to define a risk assessment plan.

One should be aware that there are always some factors that can affect the duration of risk assessment. Sommerville [7] advises to use the following rule of thumb – first make an estimate as if nothing will go wrong, then increase your estimate to cover anticipated problems (Sommerville adds 30 per cent) and then add some per cent to your estimate to cover other things you hadn't thought of (Sommerville adds 20 per cent). Anticipated problems may include:

- People working on a project may fall ill or may leave.
- Essential support software and hardware may break down or be delivered late.
- The new and technically advanced project can have some parts that may turn out to be more difficult and take longer than originally anticipated.

Hoffer [29] gives examples of other factors that can affect the project execution (we adjusted some descriptions to suite to the risk assessment):

- Perceptions and willingness of stakeholders to participate in the project.
- Management commitment to the project.
- Familiarity of the risk assessment team with the proposed assessment area.
- Familiarity of the risk assessment team with assessment of similar systems of similar size.

In addition we can list the following factors that should be taken into account:

- Different stakeholders participating in a risk assessment can have different knowledge of risk assessment and risk management.
- It can take time to "clean up" results between the sub-processes and activities.
- The potential need for additional or updated system descriptions may be more than anticipated.

As a result of this sub-activity, the Assessment plan table [5] shown in Table 5.6 below should be filled in to document task types, dates of their execution, and the list of persons participating in each task

Table 5.6: Assessment plan table

Date	Task Type	Task	Participating Roles
<Date>	<Type>	<Task>	<List taken from Assessment roles table>

5.2.1.4 Identification of applied value categories

The objective of this sub-activity is to define what kind of value categories should be used in the risk assessment. The stakeholders should agree on whether values for consequences, frequencies and risks should be qualitative, quantitative, or combination of both.

Specification of frequency values

Stakeholders should agree on what kind of frequency values (qualitative or quantitative) can be used. The proposal for the frequency values range (scale) is shown in Table 5.7 [5]. The range chosen for the frequencies should be in the same order throughout the assessment. The quantitative frequency values should be numbers that show probability of a risk. The probability should be between 1 and 0, where 1 indicates that the risk will happen for sure, and 0 that it cannot happen. The corresponding recommended set of qualitative values is: {rare, unlikely, possible, likely, almost certain}.

The frequency values of risks (e.g. denial of component functionality) can be measured in:

- the number of unwanted incidents per year (e.g. number of denials of component functionality).
- the number of unwanted incidents per demands (number of denials of component functionality/number of demands).
- the percent of times the service/system or component is used.

Table 5.7: Qualitative and quantitative frequency values

	Frequency Values				
Category	Rare	Unlikely	Possible	Likely	Almost certain
Measured in terms of occurrences per year/month	1/100	1/10 - 1/50	1/10 - 1	1 –12	> 12
Measured in terms of occurrences per demands	1/10000		1/50		1/1
Measured in the percent of times the service/system or component is used	0.00 – 0.01 less often then 1%	0.01 – 0.05 between 1% and 5%	0.05 – 0.20 between 5% and 20%	0.20 – 0.50 between 20% and 50%	0.50 – 1.00 between 50% and 100%

The agreed set of frequency values should be documented in the Frequency values table shown in Table 5.8. The construction of table will assist to the achievement of two purposes: the documentation of assessment results and reusability of assessment results (e.g. documented frequency values can be used in another assessment).

Table 5.8: Frequency values table

	Frequency Values				
Category	Rare	Unlikely	Possible	Likely	Almost certain
<Category description>	<frequency value>	<frequency value>	<frequency value>	<frequency value>	<frequency value>

Specification of consequence values

Stakeholders should agree on whether consequence values should be quantitative or qualitative. The quantitative consequence values should be in the same order as the scale that will be used to value assets (see Activity 1.4). In the case of qualitative consequence values, the stakeholders should agree on how consequence values will be computed. One can use four alternative approaches to assign consequence values for the availability aspects risks:

- In the first approach, consequence values should reflect how the system unavailability (measured in lost hours) might affect aspects that depend on the system availability. Figure 5.3 shows the categorization of consequences of the reduction of system availability. Consequence values within the chosen consequence domain should be assigned according to the following set: {insignificant, minor, moderate, major, catastrophic}. For example, one can decide that the unavailability of the environment control system for a period of 2 hours may have minor consequence, while unavailability of this system for a period of 10 hours may have catastrophic consequence.

- In the second approach, the consequence is measured in the loss of assets value. The consequence values can be defined with the help of the Asset consequence values table shown in Table 5.9. This table shows how consequence values depend on the percentages of the loss of asset value because of an unwanted incident.
- In the third approach, the consequence is measured in the loss of target system availability. The consequence values can be defined with the help of the Target system consequence values table shown in Table 5.10. This table shows how consequence values depend on the reduction of the availability of target system due to an unwanted incident.

- In the fourth approach, we assign consequence values according to the level of loss of income of the organisation where the system is deployed. In this approach we have to consider financial consequences that an unwanted incident can cause to the organisation. When we compute the financial consequences of an unwanted incident, we can compare the lost income caused by this unwanted incident to the total income of organisation. Another way to define consequence values is to determine the total cost of recovery from the unwanted incident and then compare this total cost to the income of the target organisation. Table 5.11 shows a proposal for the Total income consequence values table. The consequence value of an unwanted incident is computed in the following way:

    1. First we compute the lost income (LI) of organization with the help of the following formula: LI = D/(U+D)*I where
    LI is a lost income.
    D is the system downtime during Service Time (time when the system should be available).
    U is the system uptime during the Service Time.
    I is the income of organization during the Service Time if the system is up all the time.
    2. Then we compute the total cost of recovery (TCR) from an unwanted incident (the lost income (LI) has to be added to the cost of recovery (CR): TCR = LI + CR).
    3. Now we determine the consequence percent (CP) comparing the total cost of recovery to the monthly income (MI) of the target organization: CP = (TCR/MI)*100. If we are only interested in the comparison of the lost income with the total income of organisation, the CP is defined as follows: CP = (LI/MI)*100.

4. Finally, when we know the CP, we use the Total income consequence values table to determine the consequence values of unwanted incidents.

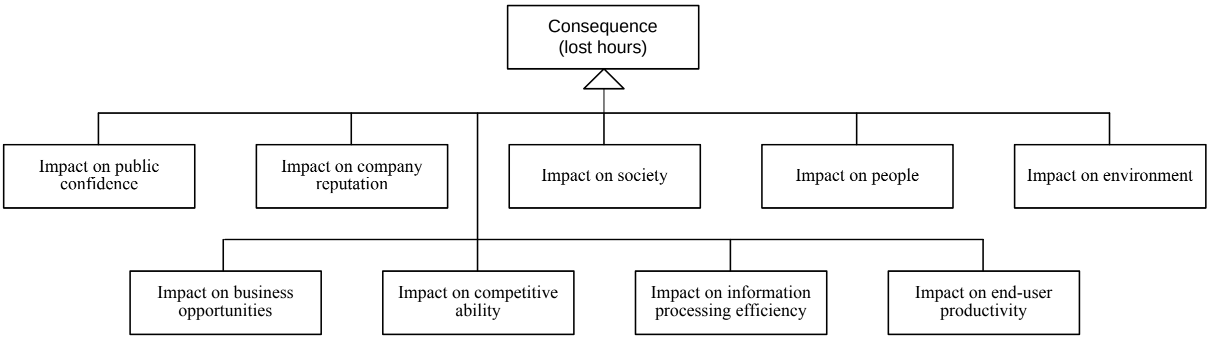

Consequence (lost hours)
Impact on public confidence
Impact on company reputation
Impact on society
Impact on people
Impact on environment
Impact on business opportunities
Impact on competitive ability
Impact on information processing efficiency
Impact on end-user productivity

Figure 5.3: Categorization of consequences of system unavailability

Table 5.9: Asset consequence values table

	Consequence Values				
Category	Insignificant	Minor	Moderate	Major	Catastrophic
Measured in the loss of asset value	0-01%	0.1-1%	1-5%	5-10%	10-100%

Table 5.10: Target system consequence values table

	Consequence Values				
Category	Insignificant	Minor	Moderate	Major	Catastrophic
Measured in the loss of target system availability	0-01%	0.1-1%	1-5%	5-10%	10-100%

Table 5.11: Total income consequence values table

	Consequence Values				
Category	Insignificant	Minor	Moderate	Major	Catastrophic
Total cost of recovery from an unwanted incident compared to the total income of organisation	0-01%	0.1-1%	1-5%	5-10%	10-100%
Lost income caused by an unwanted incident compared to the total income of organisation	0-01%	0.1-1%	1-5%	5-10%	10-100%
Measured in the impact on business	No impact on business. Minor delays	Lost profits (Lost project phases)	Reduce the resources of one or more departments. Loss of a couple of customers	Close down department(s) or business sectors	Out of business

The agreed set of consequence values should be documented in the Consequence values table shown in Table 5.12. The construction of table will assist to the achievement of two purposes:

the documentation of assessment results and reusability of assessment results (e.g. documented consequence values can be used in another assessment).

Table 5.12: Consequence values table

	Consequence Values				
Category	Insignificant	Minor	Moderate	Major	Catastrophic
<Category description>	<consequence value>	<consequence value>	<consequence value>	<consequence value>	<consequence value>

Specification of risk values

Stakeholders should agree on whether risk values should be quantitative or qualitative. One also has to agree on how to calculate risk values. In case when the frequency and consequence values are quantitative, they should be multiplied [6]. If one of the quantitative values equals 0, the risk value may be assigned by the relevant stakeholder. If one of the values is qualitative, the quantitative value should be mapped to its qualitative equivalent and then risk values should be defined with the help of Risk Matrix [5] shown in Table 5.13. In the case the frequency and consequence values are qualitative one should apply Risk Matrix. The recommended set of risk values is: {no risk (N), low risk (L), moderate risk (M), high risk (H), and extreme risk (E)}.

Table 5.13: Risk Matrix

	Frequency values				
Consequence Values	**Rare**	**Unlikely**	**Possible**	**Likely**	**Certain**
Insignificant	N	N	L	L	M
Minor	N	L	L	M	M
Moderate	L	L	M	M	H
Major	L	M	M	H	H
Catastrophic	M	M	H	H	E

The agreed set of risk values and their mode of computation should be documented in the Risk values table shown in Table 5.14.

Table 5.14: Risk values table

Chosen risk value category	**Computation mode**	**Level**	**Risk value**	**Risk value description**
<description>	<mode description>	A	<value>	<description>
		B		
		C		
		D		
		E		

Specification of treatment action priorities

Stakeholders should agree on how to assign priorities for treatment actions. The priority should be based on the level of treatment action value that can be assigned with the help of the Risk treatment action priority matrix shown in Table 5.15. The identification of treatment action values implies the assignment of values to treatment action benefits and costs. The stakeholders should agree on the scale that should be used for the assignment of values. We recommend to use the following scale for the benefit, cost and action values: “very low” (VL), “low” (L), “moderate” (M), “high” (H), “very high” (VH). The relationship among benefit, cost and action values should be agreed upon and demonstrated as in Table 5.15.

Table 5.15: Risk treatment action priority matrix

	Cost of risk treatment action				
Risk treatment action benefit	**Very low**	**Low**	**Moderate**	**High**	**Very high**
Very low	L	VL	VL	VL	VL
Low	L	L	L	VL	VL
Moderate	H	M	M	L	L
High	VH	H	H	M	M
Very high	VH	VH	H	H	M

The agreed scale for benefit, cost and action values should be documented in the Treatment action values table shown in Table 5.16

Table 5.16: Treatment action values table

Level	**Benefit Value**	**Cost Value**	**Treatment Action Value**
A	<value>	<value>	<value>
B			
C			
D			
E			

5.2.2 Activity 1.2: Specification of the target of evaluation

The objective of this activity is to define boundaries of the system that has to be assessed and describe its objectives, functions and security aspects. The organisation is always functioning in society and can be seen as a part of the society. The system in turn can be seen as a part of an organisation. The target of evaluation can be the part of the system that we are going to analyse, or the whole system. The description of the target of evaluation can help a risk assessment team to get a clear understanding of system usage and system’s role in the surrounding environment (organisation/enterprise, society). Specification of the target of evaluation also can help to delimit the part of the system to be analysed and in this way spare financial and human resources needed for risk assessment. These ideas are shown in Figure 5.4.

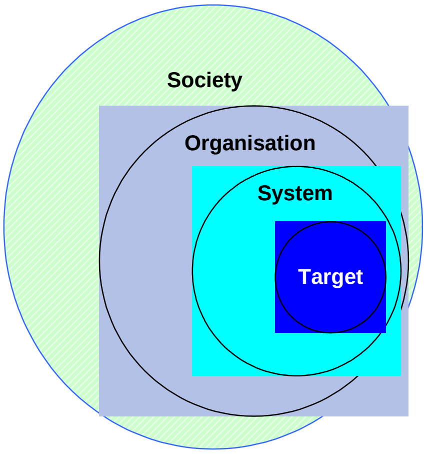


Figure 5.4: Organisation with its components as a part of society

As a first step of this activity, the system boundaries should be determined by means of defining system actors and use cases. Eeles [30] defines an actor as "someone or something outside the system that interacts with the system". An actor can be a person, software, hardware devices, an external system, data stores or networks. Finding actors helps establish the boundaries of the system since they are external to the system. A use case is a "description of a complete flow of events that results in something of value to an actor" [30].

The procedure for the first step will be following:

- Make an informal drawing – domain picture that represents an overall understanding of a situation.
- Find all actors.
- Find all use cases.
- Document actors and use cases in UML use case diagram.

Some of questions defined by COMET – Component and Model based development Methodology [31] can be helpful in defining the target system actors:

- Who uses the system?
- Who maintains the system?
- What other systems use this system?
- Who gets information from the system?
- Who provides information to the system?
- Who starts up and shuts down the system?
- Does anything happen automatically at present time?

To find use cases, one has to consider what each actor requires of the system. The following set of questions defined by Eeles [30] may be useful when identifying use cases:

- For each actor, what are the tasks in which the system would be involved?
- Does the actor need to be informed about certain occurrences in the system?
- Will the actor need to inform the system about external changes?

- What information must be modified or created in the system, and what actors must participate in those changes?
- What use cases will support administration and maintenance of the system (e.g. adding new users)?

As a second step of this activity, the risk assessment team should decide whether they need detailed description of system architecture (main components). If this description is required, one can specify the main system components using UML component/deployment diagrams and/or sequence diagrams.

As a last step of this activity, the Target-of-evaluation table [5] shown in Table 5.17 should be filled in with relevant information. The system owner, who represent organisation where the system has/is deployed, and risk analysts should fill this table with information that describes objectives, functions and security aspects of the system.

Table 5.17: Target-of-evaluation table

Target:	<Target of evaluation>
Objective:	1. <Objective of Target> 2. …
Service/Functions:	1. <Service/Function of Target> 2. …
Security Aspects:	<Security>

Example. Specification of the target of evaluation: Private Lessons

An English teacher offers online help to people (students) who want to improve their English skills. To get a private English lesson, people have to register their personal information and make a prepayment with a visa card. The teacher uses the Windows 2000 operating system and he has neither a firewall nor antivirus software installed on his computer. An internal IDSL modem and a network card installed on his computer allow him to be connected to the Internet and these internal hardware components need special software that supports their functionality. The Internet provider guarantees that the teacher will have a stable Internet connection in 90% of all days of the year. With the help of standard application program for communication through the Internet (e.g. Net Meeting), the teacher communicates with students and sees them on the monitor. He uses web camera with microphone, speakers and special application software Net Customer to view users statistics and to be notified about the order of new lesson. Figure 5.5 below shows the domain picture.

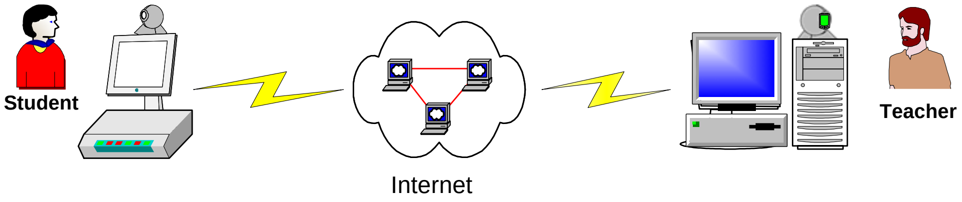


Figure 5.5: Domain picture

The identified actors and use cases are shown in Figure 5.6.

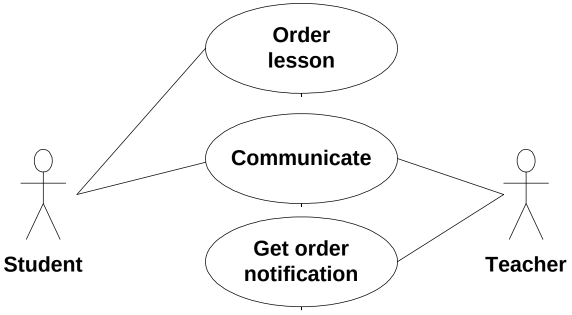


Figure 5.6: Use case diagram

The target of evaluation table is shown in Table 5.18.

Table 5.18: Private Lessons Target-of-evaluation table

Target:	Private Lessons system (Teacher)
Objective:	1. Online interactive English tutorial service
Service/Function:	1. Provide communication with students 2. Provide service order notification 3. Provide order lesson functionality
Security Aspects:	Availability should be the main concern

5.2.3 Activity 1.3: Identification of stakeholders

The objective of this activity is to identify all stakeholders of the target system. Recall that stakeholders are “those people and organizations that may affect, be affected by, or perceive themselves to be affected by, a decision or activity” [5]. Finding stakeholders helps to define those people and/or organizations that have interests and/or assets in the target system.

In this activity all stakeholders should be identified and documented in the Stakeholders table [5] shown in Table 5.19. The list of identified actors may be helpful in the identification of stakeholders. However, one should be aware of the fact that not all actors can be stakeholders, since stakeholders, by definition, are only people and/or organizations.

Table 5.19: Stakeholders table

Stakeholder ID	Stakeholder (Role)	Stakeholder (Name)	Description
<ID>	<Role>	<Name>	<Description>

***Example.* Identification of stakeholders: Private Lessons**

The identified stakeholders are documented in the Stakeholder table shown in Table 5.20.

Table 5.20: Private Lessons Stakeholder table

Stakeholder ID	Stakeholder (Role)	Stakeholder (Name)	Description
01	Teacher	Nick Norman	Gives private English lessons to students.
02	Student		Gets private English lessons and makes prepayment with a visa card

5.2.4 Activity 1.4: Identification of assets

The objective of this activity is to identify and value the assets that are relevant to the target of evaluation.

As a first step in this activity, one should identify the asset value domain(s) to be applied. It is desirable to apply generic asset value categories that allow comparison of asset values across different asset categories. The proposal for asset value domains [5] is shown in Table 5.21.

Table 5.21: Generic asset value domains

Value domain name	Asset value descriptions
Qualitative consequence values	Insignificant, Minor, Moderate, Major, Catastrophic
Binary	0/1 where 0 means asset has insignificant value, and 1 means loss of business
Ranked numbers	On the scale 1 - 10
Numeric values	e.g. as measured in economical value

We recommend to identify assets based on the following categories [5], which cover relevant aspects of and about a system:

- Human assets: Assets related to human resources, special knowledge.
- Physical assets: Includes all physical components in the system and system dependent components.
- Information assets: All information in the system and system dependent information.
- Organisational assets: Organisational concerns, organisational (system) internal regulations, routines etc.
- Law and regulation assets: External laws and regulations that influence the system.
- Software assets: All software used in the system or system dependent.
- Other assets: Assets that do not fit into one of the other themes, or assets that are composed of a grouping of the above asset classes.

The procedure for the rest of activity will be the following:

- For each identified stakeholder, identify assets in the target of evaluation:
  Go through all asset categories and identify assets with the help of questionnaires for each asset category [5] (Figure 5.7).
- Assign value to each identified asset.

- Illustrate assets in an asset diagram [5] (Figure 5.8).
- Document identified assets along with their values and stakeholders in the Asset table (Table 5.22).

There may be situations when different stakeholders are related to the same asset. In this case, the analyst should establish a "one asset – one stakeholder" relationship and only "asset owner" (usually stakeholder who is responsible for the asset) can assign value to the asset.

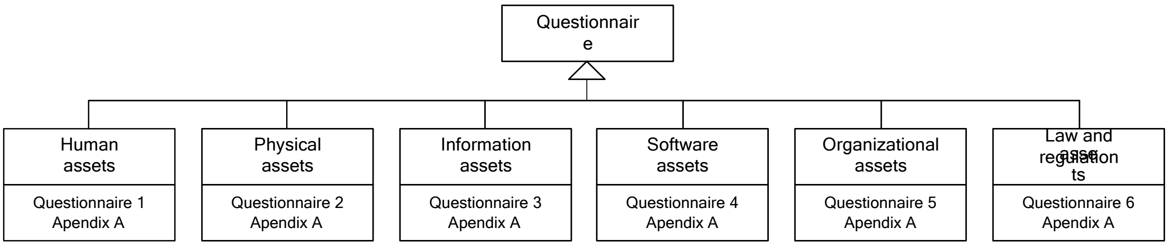

Questionnair e
Human assets
Questionnaire 1 Apendix A
Physical assets
Questionnaire 2 Apendix A
Information assets
Questionnaire 3 Apendix A
Software assets
Questionnaire 4 Apendix A
Organizational assets
Questionnaire 5 Apendix A
Law and regulation asse ts
Questionnaire 6 Apendix A

Figure 5.7: Questionnaire guide

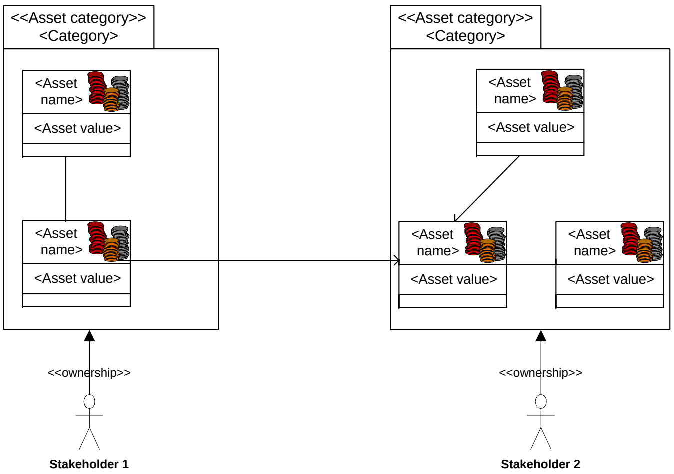


Figure 5.8: Asset diagram

Table 5.22: Asset table

ID	Stakeholder	Asset Category	Asset	Description	Value
<ID>	<Stakeholder>	<Category>	<Asset>	<Description>	<Value>

Example. Identification of assets: Private Lessons

The asset diagram is shown in Figure 5.9. The asset table is shown in Table 5.23 and documents stakeholders, asset themes and assets together with the description of assets and their values. Both student and the teacher have availability of service as an asset that is very important to them. The student pays 300 NOK for one lesson and the teacher is planning to give 6 lessons per day.

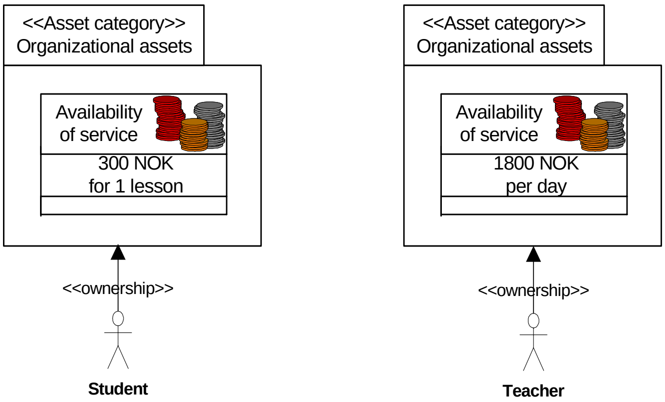


Figure 5.9: Private Lessons Asset diagram

Table 5.23: Private Lessons Asset table

ID	Stakeholder	Asset Category	Asset	Description	Value
01	Teacher	Organizational	Availability of service	The teacher offers tutorial service to the students.	1800 NOK per day
02	Student	Organizational	Availability of service	The student gets tutorial service from the teacher	300 NOK for 1 lesson

5.2.5 Activity 1.5: Identification of the risk acceptance criteria

The objective of this activity is to identify the risk acceptance criteria that will be used to determine whether a given risk is acceptable or not.

In this activity, each stakeholder has to assign risk acceptance criteria for each asset that the stakeholder has in the target system. The risk acceptance criteria should reflect the acceptable potential level of risk that an asset can be exposed to. The risk acceptance criteria may be defined with respect to single risks, group of risks or total risks. The acceptance values can be qualitative or quantitative and may be defined on the basis of consequence, frequency or risk values. The acceptance values should be of the same domain. This can help to avoid misunderstandings among stakeholders and contribute to the better reusability of availability assessment results. We recommend the risk acceptance criteria to be formulated on the form shown in Figure 5.10.

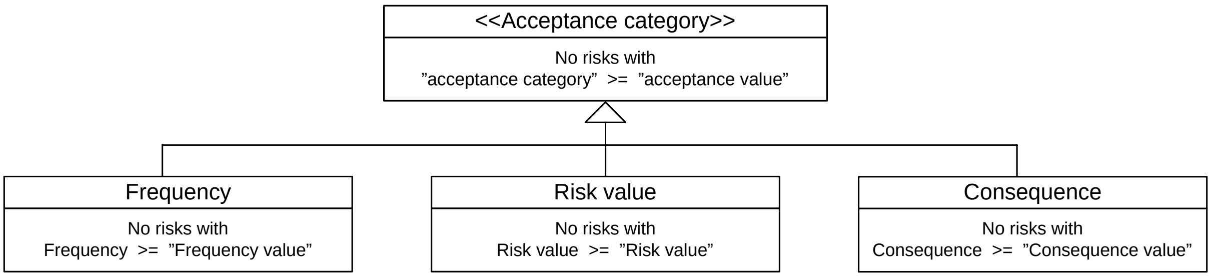

<<Acceptance category>>
No risks with
”acceptance category” >= ”acceptance value”
Frequency
No risks with
Frequency >= ”Frequency value”
Risk value
No risks with
Risk value >= ”Risk value”
Consequence
No risks with
Consequence >= ”Consequence value”

Figure 5.10: Risk acceptance criteria alternatives

The chosen risk acceptance criteria for each asset should be documented in the Risk acceptance table shown in Table 5.24

Table 5.24: Risk acceptance table

Stakeholder	Asset category	Asset	Risk acceptance criteria
<stakeholder>	<category>	<asset>	<description>

Example. Identification of the risk acceptance criteria: Private Lessons

The risk acceptance table is shown in Table 5.25 and documents stakeholders, asset categories and assets along with the description of risk acceptance criteria.

Table 5.25: Private Lessons Risk acceptance table

Stakeholder	Asset category	Asset	Risk acceptance criteria
Teacher	Organizational	Availability of service	No risks that have a risk value > Low
Student	Organizational	Availability of service	No risks that have a risk value > Low

5.3 Risk identification

The objective of the risk identification sub-process is to define the availability aspects risks that are relevant for the target of evaluation. The risk identification sub-process consists of two activities that will typically be carried out in a sequential order:

▪ Identification of risks to availability aspects
▪ Fault tree analysis

5.3.1 Activity 2.1: Identification of risks to availability aspects

The objective of this activity is to identify availability aspects risks that are relevant for the target of evaluation. During this activity, all assets of each stakeholder are considered and possible risks are identified and documented along with relevant entities in the availability risks tables. The construction of availability risks tables will insure that all relevant availability aspects have been considered and relevant entities of availability aspects are discovered. Guidelines in chapter 4 describe assets that can be affected by the reduction of availability aspects.

During the risk identification each availability aspect is considered with respect to how the reduction of availability aspect can affect assets of each stakeholder. When the software availability is considered, the identification of risks can be narrowed to the identification of application software risks. It is not necessary to consider operating system availability risks in this sub-process because other availability aspects depend on the operating system availability and thus an operating system always has to be considered (it is done in the template for the analysis of operating system availability). It is also not necessary to consider availability risks to internal and external hardware software components in this sub-process because these risks are analysed in the templates for the analysis of hardware availability.

Guidelines for the identification of availability aspects risks of the target of evaluation

```
For each stakeholder
    For each asset that this stakeholder has
        For each availability aspect at level 1, 2, and 3 as defined in figures 4.3, 4.8, 4.11, 4.13
```

- Define whether the asset can be affected by the denial of availability aspect.
- If the asset can be affected, document the stakeholder, availability aspect, availability aspect risk and relevant entity of availability aspect in the Availability risks table shown in Table 5.26. It may be convenient to make one table for each availability aspect.

Table 5.26: Availability risks table

Stakeholder	Asset	Availability aspect	Risk	Relevant entity
<Stakeholder>	<Asset>	<Availability aspect>	<Risk>	<Entity>

Example. Identification of risks to availability aspects: Private Lessons

In this activity we concentrate on the one stakeholder – the teacher, because the availability of the service that he offers to the students, depends on the availability of host node (service node – computer that the teacher uses to communicate with the students) and the availability of the teacher to give private lessons. Table 5.27 below shows the network availability risks table for the teacher.

Table 5.27: Private Lessons Network availability risks table

Stakeholder	Asset	Availability aspect	Risk	Relevant entity
Teacher	Availability of service	Network availability	Denial of Network availability	Internet connection

Without software application Net Meeting the teacher is not able to communicate through the Internet with his students. If Net Customer software is not available, the teacher will not be notified about the order of new lesson. Table 5.28 below shows the software availability risks table for the teacher.

Table 5.28: Private Lessons Software availability risks table

Stakeholder	Asset	Availability aspect	Risk	Relevant entity
Teacher	Availability of service	Host application software availability	Denial of host application software availability	Net Meeting Net Customer

IDSL modem and network card are necessary to have the Internet connection and without web camera, monitor and speakers, the teacher will not be seen by the students and he will not be able to see and hear the students. Table 5.29 shows the hardware availability risks table for the teacher.

Table 5.29: Private Lessons Hardware availability risks table

Stakeholder	Asset	Availability aspect	Risk	Relevant entity
Teacher	Availability of service	Host internal hardware availability	Denial of host internal hardware availability	IDSL modem Network card
		Host external hardware availability	Denial of host external hardware availability	Web camera Monitor Speakers

Without the teacher, the service has no value and the students cannot get private lessons. Table 5.30 below shows the human availability risks table for the teacher.

Table 5.30: Private Lessons Human availability risks table

Stakeholder	Asset	Availability aspect	Risk	Relevant entity
Teacher	Availability of service	Human availability	Denial of Human availability	Teacher

5.3.2 Activity 2.2: Fault tree analysis

The objective of the fault tree analysis activity is to identify causes that may lead to the risks identified during the previous activity. During this activity the fault trees, which show unwanted events, are built and the relationships among these events are established.

For building of fault trees one can use *Templates for the availability risk analysis* that are described in chapter 4.7. The fault tree analysis activity consists of several steps that will typically be carried out in a sequential order:

- Insert availability aspects risks, documented in the availability risks tables, as top events in fault trees.

- Build fault trees with the help of templates described in chapter 4.7: (see Figure 5.11)
  To build the fault tree that has the top event:
  - Denial of host application software availability, use the template from Figure 4.16.
  - Denial of host operating system availability, use the template from Figure 4.17.
  - Denial of host hardware availability, use the template from Figure 4.18.
  - Denial of host node availability, use the template from Figure 4.15.
  - Denial of host security service availability, use the template from Figure 4.19.

- For each event identify possible causes that may lead to it [1] and place them at the next level in the fault tree. The identified events have to be connected to the top event through a logical port that can be of three kinds: an *and-port*, an *or-port* or a *xor-port*.

  - The *and-port*: All events under this port have to be occurred before the event over the *and-port* can happen.
  - The or-port: At least one event under this port has to be occurred before the event over the *or-port* can happen.
  - The *xor-port*: Only one event under this port has to be occurred before the event over the *xor-port* can happen.

[1] Description in the chapter 4 *Availability decomposed* of relationship of availability aspects to other availability aspects can help in the identification of unwanted incidents

- If identified events are described on an appropriate level of abstraction – the building of the fault tree can be finished, otherwise the rest of the fault tree is constructed in the same way as described in the previous step on the basis of each new identified event until the desired level of abstraction is reached.

- If there is still need for more detailed description of incidents, one can use the CORAS [5] guidelines for the use of HasOp [11] for risk identification.

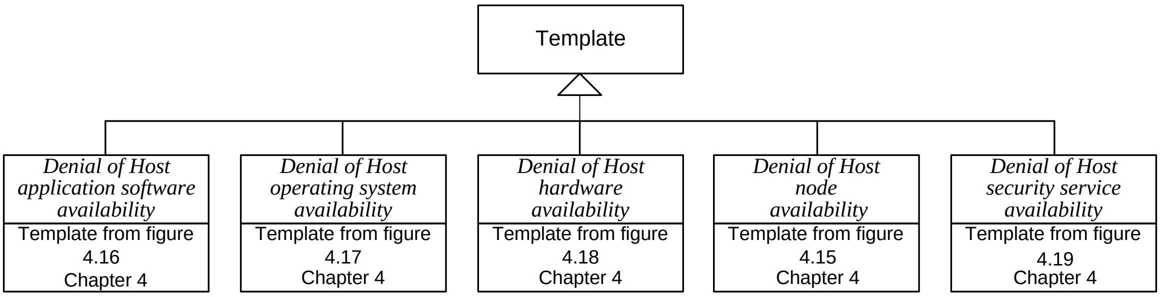

Template
Denial of Host application software availability
Template from figure 4.16 Chapter 4
Denial of Host operating system availability
Template from figure 4.17 Chapter 4
Denial of Host hardware availability
Template from figure 4.18 Chapter 4
Denial of Host node availability
Template from figure 4.15 Chapter 4
Denial of Host security service availability
Template from figure 4.19 Chapter 4

Figure 5.11: Fault tree template guide

***Example.* Fault tree analysis: Private Lessons**

As we can see from the availability risks tables (Tables 5.27…5.30), the availability of service that the teacher offers to the students can be affected by the reduction of the network availability, host node application software availability, host node internal and external hardware availability, and human availability (teacher). The availability of host node also can be affected by the denial of host operating system availability, power supply service availability, and host authorization availability. Figures 5.12 and 5.13 show these ideas. To build the fault tree that has the top event *Denial of host node availability*, we have used the template from Figure 4.15.

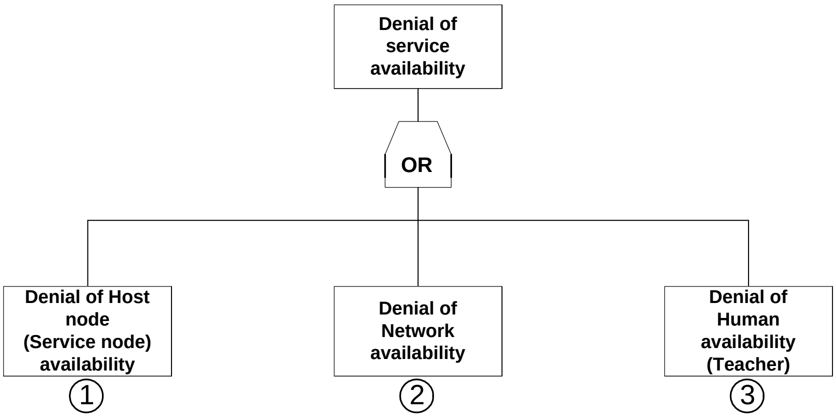

Denial of service availability
OR
Denial of Host node (Service node) availability
Denial of Network availability
Denial of Human availability (Teacher)
①
②
③

Figure 5.12: Fault tree with the top event Denial of service availability

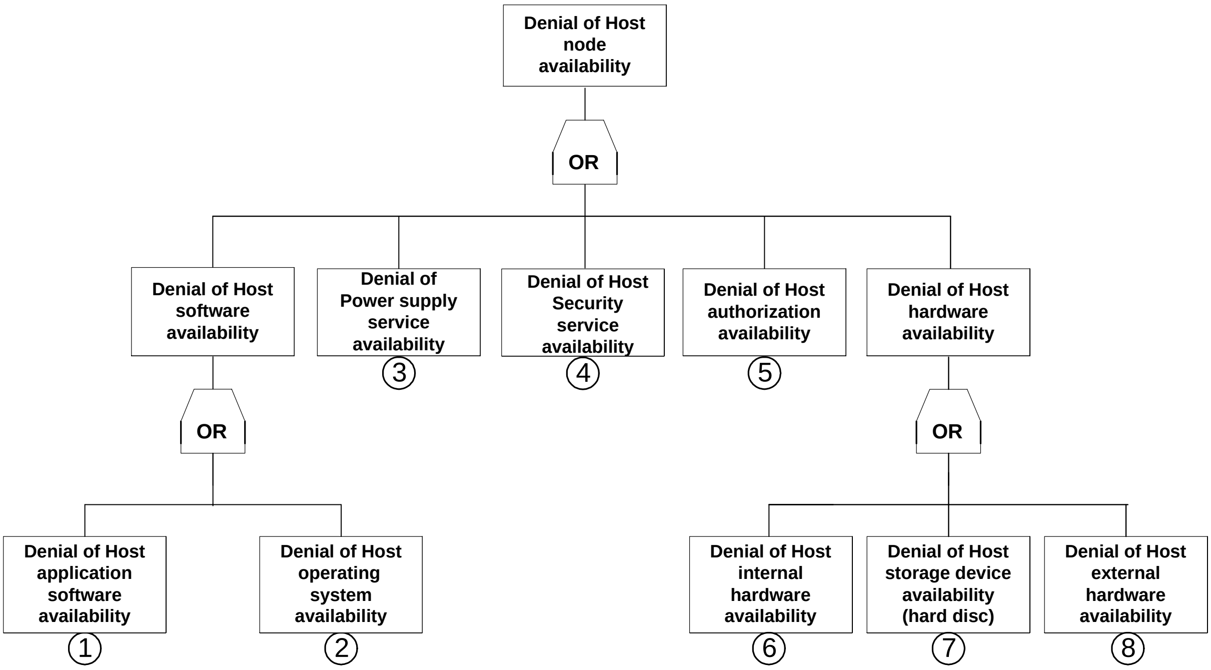

Denial of Host node availability
OR
Denial of Host software availability
Denial of Power supply service availability
Denial of Host Security service availability
Denial of Host authorization availability
Denial of Host hardware availability
3
4
5
OR
OR
Denial of Host application software availability
Denial of Host operating system availability
Denial of Host internal hardware availability
Denial of Host storage device availability (hard disc)
Denial of Host external hardware availability
1
2
6
7
8

Figure 5.13: Fault tree with the top event Denial of host node availability

Figure 5.14 shows the fault tree for the availability risk *Denial of host application software availability* and is constructed with the help of the template from Figure 4.16.

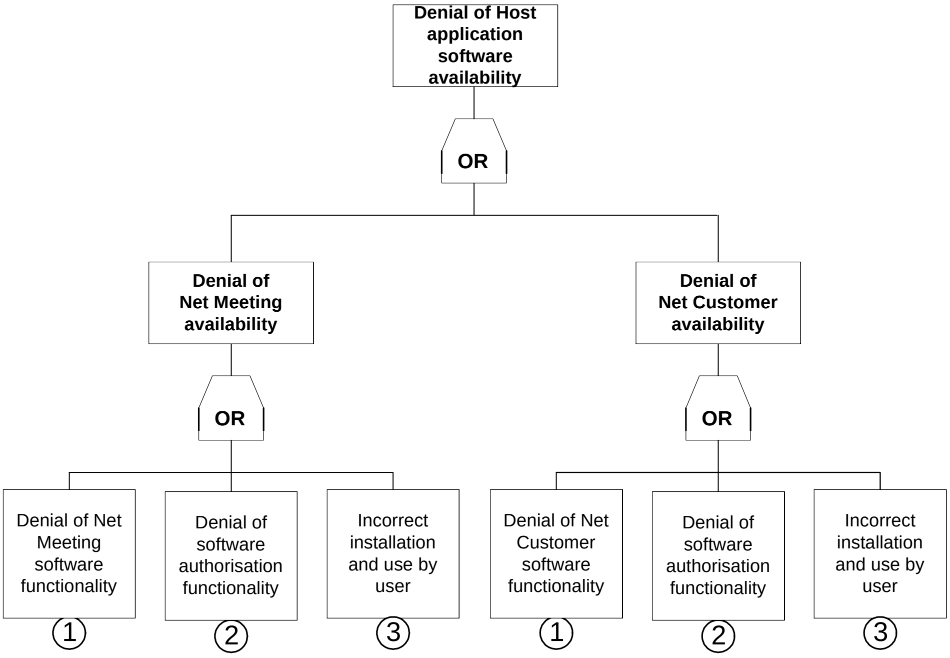

Denial of Host application software availability
OR
Denial of Net Meeting availability
Denial of Net Customer availability
OR
OR
Denial of Net Meeting software functionality
Denial of software authorisation functionality
Incorrect installation and use by user
Denial of Net Customer software functionality
Denial of software authorisation functionality
Incorrect installation and use by user
1
2
3
1
2
3

Figure 5.14: Fault tree with the top event Denial of host application software availability

Figure 5.15 shows the fault tree for the availability risk *Denial of host operating system availability* and is constructed with the help of the template from Figure 4.17.

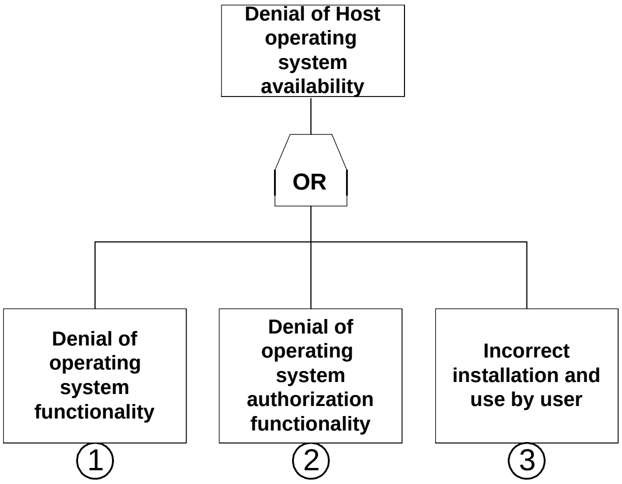

Denial of Host operating system availability
OR
Denial of operating system functionality
Denial of operating system authorization functionality
Incorrect installation and use by user
1
2
3

Figure 5.15: Fault tree with the top event Denial of host operating system availability

For the construction of hardware availability fault trees we can use the template from Figure 4.18. Figures 5.16 and 5.17 show the fault trees for the availability risks *Denial of host internal hardware availability* and *Denial of host external hardware availability*.

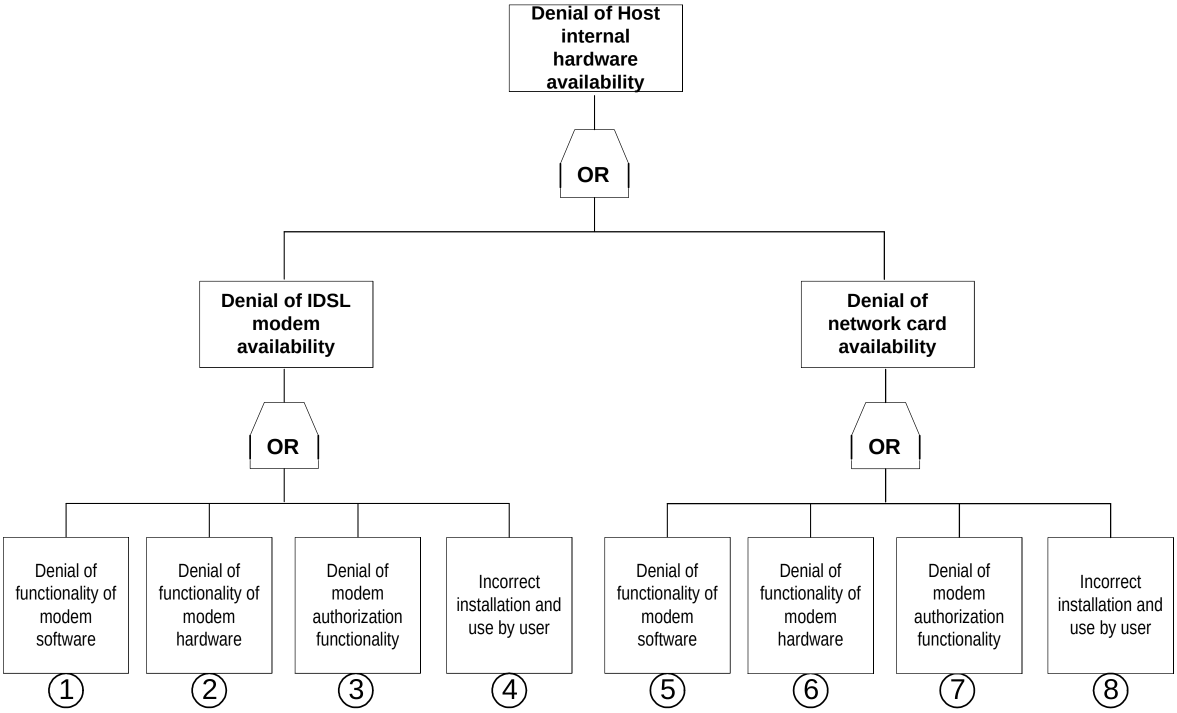

Denial of Host internal hardware availability
OR
Denial of IDSL modem availability
Denial of network card availability
OR
OR
Denial of functionality of modem software
Denial of functionality of modem hardware
Denial of modem authorization functionality
Incorrect installation and use by user
Denial of functionality of modem software
Denial of functionality of modem hardware
Denial of modem authorization functionality
Incorrect installation and use by user
1
2
3
4
5
6
7
8

Figure 5.16: Fault tree with the top event Denial of host internal hardware availability

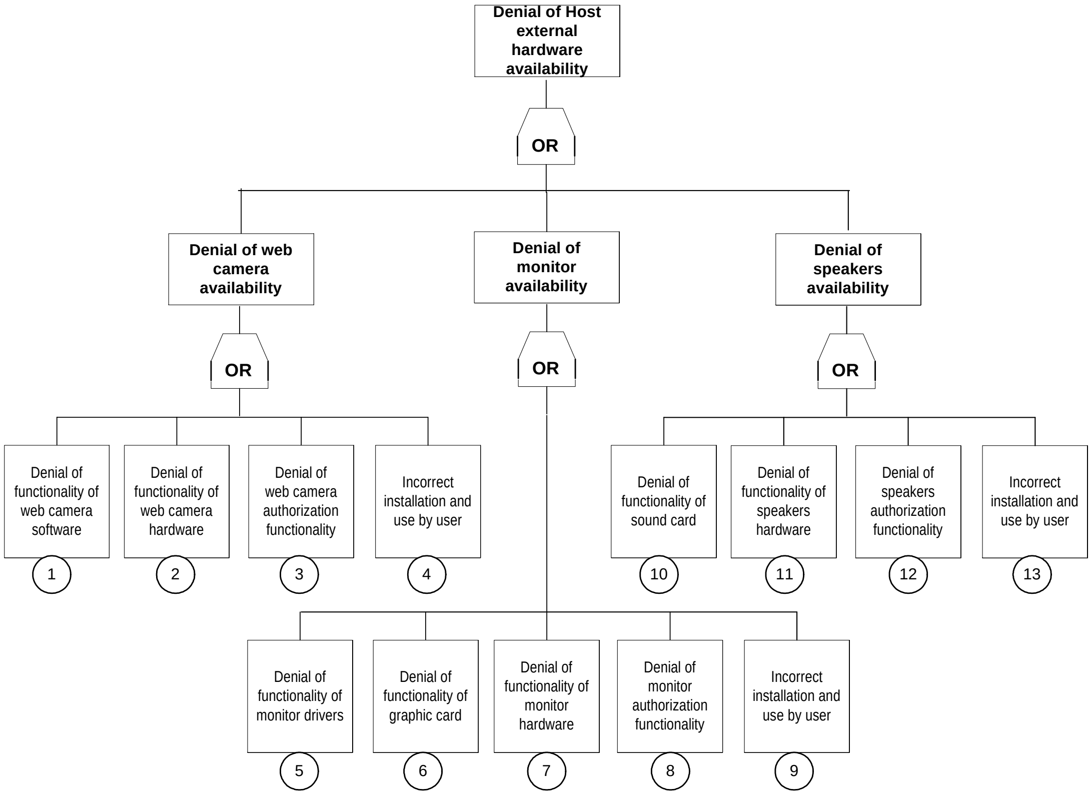

Denial of Host external hardware availability
OR
Denial of web camera availability
Denial of monitor availability
Denial of speakers availability
OR
OR
OR
Denial of functionality of web camera software
Denial of functionality of web camera hardware
Denial of web camera authorization functionality
Incorrect installation and use by user
Denial of functionality of sound card
Denial of functionality of speakers hardware
Denial of speakers authorization functionality
Incorrect installation and use by user
1
2
3
4
10
11
12
13
Denial of functionality of monitor drivers
Denial of functionality of graphic card
Denial of functionality of monitor hardware
Denial of monitor authorization functionality
Incorrect installation and use by user
5
6
7
8
9

Figure 5.17: Fault tree with the top event Denial of host external hardware availability

The template from Figure 4.19 can help us to build the fault tree for the risk *Denial of host security service availability*. Figure 5.18 shows the relevant fault tree.

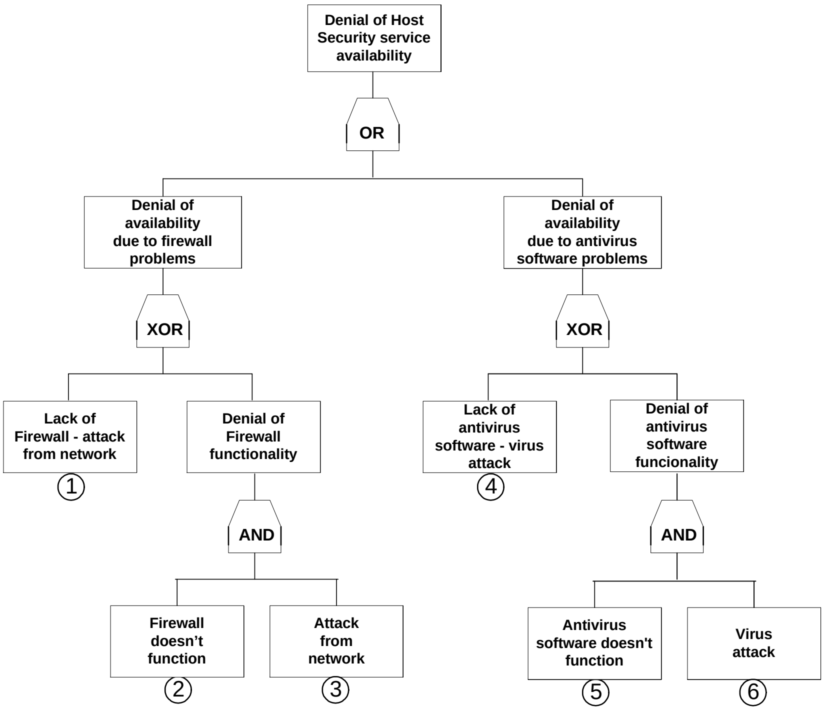

Denial of Host Security service availability
OR
Denial of availability due to firewall problems
Denial of availability due to antivirus software problems
XOR
XOR
Lack of Firewall - attack from network
1
Denial of Firewall functionality
Lack of antivirus software - virus attack
4
Denial of antivirus software funcionality
AND
AND
Firewall doesn't function
2
Attack from network
3
Antivirus software doesn't function
5
Virus attack
6

Figure 5.18: Fault tree with the top event Denial of host security service availability

5.4 Risk analysis

The objective of the risk analysis sub-process is to describe consequences and frequencies of identified risks. The inputs to this sub-process are risks that were identified during the risk identification sub-process. The risk analysis sub-process consists of two activities that can be carried out in any order:

▪ Consequence evaluation
▪ Frequency evaluation

5.4.1 Activity 3.1: Consequence evaluation

The objective of this activity is to analyse the consequence of the identified risks and evaluate their impact on the enterprise or system level. The consequence can be measured in the loss of assets values, the loss of availability of the target system or financial losses of the target organisation. The consequence value also can be assessed based on the information from previous similar assessments, historical data, available statistic information, and subjective assessment of RA-team or experts judgment.

The procedure for this activity is the following:

- Input for this activity are risks identified during the risk identification sub-process.

- The consequence table for each availability aspect should be filled in and document stakeholders, assets, risks and their consequence values. The consequence values should be defined according to the scale that has been identified during Activity 1.1. Table 5.31 shows the general form of consequence table and figures A.2, A.3, A.4, A.5 in Appendix A show consequence tables for different availability aspects.

- If consequence values are missing for some unwanted incidents, one can use the CORAS [5] guidelines for use of FMECA [13], Markov analysis [15] or Event tree analysis [32] for consequence evaluation.

Table 5.31: Consequence table

Stakeholder	Asset	Risk	Risk scenario	Consequence value	Consequence description
<Stakeholder>	<Asset>	<Risk>	<Risk scenario>	<Consequence value>	<Consequence description>

***Example.* Consequence evaluation: Private Lessons**

Recall that a student pays 300 NOK for one lesson and the teacher is planning to give 6 lessons per day. We assume that the teacher is planning to give private lessons 22 days per month. The total monthly income of the teacher will be:

300 * 6 * 22 = 39600 NOK. We determine consequence values with the help of Total income consequence values table (Table 5.11). The consequence tables for the teacher are depicted in tables below and show identified consequence values together with their description.

Table 5.32: Private Lessons Consequence table for software availability risks

Stakeholder	Asset	Risk			Risk scenario	Consequence value	Consequence description
Teacher	Availability of service	Denial of host Software availability	Denial of host operating system availability		The host operating system doesn't function or malfunction	Major	It takes the teacher one day to reinstall the operating system and application programs that he uses. Additionally he pays 300 Kr for technical support service. TCR = 1800 + 300 = 2100 NOK CP = (2100/39600)*100 = 5,30%
			Denial of host application software availability	Denial of Net Meeting availability	Application software Net Meeting doesn't function or malfunction	Major	The teacher hasn't an alternative program to use. It takes him one day to get an updated version of Net Meeting and install it. The newer version of NM costs 400 NOK. TCR = 1800 + 400 = 2200 NOK CP = (2200/39600)*100 = 5,55%
				Denial of Net Customer availability	Application software Net Customer doesn't function or malfunction	Minor	The teacher has an alternative program to use in case of denial of Net Meeting availability. It can take him 1 hour to install the alternative program. This alternative program is freeware and costs nothing for the teacher TCR = 300 + 0 = 300 NOK CP = (300/39600)*100 = 0,75%

Table 5.33: Private Lessons Consequence table for hardware availability risks

Stakeholder	Asset	Risk			Risk scenario	Consequence value	Consequence description
Teacher	Availability of service	Denial of host Hardware availability	Denial of host storage device availability		The host hard disc doesn't function or malfunction	Catastrophic	The teacher hasn't an alternative hard disc to use. It takes him two days to get a new hard disc and install it along with operating system and application programs. A new hard disc costs 800 NOK. TCR = 3600 + 800 = 4400 NOK CP = (4400/39600)*100 = 11,11%
			Denial of host internal hardware availability	Denial of modem availability	The modem doesn't function or malfunction. As result of it, the teacher's computer can't be connected to the Internet	Moderate	The teacher has an alternative extern modem that he can use in case of denial of the intern modem. The teacher has paid 400 NOK for the extern modem and it takes him 1 hour to install it. TCR = 300 + 400 = 700 NOK CP = (700/39600)*100 = 1,76%

				Denial of network card availability	The network card doesn't function or malfunction. As result of it, the teacher can't be connected to the Internet	Minor	The teacher has an additional network card that he can use in case of denial of the internal network card. He has got this network card free of charge from his friend and it takes him 1 hour to install it. TCR = 300 + 0 = 300 NOK CP = (300/39600)*100 = 0,75%
			Denial of host external hardware availability	Denial of monitor availability	The monitor doesn't function or malfunction	Major	The teacher hasn't an additional monitor. The reparation of monitor takes 5 days. It is more profitable for teacher to buy a new monitor than wait for reparation. The new monitor costs 2000 NOK and it takes the teacher 4 hours to buy a new monitor and install it. TCR = 1200 + 2000 = 3200 NOK CP = (3200/39600)*100 = 8,08%
				Denial of web camera availability	The web camera doesn't function or malfunction	Moderate	The teacher hasn't an additional web camera. The reparation of web camera is too costly. It is more profitable for the teacher to buy a new web camera. The new web camera costs 400 NOK and it takes the teacher 3 hours to buy and install the new web camera. TCR = 900 + 400 = 1300 NOK CP = (1300/39600)*100 = 3,28%
				Denial of speakers availability	Speakers don't function or malfunction	Minor	The teacher has additional speakers that he can use in case of denial of the old speakers. He has got these speakers free of charge from his friend and it takes him 1 hour to install them. TCR = 300 + 0 = 300 NOK CP = (300/39600)*100 = 0,75%

Table 5.34: Private Lessons Consequence table for host security service availability risks

Stakeholder	Asset	Risk		Risk scenario	Consequence value	Consequence description
Teacher	Availability of service	Denial of host security service availability	Lack of firewall – host is attacked from the Internet	The host node is attacked from the Internet	Major	As a result of attack from the Internet the operating system and application programs don't function or malfunction. The teacher has to reinstall the operating system and application programs. It takes him the whole day to reinstall the operating system and all application programs. Additionally he pays 300 Kr for technical support service. TCR = 1800 + 300 = 2100 CP = (2100/39600)*100 = 5,30%

			Lack of antivirus software – host is attacked by computer virus	The host node is attacked by computer virus	Major	As a result of computer virus the operating system and application programs don't function or malfunction. The teacher has to reinstall the operating system and application programs. It takes him the whole day to reinstall the operating system and all application programs. Additionally he pays 300 Kr for technical support service. TCR = 1800 + 300 = 2100 CP = (2100/39600)*100 = 5,30%

Table 5.35: Private Lessons Consequence table for host availability risks

Stakeholder	Asset	Risk		Risk scenario	Consequence value	Consequence description
Teacher	Availability of service	Denial of host availability	Denial of host Software availability	The host software doesn't function or malfunction		The consequence of denial of availabilities of host operating system and application programs Net Meeting and Net Customer
			Denial of host Hardware availability	The host hardware doesn't function or malfunction		The consequence of denial of availabilities of host hard disc, modem, network card, monitor, web camera and speakers.
			Denial of power supply service availability	The local provider of electricity has technical problems and can't provide electricity to the teacher's house	Moderate	The statistic shows that it usually takes no longer then 2 hours for electricity provider to fix technical problems. TCR = 600 + 0 = 600 NOK CP = (600/39600)*100 = 1,51%
			Denial of host security service availability	The host is attacked from the internet and/or by computer virus		The consequence of lack of firewall and antivirus software
			Denial of host authorization availability	The host computer hadn't protection against possible theft or unauthorized access. It is stolen or damaged by criminals	Catastrophic	As a result of theft of computer the teacher has to buy a new computer and install operating system along with application programs. It will take him 2 days to fix the house door, buy a new computer and install an operating system with application programs. The new computer costs 7000 NOK TCR = 3600 + 7000 = 10600 NOK CP = (10600/39600) = 26,76%

Table 5.36: Private Lessons Consequence table for service availability risks

Stakeholder	Asset	Risk		Risk scenario	Consequence value	Consequence description
Teacher	Availability of service	Denial of Service availability	Denial of host availability	The host is not available		The consequence of denial of availabilities of host software, hardware, power supply service, host authorization and security service

			Denial of Network availability	The local Internet provider has technical problems and can’t provide access to the Internet	Moderate	The statistic shows that it usually takes no longer then 4 hours for Internet provider to fix technical problems. TCR = 1200 + 0 = 1200 NOK CP = (1200/39600)*100 = 3,03%
			Denial of Human availability	The teacher is not available because he is ill or absent	Moderate	The statistic provided by the teacher’s doctor shows that in average the teacher was ill no longer than 1 day. TCR = 1800 + 0 = 1800 NOK CP = (1800/39600)*100 = 4,54%

5.4.2 Activity 3.2: Frequency evaluation

The objective of this activity is to evaluate the frequency of risks identified during the risk identification sub-process. The inputs for this activity are risks identified in the fault tree analysis activity. During the frequency evaluation activity, the frequency of the top event in a fault tree is identified by applying the frequencies for the events on the level below the top event. In general, the frequency of an event is identified by applying the frequencies for the events that are on one level below the event of interest.
One can assign frequencies to risks using either qualitative or quantitative frequency values. Quantitative analysis of fault trees uses the minimal cut sets to compute the probability of the top event of a fault tree. A minimal cut set is a minimal set of basis (basic) events that can cause the top event. If all basis events are independent, the probability of a cut set is determined by multiplying together the probability of basis events. The probability of top event in a fault tree with *n* minimal cut sets can be computed with the help of the following formula: $\boldsymbol{1-((1-p_1)*(1-p_2)*....*(1-p_n))}$ where $\boldsymbol{p_1}$ is the probability of cut set 1 and $\boldsymbol{n}$ is the number of cut sets.

Often the basis events are of a qualitative nature. In this case one can use subjective probabilities based on expert judgement. Applying qualitative values, one should consider all the combinations of qualitative values in each cut-set and choose the ones that give the highest contribution to the occurrence probability of the top event. For more information about qualitative analysis we refer to [12].

The frequency values of risks also can be determined with the help of information from previous similar assessments, historical data, available statistic information, subjective assessment of RA-team or experts judgment. The frequency values also can be collected from producers of software and hardware or user support companies that have statistic about the use of particular software or hardware. If RA-team finds it difficult to assign frequency values for some risks, one can use CORAS [5] guidelines for the application of Markov analysis [15] for frequency evaluation.

If risks are organised in fault trees using quantitative values, it is possible to compute automatically the frequency of the top event. As a result of this activity, the frequency values along with their description, stakeholders, assets, risks and risks scenarios should be documented in the frequency table. It is convenient to have one frequency table for each availability aspect. Table 5.37 shows the general form of frequency table and figures A.6, A.7, A.8, A.9 in Appendix A show frequency tables for different availability aspects.

Table 5.37: Frequency table

Stakeholder	Asset	Risk	Risk scenario	Frequency value	Frequency description
<Stakeholder>	<Asset>	<Risk>	<Risk scenario>	<Frequency value>	<Frequency description>

Example. Frequency evaluation: Private Lessons

In the fault trees that we constructed in the fault trees analysis activity, every basis event can be sufficient to cause the root event. That is why we use "OR" ports and the probability of the root event can be computed with the help of the following formula:
$1-((1-p_1)*(1-p_2)*....*(1-p_n))$*** where ***$p_1$ is probability of event 1 and ***n*** is the number of basis events.

The fault trees with identified frequencies of top events are shown in figures below.

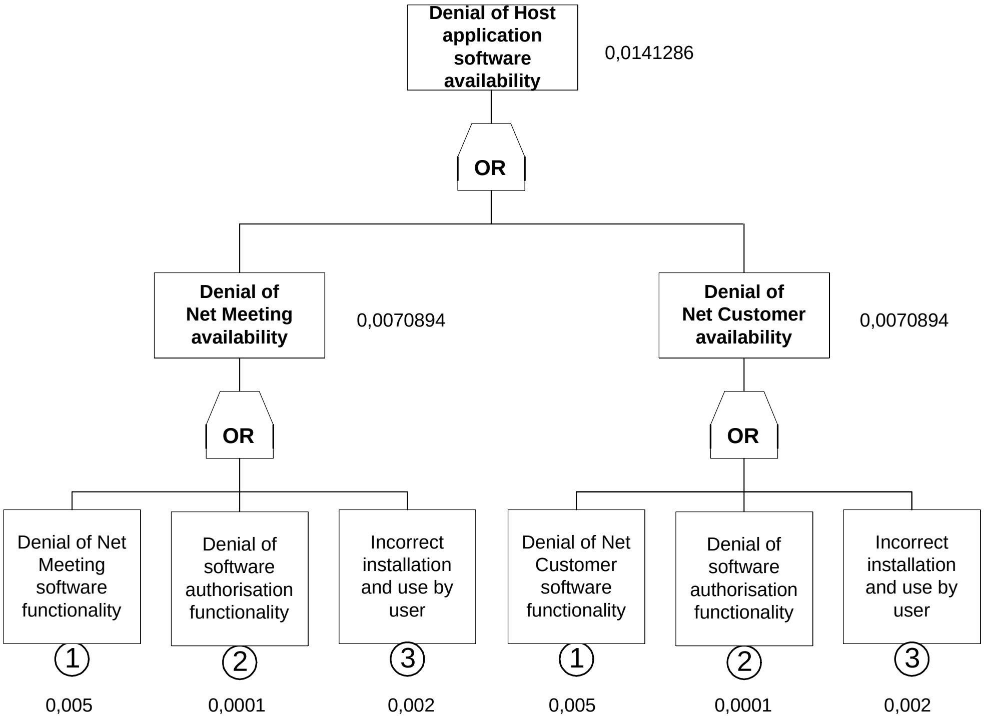

Denial of Host application software availability
0,0141286
OR
Denial of Net Meeting availability
0,0070894
Denial of Net Customer availability
0,0070894
OR
OR
Denial of Net Meeting software functionality
1
0,005
Denial of software authorisation functionality
2
0,0001
Incorrect installation and use by user
3
0,002
Denial of Net Customer software functionality
1
0,005
Denial of software authorisation functionality
2
0,0001
Incorrect installation and use by user
3
0,002

Figure 5.19: Determination of frequency for the denial of host application software availability

Figure 5.19 shows the fault tree with the probability of top event *Denial of host application software availability* that was determined by computing the probabilities of risks *Denial of Net Meeting availability* and *Denial of Net Customer availability*. The probabilities of these risks were determined by computing the probabilities of basis events on the lowest level of the relevant fault tree. The probabilities of these basis events were collected from the producers of application software and user support companies that have statistic about the use of particular software.

Figure 5.20 shows the fault tree with the probability of top event *Denial of host operating system availability*. The probabilities of basis events: *Denial of operating system functionality*, *Denial of operating system authorization functionality* and *Incorrect installation and use of operating system by user*, were collected from the user support company used by the teacher.

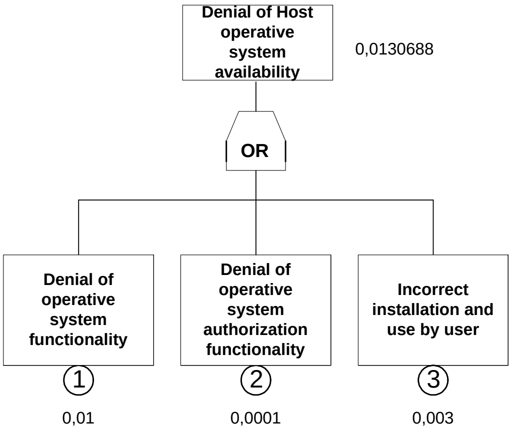

Denial of Host operative system availability
0,0130688
OR
Denial of operative system functionality
Denial of operative system authorization functionality
Incorrect installation and use by user
1
2
3
0,01
0,0001
0,003

Figure 5.20: Determination of frequency for the denial of host operating system availability

Figure 5.21 shows the fault tree with the probability of top event *Denial of host internal hardware availability* that was determined by computing the probabilities of risks *Denial of IDSL modem availability* and *Denial of network card availability.* The probabilities of these two risks are determined by computing the probabilities of basis events depicted on the lowest level in the fault tree. The probabilities of basis events were collected from the user support company used by the teacher.

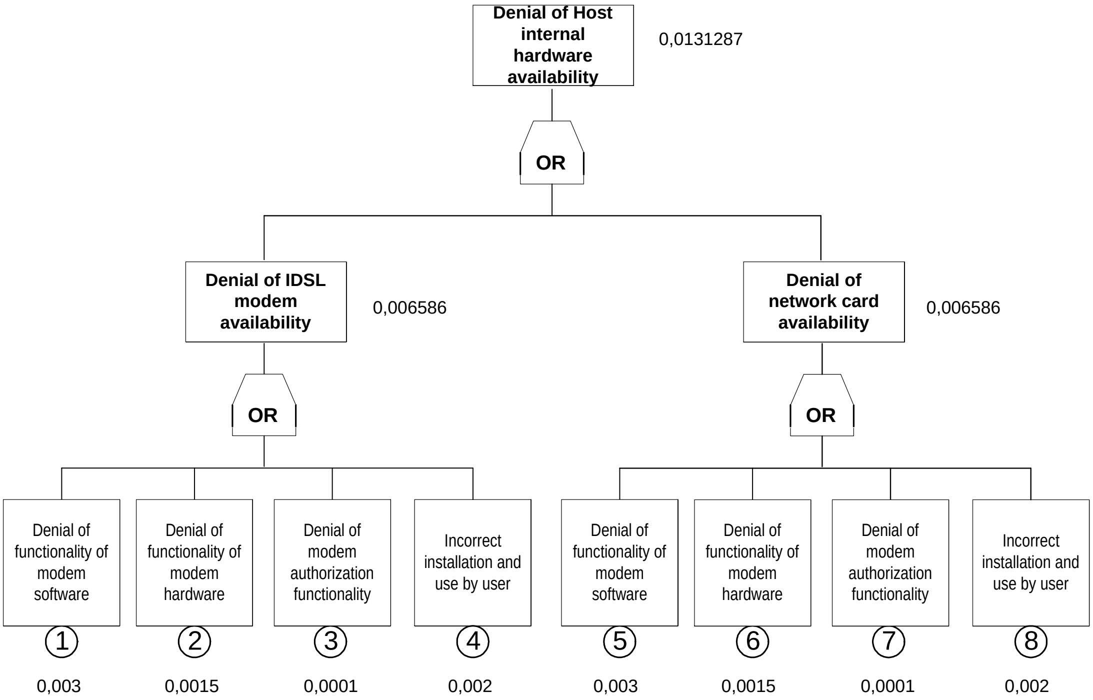

Denial of Host internal hardware availability
0,0131287
OR
Denial of IDSL modem availability
0,006586
Denial of network card availability
0,006586
OR
OR
Denial of functionality of modem software
Denial of functionality of modem hardware
Denial of modem authorization functionality
Incorrect installation and use by user
Denial of functionality of modem software
Denial of functionality of modem hardware
Denial of modem authorization functionality
Incorrect installation and use by user
1
2
3
4
5
6
7
8
0,003
0,0015
0,0001
0,002
0,003
0,0015
0,0001
0,002

Figure 5.21: Determination of frequency for the denial of host internal hardware availability

Figure 5.22 shows the fault tree with the probability of top event *Denial of host external hardware availability* that was determined by computing the probabilities of risks *Denial of web camera availability, Denial of monitor availability* and *Denial of speakers availability.* The probabilities of these risks are determined by computing the probabilities of basis events depicted on the lowest level in fault tree. The probabilities of basis events were collected from the user support company used by the teacher.

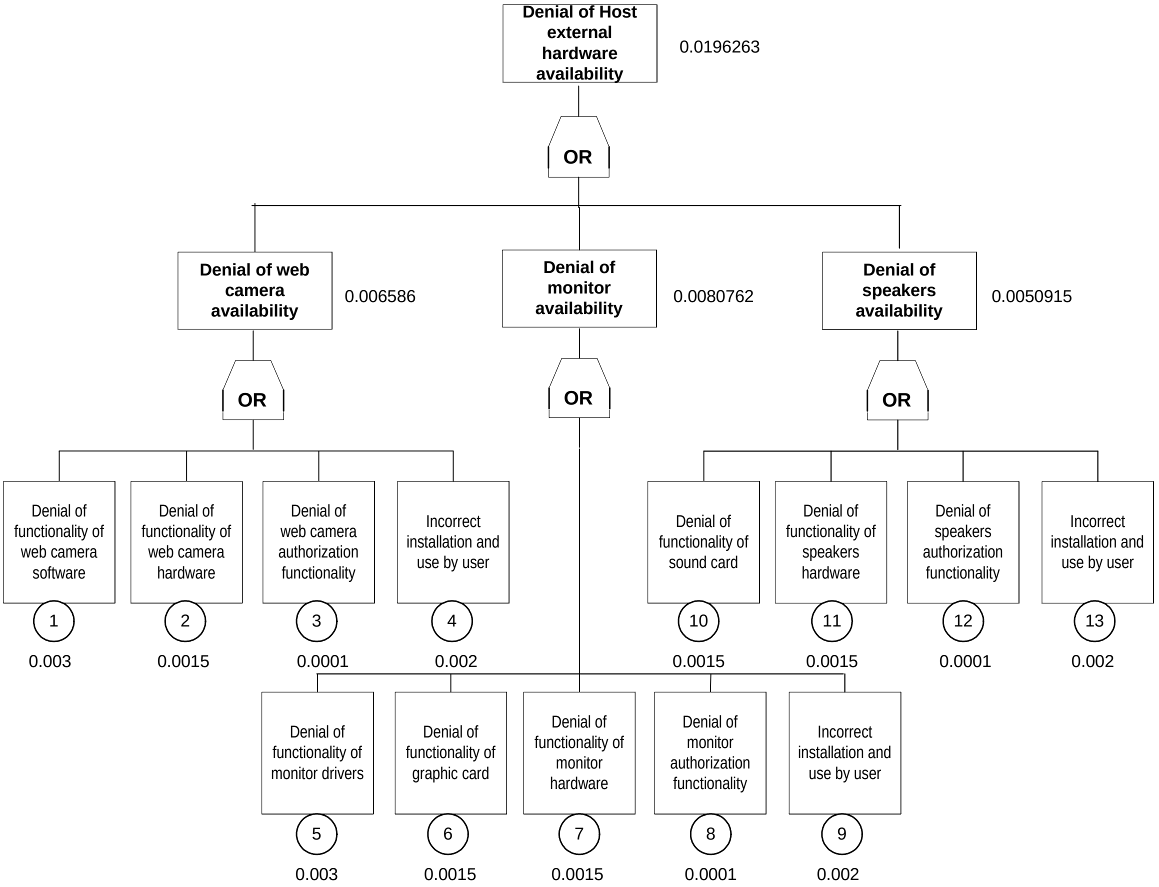

Denial of Host external hardware availability
0.0196263
OR
Denial of web camera availability
0.006586
Denial of monitor availability
0.0080762
Denial of speakers availability
0.0050915
OR
OR
OR
Denial of functionality of web camera software
1
0.003
Denial of functionality of web camera hardware
2
0.0015
Denial of web camera authorization functionality
3
0.0001
Incorrect installation and use by user
4
0.002
Denial of functionality of sound card
10
0.0015
Denial of functionality of speakers hardware
11
0.0015
Denial of speakers authorization functionality
12
0.0001
Incorrect installation and use by user
13
0.002
Denial of functionality of monitor drivers
5
0.003
Denial of functionality of graphic card
6
0.0015
Denial of functionality of monitor hardware
7
0.0015
Denial of monitor authorization functionality
8
0.0001
Incorrect installation and use by user
9
0.002

Figure 5.22: Determination of frequency for the denial of host external hardware availability

Figure 5.23 shows the fault tree with the probability of top event *Denial of host security service availability* that was determined by computing the probabilities of risks *Denial of security service due to firewall problems* and *Denial of security service due to antivirus software problems*. The teacher has neither firewall nor antivirus software. That is why the probabilities of risks on the second level of fault tree were determined by computing the probabilities of risks *Lack of firewall* and *Lack of antivirus software.* The probabilities of these basis events were determined by analysing statistical information that shows percentage of personal computers attacked from the Internet or affected by virus.

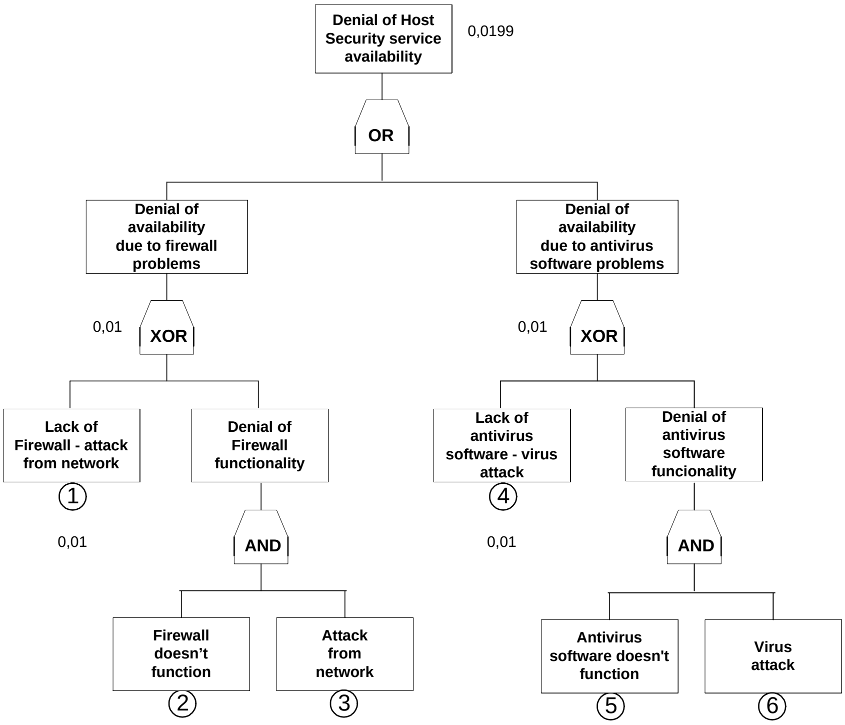

Denial of Host Security service availability
0,0199
OR
Denial of availability due to firewall problems
Denial of availability due to antivirus software problems
0,01
XOR
0,01
XOR
Lack of Firewall - attack from network
1
Denial of Firewall functionality
Lack of antivirus software - virus attack
4
Denial of antivirus software funcionality
0,01
AND
0,01
AND
Firewall doesn't function
2
Attack from network
3
Antivirus software doesn't function
5
Virus attack
6

Figure 5.23: Determination of frequency for the denial of host security service availability

We have now enough information to determine the frequency of risk *Denial of host node availability* shown in Figure 5.24. The frequency of risk *Denial of power supply service availability* was collected from the local power supply company. The frequency of risk *Denial of host authorization availability* was determined by analysing the information provided by the local police office. This information shows statistic about the number of burglaries in the teacher's house area and we decided to assign the frequency value to be equal the probability of housebreaking in the teacher's house.

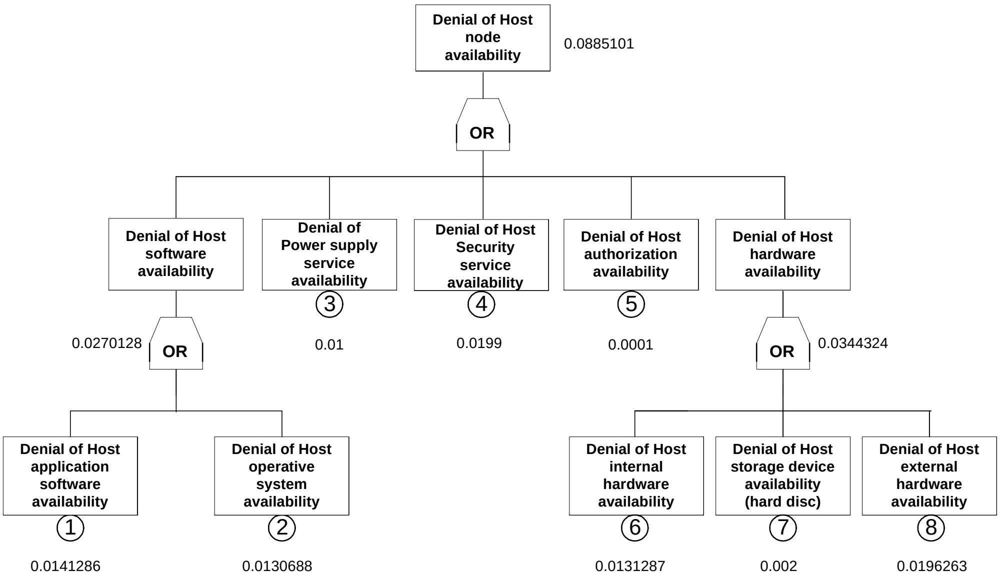

Denial of Host node availability
0.0885101
OR
Denial of Host software availability
Denial of Power supply service availability
Denial of Host Security service availability
Denial of Host authorization availability
Denial of Host hardware availability
0.0270128
OR
3
0.01
4
0.0199
5
0.0001
OR
0.0344324
Denial of Host application software availability
1
0.0141286
Denial of Host operative system availability
2
0.0130688
Denial of Host internal hardware availability
6
0.0131287
Denial of Host storage device availability (hard disc)
7
0.002
Denial of Host external hardware availability
8
0.0196263

Figure 5.24: Determination of frequency for the denial of host node availability

Now we can determine the frequency of risk *Denial of Service availability.*
Figure 5.25 shows the relevant fault tree where the probability of top event was determined by computing the probabilities of risks *Denial of host node availability, Denial of Network availability* and *Denial of human availability.* The probability of denial of the Internet connection was collected from the Internet provider. The teacher himself provided the probability that the service will not be available because of his absence or illness.

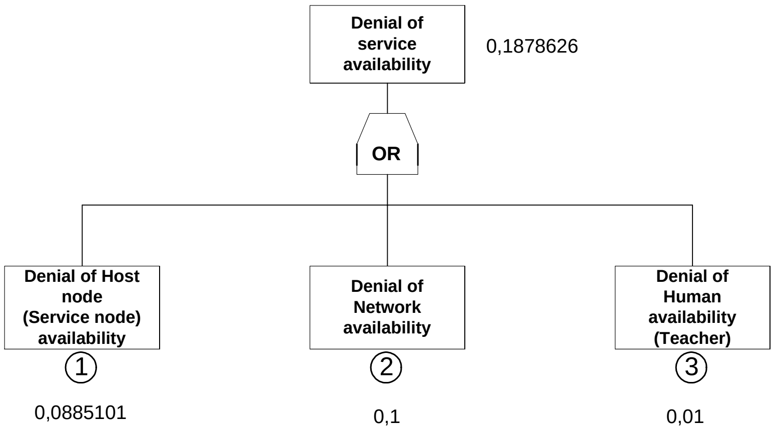

Denial of service availability
0,1878626
OR
Denial of Host node (Service node) availability
1
0,0885101
Denial of Network availability
2
0,1
Denial of Human availability (Teacher)
3
0,01

Figure 5.25: Determination of frequency for the denial of service availability

The identified frequencies of top events in fault trees are documented in the frequency tables shown in figures below.

Table 5.38: Private Lessons Frequency table for software availability risks

Stakeholder	Asset	Risk			Risk scenario	Frequency value	Frequency description
Teacher	Availability of service	Denial of host Software availability	Denial of host operating system availability		The host operating system doesn’t function or malfunction	0,0130688	The frequencies of risks that cause the denial of host operating system, were collected from the user support company used by the teacher
			Denial of host application software availability	Denial of Net Meeting availability	Net Meeting doesn’t function or malfunction	0,0070894	The frequencies of risks that cause the denial of Net Meeting, were collected from the user support company used by the teacher
				Denial of Net Customer availability	Net Customer doesn’t function or malfunction	0,0070894	The frequencies of risks that cause the denial of Net Customer were collected from the user support company used by the teacher

Table 5.39: Private Lessons Frequency table for hardware availability risks

Stakeholder	Asset	Risk		Risk scenario	Frequency value	Frequency description
Teacher	Availability of service	Denial of host Hardware availability	Denial of host storage device availability	The host hard disc doesn’t function or malfunction	0,002	The frequency is defined by analysing statistical information from a technical support company

			Denial of host internal hardware availability	Denial of modem availability	The modem doesn't function or malfunction. As result of it, the teacher's computer can't be connected to the Internet	0,006586	The frequencies of risks that cause the denial of modem were collected from the user support company used by the teacher
				Denial of network card availability	The network card doesn't function or malfunction. As result of it, computer can't be connected to the Internet	0,006586	The frequencies of risks that cause the denial of network card were collected from the user support company used by the teacher
			Denial of host external hardware availability	Denial of monitor availability	The monitor doesn't function or malfunction	0,0080762	The frequency is defined by analysing statistical information from a technical support company
				Denial of web camera availability	The web camera doesn't function or malfunction	0,006586	The frequency is defined by analysing statistical information from a technical support company
				Denial of speakers availability	Speakers don't function or malfunction	0,0050915	The frequency is defined by analysing statistical information from a technical support company

Table 5.40: Private Lessons Frequency table for host security service availability risks

Stakeholder	Asset	Risk		Risk scenario	Frequency value	Frequency description
Teacher	Availability of service	Denial of host security service availability	Lack of firewall – host is attacked from the Internet	The host node is attacked from the Internet	0,01	The probability is determined by analysing statistical information that shows percentage of personal computers attacked from the Internet
			Lack of antivirus software – host is attacked by computer virus	The host node is attacked by computer virus	0,01	The probability is determined by analysing statistical information that shows percentage of personal computers attacked by computer virus

Table 5.41: Private Lessons Frequency table for host availability risks

Stakeholder	Asset	Risk		Risk scenario	Frequency value	Frequency description
Teacher	Availability of service	Denial of host availability	Denial of host Software availability	The host software doesn't function or malfunction	0,0270128	The frequency is defined by determine the frequency of denial of availabilities of operating system and application programs Net Meeting and Net Customer
			Denial of host Hardware availability	The host hardware doesn't function or malfunction	0,0344324	The frequency is defined by determine the frequency of denial of availabilities of host hard disc, host internal and external hardware

			Denial of power supply service availability	The local provider of electricity has technical problems and can't provide electricity to the teacher's house	0,01	The probability is determined by analysing statistical information provided by the local electricity provider
			Denial of host security service availability	The host is attacked from the internet and/or by computer virus	0,0199	The probability is determined by analysing statistical information that shows percentage of personal computers attacked from the Internet or by computer virus
			Denial of host authorization availability	The host computer hadn't protection against possible theft or unauthorized access. It is stolen or damaged by criminals (plotters	0,0001	The probability is determined by analysing statistical information provided by the local police office

Table 5.42: Private Lessons Frequency table for service availability risks

Stakeholder	Asset	Risk		Risk scenario	Frequency value	Frequency description
Teacher	Availability of service	Denial of Service availability	Denial of host availability	The host is not available	0,0885101	The frequency is determined by computing the frequencies of the following risks: - Denial of host software availability - Denial of host hardware availability - Denial of host power supply service availability - Denial of host security service availability - Denial of host authorization availability
			Denial of Network availability	The local Internet provider has technical problems and can't provide access to the Internet	0,1	The probability is determined by analysing statistical information provided by the local Internet provider
			Denial of Human availability	The teacher is not available because he is ill or absent	0,01	The frequency is provided by the teacher himself.

5.5 Risk evaluation

The objective of the risk evaluation sub-process is to determine the levels of availability risks, categorise risks into risk treatment categories and assign priority for each risk and risk treatment category. The risk evaluation sub-process consists of four activities that will typically be carried out in a sequential order:

- Identification of risks values
- Update of risks values
- Categorisation of risks into risk treatment categories
- Specification of priorities of risk treatment categories

5.5.1 Activity 4.1: Identification of risks values

The objective of this activity is to determine the risk value for each risk. The risk value is an estimate of risk severity deduced from the consequence value and the frequency value.

To assign the risk values, one should use the rules for determining the risk values from the consequence and frequency values that have been identified during Activity 1.1. The rules for assigning the risk values may be displayed in one or more Risk Matrix (Table 5.13 Activity 1.1).

The following approaches may be used for the determination of risk values of risks that have consequence and frequency values of the same or different domains:

- If both values are quantitative, they should be multiplied [6].
- If one of quantitative values equals 0, the risk may be assigned a risk value by the relevant stakeholder.
- If both values are qualitative, the Risk Matrix may be applied directly.
- If one of the values is quantitative, this value has to be mapped to its qualitative equivalent before the Risk Matrix may be applied:
    - A quantitative consequence value should be mapped in the Consequence values table (Table 5.12) to its qualitative equivalent.
    - A quantitative frequency value should be mapped in the Frequency values table (Table 5.8) to its qualitative equivalent.

As a result of this activity, the Risks levels table shown in Table 5.43 should be constructed and document all risks along with their consequence, likelihood (frequency) and risk values.

Table 5.43: Risks levels table

Stakeholder	Asset	Risk	Consequence Value	Frequency Value	Risk Value
<..>	<..>	<..>	<..>	<..>	<..>

***Example.* Identification of risks values: Private Lessons**

Table 5.44 documents all risks along with their identified risk values. For the identification of risk values we applied the Risk Matrix (Table 5.13)

Table 5.44: Private Lessons Risks levels table

Stakeholder	Asset	Risk			Consequence Value	Frequency Value	Risk Value
Teacher	Availability of service	Denial of host software availability	Denial of host operating system availability		Major	Unlikely	Moderate
			Denial of host application software availability	Denial of Net Meeting availability	Major	Rare	Low
				Denial of Net Customer availability	Minor	Rare	No risk
		Denial of host Hardware availability	Denial of host storage device availability		Catastrophic	Rare	Moderate
			Denial of host internal hardware availability	Denial of modem availability	Moderate	Rare	Low
				Denial of network card availability	Minor	Rare	No risk
			Denial of host external hardware availability	Denial of monitor availability	Major	Rare	Low
				Denial of web camera availability	Moderate	Rare	Low
				Denial of speakers availability	Minor	Rare	No risk
		Denial of host security service availability	Lack of firewall – host is attacked from the Internet		Major	Unlikely	Moderate
			Lack of antivirus software – host is attacked by computer virus		Major	Unlikely	Moderate
		Denial of host power supply service availability			Moderate	Unlikely	Low
		Denial of host authorization availability			Catastrophic	Rare	Moderate
		Denial of network availability			Moderate	Possible	Moderate
		Denial of human availability			Moderate	Unlikely	Low

5.5.2 Activity 4.2: Update of risks values

The objective of this activity is to update risks values in order to eliminate risks that have acceptable risk values.

The procedure for this activity is the following:

- For each risk compare the risk value (and possible the consequence and frequency values) with the risk evaluation criteria and conclude weather a risk is accepted or not.

- If a risk is accepted, the risk value should be changed to “accepted”, and the risk will not be evaluated further. If a risk is not accepted, the risk value remains the same.
- Updated risk values should be documented in the Updated risk levels table shown in Table 5.45.

Table 5.45: Updated risk levels table

Stakeholder	Asset	Risk	Consequence Value	Frequency Value	Updated Risk Value
<..>	<..>	<..>	<..>	<..>	<..>

Example. Update of risks values: Private Lessons

We compared the risk values documented in the Risk levels table (Table 5.44) with the risk evaluation criteria and documented updated risk values in Table 5.46. As you can see from the table, we accepted all risks that have risk value less than “Moderate.”

Table 5.46: Private Lessons Updated risk levels table

Stakeholder	Asset	Risk			Consequence Value	Frequency Value	Updated Risk Value
Teacher	Availability of service	Denial of host software availability	Denial of host operating system availability		Major	Unlikely	Moderate
			Denial of host application software availability	Denial of Net Meeting availability	Major	Rare	Accepted
				Denial of Net Customer availability	Minor	Rare	Accepted
		Denial of host Hardware availability	Denial of host storage device availability		Catastrophic	Rare	Moderate
			Denial of host internal hardware availability	Denial of modem availability	Moderate	Rare	Accepted
				Denial of network card availability	Minor	Rare	Accepted
			Denial of host external hardware availability	Denial of monitor availability	Major	Rare	Accepted
				Denial of web camera availability	Moderate	Rare	Accepted
				Denial of speakers availability	Minor	Rare	Accepted
		Denial of host security service availability	Lack of firewall – host is attacked from the Internet		Major	Unlikely	Moderate
			Lack of antivirus software – host is attacked by computer virus		Major	Unlikely	Moderate
		Denial of host power supply service availability			Moderate	Unlikely	Accepted

		Denial of host authorization availability	Catastrophic	Rare	Moderate
		Denial of network availability	Moderate	Possible	Moderate
		Denial of human availability	Moderate	Unlikely	Accepted

5.5.3 Activity 4.3: Categorisation of risks into risk treatment categories

The objective of this activity is to organise risks into risk treatment categories to make the risk treatment more effective.

The procedure for this activity is the following:

- Identify the risk treatment categories and document them in the first column of the Risk treatment categories table (Table 5.47).
- For each non-accepted risk identify the risk treatment category the risk belongs to, and document it in the second column of the Risk treatment categories table.

Risks that can affect each availability aspect category may require different treatment options and approaches. That is why the risk treatment categories may be selected on the basis of availability aspect categories. Propose for the risk treatment categories is given in the Possible risk treatment categories table shown in Table 5.48.

Table 5.47: Risk treatment categories table

Risk Treatment Category	Risks
<Category>	<List of risks>

Table 5.48: Possible risk treatment categories

Risk Treatment Category
1. Host (Node) operating system availability risks 2. Host (Node) application software availability risks 3. Host (Node) storage device availability risks 4. Host (Node) hardware availability risks 5. Host (Node) security service availability risks (firewall) 6. Host (Node) security service availability risks (antivirus software) 7. Host (Node) power supply service availability risks 8. Host (Node) authorization availability risks 9. Network availability risks (for network consumer) 10. Network availability risks (for network provider) 11. Human availability risks

***Example.* Categorisation of risks into risk treatment categories: Private Lessons**

The categorization of risks into risk treatment categories is shown in Table 5.49.

Table 5.49: Private Lessons Risk treatment categories table

Risk Treatment Category	Risks
Host operating system availability risks	1. Denial of host operating system availability
Host storage device availability risks	1. Denial of host hard disk availability
Host security service availability risks (firewall)	1. Lack of firewall – host is attacked from the Internet
Host security service availability risks (antivirus software)	1. Lack of antivirus software – host is attacked by a computer virus
Host authorization availability risks	1. Denial of host authorization availability
Network availability risks (for network consumer)	1. Denial of Network availability

5.5.4 Activity 4.4: Specification of priorities of risk treatment categories

The objective of this activity is to specify priorities of risk treatment categories. The priority should be based on the level of risk treatment category value. The risk treatment category value should be assigned for each risk treatment category and documented along with the risk treatment category priority in the Risk treatment category priority table shown in Table 5.50. It is convenient to have the Risk treatment category priority table sorted by priority.

The risk treatment category value can be calculated in different ways:

- *The maximum risk value*. The risk treatment category value is assigned the maximum risk value of its risks.
- *The total risk value*. The risk treatment category value is the sum of the risk values of all the risks included in this risk treatment category:
- If the risk values are quantitative, a calculation can be done directly.
- If the risk values are qualitative, before a calculation they have to be assigned numeric values according to the agreed scale (e.g. no risk (N) = 0; extreme risk (E) = 4;).
- *The average risk value*. The risk treatment category value is the average of the risk values of all the risks included in this risk treatment category. The qualitative values should be assigned numeric values before a calculation.
- *The highest risk value*. The risk treatment category value consists of two elements:
  - The highest risk value represented in this risk treatment category.
  - The number of risks with the highest risk level.

Table 5.50: Risk treatment category priority table

Risk Treatment Category	Risks	Risk Treatment Category Value	Risk Treatment Category Priority
<Category>	<List of risks>	<Value>	<Priority>

Example. Specification of priorities of risk treatment categories: Private Lessons

We decided to use the *highest risk value approach* to define values of risk treatment categories. The identified values and priorities of risk treatment categories are shown in Table 5.51. The risk treatment category value consists of two elements: a letter that denotes the highest risk value represented in this category and the number of risks with the highest risk level. In our case all risk treatment categories have the same priority.

Table 5.51: Private Lessons Risk treatment category priority table

Risk Treatment Category	Risks	Risk Treatment Category Value	Risk Treatment Category Priority
Host operating system availability risks	1. Denial of host operating system availability	M1	1
Host storage device availability risks	1. Denial of host storage device availability	M1	1
Host security service availability risks (firewall)	1. Lack of firewall – host is attacked from the Internet	M1	1
Host security service availability risks (antivirus software)	1. Lack of antivirus software – host is attacked by a computer virus	M1	1
Host authorization availability risks	1. Denial of host authorization availability	M1	1
Network availability risks	1. Denial of Network availability	M1	1

5.6 Risk treatment

The objective of the risk treatment sub-process is to define treatment approaches and treatment options along with treatment actions within each treatment option for each risk within each risk treatment category. In the final phase of this sub-process, the treatment actions should be prioritised based on their costs and benefits. The Risk treatment sub-process consists of two activities that will typically be carried out in a sequential order:

- Identification of treatment options
- Specification of risks treatment priorities

5.6.1 Activity 5.1: Identification of treatment options

The objective of this activity is to define treatment approaches and treatment options along with treatment actions (see Figure 5.26) within each treatment option for each risk within each treatment category identified during the Risk evaluation sub-process.
For each risk treatment category, one or several of the following treatment approaches can be considered [6]:

a) Risk avoidance
b) Reduction of likelihood
c) Reduction of consequences
d) Risk transfer
e) Risk retention

Organizational assets should be protected and companies should use *security policies* to provide the baseline from which the fundamental principles of system and assets protection are defined. For example, you can reduce the risk of unauthorized access to a building by defining in the security policy that the access to building should be controlled not only by clerk but also by electronic door lock.
But knowledge of security policy is not enough to provide the effective treatment of possible risks. You should know the system architecture, in other words how system components interact with each other. By making changes in system architecture, you can either increase or decrease the system availability. For example, you can reduce the possibility of denial of system availability by installing a firewall to protect your system against network attacks. When you install a firewall, you change your system architecture or in other words, you *redesign the system* (You implement the *new design of the system*).

Along with system architecture, you should also consider how well the functionality of system components conforms to components specification and whether the probability of risks to these components has changed. While *testing* of components can help you to define that system components are functioning correctly, a *monitoring* can help you to decide whether or not some particular risks are becoming more or less probable. For example, a network administrator can test network equipment to be sure that it works correctly, and he can install a program for monitoring network traffic that will notify him about increased network traffic (it can affect the functionality of network equipment) or link state changes.

Within each of the chosen treatment approaches, treatment may involve different treatment options. Consideration of different treatment options may help us to look at the risk treatment from different perspectives and in this way increase the number of possible solutions. Thus, if we consider *Revising the security policy* as a treatment option, a security policy can be changed to not allow the use of a critical system component (risk avoidance) or security policy can specify that financial consequences of denial of component availability should be covered by insurance (risk transfer). You can write requirement in security policy that only competent users (certified users) can use this component (reduction of likelihood) or you can specify that recovery from denial of component availability should be done only by specialized company (reduction of consequence).

Considering *Redesigning system* as a treatment option, we can decide to avoid all potential single points of failure through redundancy of critical components (reduction of likelihood) or we can specify that critical components should not be connected to the Internet (risk avoidance). We can reduce the consequence of localized physical disasters by physical separation of critical system components (reduction of consequence) or we can decide to lease parts of the network with critical components to another network provider (risk transfer).

Considering *Strategies for testing* as a treatment option, we can decide to test regularly this critical system component and in this way reduce the likelihood of denial of component availability (reduction of likelihood) or regularly test the functionality of additional component and in this way insure possibility for replacement of critical component (reduction of consequence).

If we consider *Strategies for monitoring* as a treatment option, we can decide to install software for monitoring of functionality of critical system component (reduction of likelihood) or monitoring of functionality of additional system component (reduction of consequence)
Thus, within each treatment approach, one or several of the following treatment options can be considered:

1) Revising the security policy
2) Redesigning the system
3) Strategies for testing
4) Strategies for monitoring

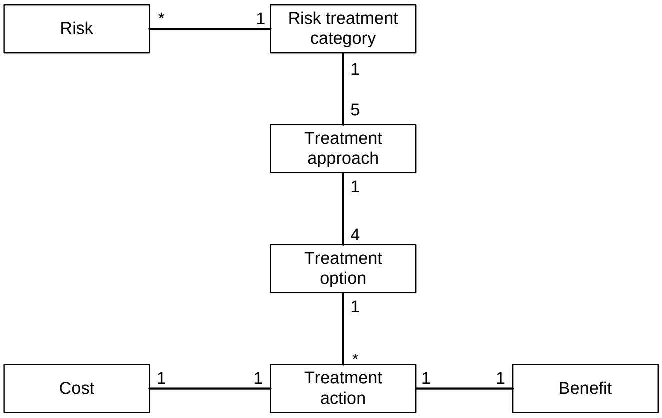


Figure 5.26: Risk treatment

Figure 5.26 shows graphical representation of risk treatment. As you can see from the figure, each risk belongs to one risk treatment category, while risk treatment category may include many risks. For each risk treatment category we can consider five treatment approaches and four treatment options within each treatment approach. Within each treatment option we can consider different treatment actions where each of them has cost and benefit.

For the identification of treatment options and treatment actions within each treatment option, one can use *Templates for risk treatment* that are shown in Appendix B. The identified treatment options and treatment actions have to be documented in the risk treatment tables that should be constructed for each risk treatment category. Templates for risk treatment and risk treatment tables play different roles in this activity. Templates for risk treatment should facilitate communication among stakeholders and assist them in the identification of treatment options and treatment actions within each treatment option. Risk treatment tables should be used to document identified risk treatment options and treatment actions along with treatment actions costs and benefits.

The identification of treatment options activity consists of two steps that will typically be carried out in sequential order:

- For each risk treatment category identify risk treatment options and treatment actions with the help of *Templates for risk treatment* (see Risk treatment templates guide in Figure 5.27):
  For identification of treatment options for risk treatment category:
  - *Host application software availability risks*, use the templates from figures B.1, B.2, B.3.
  - *Host operating system availability risks*, use the templates from figures B.4, B.5, B.6.
  - *Host hardware availability risks*, use the templates from figures B.7, B.8, B.9, B.10.
  - *Host storage device availability risks*, use the templates from figures B.11, B.12, B.13.
  - *Host security service availability risks (firewall)*, use the template from FigureB.14.
  - *Host security service availability risks (antivirus software)*, use the template from FigureB.15.
  - *Host authorization availability risks*, use the template from Figure B.16.
  - *Host power supply service availability risks*, use the template from Figure B.17.
  - *Human availability risks*, use the template from Figure B.18.
  - *Network availability risks (for network provider)*, use the template from Figure B.19.
  - *Network availability risks (for network consumer)*, use the template from Figure B.20.

- For each risk treatment category document identified treatment options and treatment actions in the Risk treatment table shown in Table 5.52.

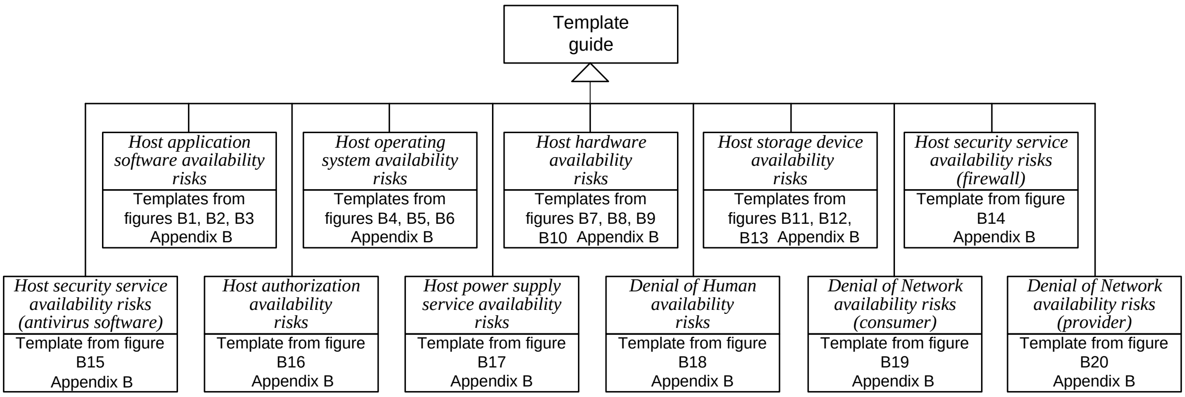

Template guide
Host application software availability risks
Templates from figures B1, B2, B3 Appendix B
Host operating system availability risks
Templates from figures B4, B5, B6 Appendix B
Host hardware availability risks
Templates from figures B7, B8, B9 B10 Appendix B
Host storage device availability risks
Templates from figures B11, B12, B13 Appendix B
Host security service availability risks (firewall)
Template from figure B14 Appendix B
Host security service availability risks (antivirus software)
Template from figure B15 Appendix B
Host authorization availability risks
Template from figure B16 Appendix B
Host power supply service availability risks
Template from figure B17 Appendix B
Denial of Human availability risks
Template from figure B18 Appendix B
Denial of Network availability risks (consumer)
Template from figure B19 Appendix B
Denial of Network availability risks (provider)
Template from figure B20 Appendix B

Figure 5.27: Risk treatment templates guide

Table 5.52: Risk treatment table

ID	Risk	Approach	Treatment Option	Treatment Action	Benefit	Cost
<id>	<risk>	a)	1)	<treatment>	<benefit>	<cost>
			2)			
			3)			
			4)			
		b)	1)			
			2)			
			3)			
			4)			
		c)	1)			
			2)			
			3)			
			4)			
		d)	1)			
			2)			
			3)			
			4)			
		e)	1)			
			2)			
			3)			
			4)			

Figure 5.28 shows the general structure of risk treatment templates. From the figure we can see that to make the treatment of a risk on the highest level, we have to treat risks that can lead to this risk. For example, to treat the risk *Denial of application software availability*, we have to make the treatment of risks: *Denial of application software functionality*, *Denial of application software authorization functionality*, and *Incorrect installation and use of application software*. For each of risks that can lead to the risk on the highest level we constructed template that will facilitate the identification of risk treatment options and risk treatment actions. In each of constructed templates, the treatment actions were defined by considering different treatment approaches (the level 3 in Figure 5.28) and different treatment options within each of treatment approaches (the lowest level in Figure 5.28).

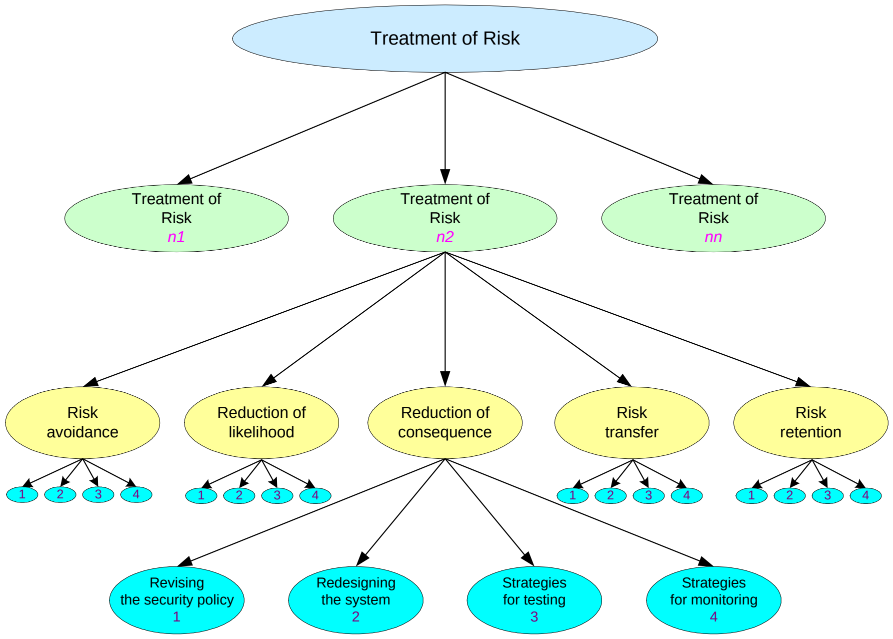


Figure 5.28: General structure of risk treatment templates

***Example.* Identification of treatment options: Private Lessons**

The identified with the help of templates risk treatment options and risk treatment actions are documented in the risk treatment tables shown in figures C.1 – C.6 in Appendix C. The risk treatment tables were constructed for each identified risk treatment category.

5.6.2 Activity 5.2: Specification of risks treatment priorities

The objective of this activity is to define priority among risk treatment actions. The inputs for this activity are the risks with identified risk treatment options and risk treatment actions as well as risk treatment actions costs and benefits that were documented in the risk treatment tables in Activity 5.1. The priority should be defined for each risk treatment action identified for a treatment of a particular risk.

The priority should be based on the level of treatment action value that can be assigned with the help of the Risk treatment action priority matrix chosen in Activity 1.1 (Table 5.15). The identification of treatment action values implies an assignment of values to the benefit and cost of each treatment action. Treatment actions benefits and costs should be assigned values according to the scale chosen in Activity 1.1.

As a result of this activity, the Risk treatment priority table shown in Table 5.53 should be constructed for each risk treatment category and document the costs, benefits and priorities of treatment actions within each risk of treatment category.

Table 5.53: Risk treatment priority table

ID	Risk	Approach	Treatment Option	Treatment Action	Benefit	Cost	Treatment Action Priority
<id>	<risk>	a)	1)	<treatment>	<benefit>	<cost>	<priority>
			2)				
			3)				
			4)				
		b)	1)				
			2)				
			3)				
			4)				
		c)	1)				
			2)				
			3)				
			4)				
		d)	1)				
			2)				
			3)				
			4)				
		e)	1)				
			2)				
			3)				
			4)				

Example. Specification of risks treatment priorities: Private Lessons

First we assigned values for the benefits and costs of all treatment actions. All treatment actions benefits and costs were assigned values according to the following scale: “very low” (VL), “low” (L), “moderate” (M), “high” (H), “very high” (VH). Then, we identified the risk treatment actions priorities with the help of the Risk treatment action priority matrix (Table 5.15). The identified priorities of risk treatment actions are shown in Appendix C, figures C7 – C.12.

6 Using MODA to assess a Chat Service

To evaluate the suitability of MODA we conducted a case study using MODA to assess the availability of a chat service. In this chapter we summarise our experiences from this case study. In particular, we discuss to what extent the success criteria formulated in chapter 3 have been fulfilled.

The chat service AMIGOS [33] is offered by a business company to the public. The intended users of AMIGOS chat service are people who use PDA terminals with Internet access. To use the chat service, the user has to open a chat terminal program on the PDA and type his username and password. When the user successfully logs into the service, he gets access to his private account that contains all relevant information that the user will need in order to interact with other people. The system owner – the business company estimates that the service is used about 30000 hours each month and it charges 1$ for each hour of service usage. The chat service is implemented on two nodes: UnixSuper and UnixSuperDuper. These two nodes and user's PDA communicate through the Internet. Successfully logged in users get access to his or her private account and can choose among different chat rooms. When the user chooses a chat room, the chat window opens on the PDA terminal and he or she can start to chat with other service users.

The purpose of this case study is to check how MODA meets its success criteria, namely:

- Success criterion 1: MODA should target availability in a security context.
- Success criterion 2: MODA should be time efficient.
- Success criterion 3: MODA should be cost effective from a reusability perspective.
- Success criterion 4: MODA should be user friendly assisting its users by providing guidelines, templates and checklists.

We describe the availability risk assessment of AMIGOS chat service in Appendix D. Appendix D is structured into six sections. The first five describe the practical use of corresponding five MODA sub-processes for the availability risk assessment of the chat service. Section D.1 documents the results from the Context identification of the chat service. The Risk identification is presented in section D.2. Section D.3 documents the results from the Risk Analysis. The Risk Evaluation is presented in section D.4. Section D.5 documents the results from the last sub-process, namely Risk Treatment. Section D.6 presents the summary of main conclusions.

This chapter is structured into four sections. Section 6.1 discusses how MODA meets its first success criterion. The second success criterion is discussed in section 6.2. Section 6.3 provides argumentation for how MODA meets its third success criterion. Section 6.4 discusses how MODA meets its fourth success criterion.

6.1 How MODA meets its first success criterion

Based on the experience from the risk assessment of the chat service, we discuss in this section how MODA meets its first success criterion. This section is structured into three sub-sections. Sub-section 6.1.1 presents how MODA supports the fulfilment of the first success criterion. Sub-section 6.1.2 shows how it worked out in the risk assessment of the chat service. The conclusion is presented in sub-section 6.1.3.

Success criterion 1	**MODA should target availability in a security context**

6.1.1 MODA support

To address availability in a security context we define it in MODA as “The property of being accessible and usable upon demand by an authorised entity” [19]. Further, we constructed templates that support the identification and treatment of security risks. For example, in the template for denial of host node availability (Figure 4.15) we define two categories of security risks. Under *Denial of host authorization availability* we consider the probability of events that can cause the denial of host availability because of lack/reduction of Host authorisation availability (e.g. the probability that computer can be stolen or accessed by an unauthorized person). Under *Denial of host security service availability* we consider the probability that the host node will be affected by an attack from the Internet (Network) or by computer virus. We consider these risks on a more detailed level in the template for denial of host security service availability (Figure 4.19).

In the risk evaluation sub-process we suggest to categorize security risks into three risk treatment categories: *Host authorization availability risks*, *Host security service availability risks (firewall)*, and *Host security service availability risks (antivirus software).* Further, we construct templates to support the treatment of risks that belong to these risk treatment categories. For instance, the template in Figure B.14 supports the identification of risk treatment options and risk treatment actions for the risk treatment category *Host security service availability risks (firewall).* The template in Figure B.15 is meant to support the treatment of risks belonging to the risk treatment category *Host security service availability risks (antivirus software).* We suggest risk treatment options and risk treatment actions for the risk treatment category *Host authorization availability risks* in the template shown in Figure B.16.

6.1.2 How it worked out

In the risk identification sub-process we have used the template for denial of host node availability (Figure 4.15) to construct the fault tree (Figure D.2.4) that among other host risks also shows security risks *Denial of host authorization availability* and *Denial of host security service availability*. Further, we have used the template for denial of host security service availability (Figure 4.19) to construct the fault tree (Figure D.2.14) that shows security risks that may affect the PDA availability. The similar trees were constructed for the risks *Denial of host (UnixSuper) security service availability*, and *Denial of host (UnixSuperDuper) security service availability*.

In the risk analysis sub-process we identified the consequences and frequencies of risks that may cause the denial of security service availability and authorization availability of PDA and chat service nodes. The consequence and frequency tables for the host security service availability risks (Tables D.3.3 and D.3.8) were constructed to document the consequences and frequencies of risks that may cause the denial of security service availability of PDA and chat service nodes. Frequencies of these risks were defined in figures D.3.1, D.3.5 and D.3.6. In Figure D.3.1 under *Lack of firewall* we considered the probability that due to the lack of firewall, the network risks (e.g. network attack) may cause the denial of PDA availability. In the same figure under *Lack of antivirus software* we considered the probability that due to the lack of antivirus software, the malicious program or virus may cause the denial of PDA availability. In figures D.3.5 and D.3.6 under *Denial of firewall functionality* we considered the probability that firewall will not protect against risks that may cause the denial of chat service nodes availability. Under *Denial of antivirus software functionality* we considered the probability that antivirus software will not protect against risks (malicious program or virus) that may cause the denial of chat service nodes availability.

In the risk evaluation sub-process we categorised risks with the help of the Possible risk treatment categories table (Table 5.48). Host node security risks were divided into three risk treatment categories (Table D.4.3): *Host authorization availability risks*, *Host security service availability risks (firewall)*, and *Host security service availability risks (antivirus software).*

In the risk treatment sub-process we identified risk treatment options and risk treatment actions for security risks with the help of three templates for risk treatment from appendix B. Templates from figures B.14 (*Lack of firewall/Attack from the network*), B.15 (*Lack of antivirus software/Virus attack*) and B.16 (*Denial of host authorization availability*) were used to define risk treatment options and actions for the corresponding risk treatment categories. The identified treatment options and treatment actions were documented in the risk treatment tables (Tables D.5.3, D.5.4, D.5.5) that were constructed for each risk treatment category.

6.1.3 Conclusion

In this chapter we evaluated how MODA meets its first success criterion. The case study of the chat service shows that MODA targets availability from a security perspective with the help of templates and guidelines. Particularly, it focuses on the most important security risks in templates targeting the identification and treatment of security risks. The case study shows that two templates can be effectively used for the identification of security risks: the template for denial of host node availability (Figure 4.15) and the template for denial of host security service availability (Figure 4.19). With the help of these templates the following five security risks may be identified:

- Denial of host authorization availability
- Lack of firewall/Attack from the network
- Denial of firewall functionality
- Lack of antivirus software/Virus attack
- Denial of antivirus software functionality

Further, with the help of the Possible risk treatment categories table (Table 5.48) these risks can be organized into three risk treatment categories (Table D.4.3). The identification of risk treatment options and risk treatment actions for these risk treatment categories can be done effectively with the help of three templates for risk treatment shown in figures B.14 (*Lack of firewall/Attack from the network*), B.15 (*Lack of antivirus software/Virus attack*) and B.16 (*Denial of host authorization availability*).

Along with the benefits mentioned above, the case study has shown that we have some challenges that are not so simple to resolve. On the one hand, MODA does not address all possible security risks (e.g. Sabotage), and on the other hand security risks that are typical for particular environment, may be defined more effectively by domain experts.

6.2 How MODA meets its second success criterion

In this section we discuss how MODA meets its second success criterion. This section is structured into three sub-sections. Sub-section 6.2.1 presents how MODA supports the fulfilment of the second success criterion. Sub-section 6.2.2 shows how it worked out in the risk assessment of the chat service. The conclusion is presented in sub-section 6.2.3.

Success criterion 2	**MODA should be time efficient**

6.2.1 MODA support

We address time efficiency in MODA by means of guidelines, templates and the predefined set of tables. For example, in the context identification sub-process we define the set of frequency and consequence values (Tables 5.7, 5.9…5.11 and Figure 5.3) to support the rapid identification of the range of frequency and consequence values. Further, in the risk identification sub-process we support the quick construction of fault trees by means of templates for availability risk analysis (Figures 4.15…4.19). In the risk analysis sub-process we facilitate the rapid construction and documentation of consequence and frequency values by means of the predefined set of consequence and frequency tables (Figures A.2…A.9 in Appendix A). To support the quick identification of the risk treatment categories we suggest eleven risk treatment categories in the Possible risk treatment categories table (Table 5.48). In the risk treatment sub-process we support the rapid identification of the risk treatment options and risk treatment actins by means of templates for risk treatment (Figures B.1…B.20 in Appendix B).

6.2.2 How it worked out

In the context identification sub-process the predefined set of frequency values (Table 5.7) helped us in the quick identification of the range of frequency values that were documented in the Frequency values table (Table D.1.1). With the help of Figure 5.3 that shows the categorisation of consequences, we rapidly defined that the consequence values for PDA user should be measured in the impact of service lost time on the user (Table D.1.2). With the help of the Total income consequence values table (Table 5.11) we quickly defined the set of consequence values for the chat service owner (Table D.1.2).

In the risk identification sub-process we quickly constructed fault trees with the help of templates for availability risk analysis. To build the fault trees that have the top events *Denial of host node (PDA) availability*, *Denial of host node (UnixSuper) availability*, and *Denial of host node (UnixSuperDuper) availability*, we have used the template from Figure 4.15. To build the fault trees that have the top event *Denial of host application software availability* (Figures D.2.5, D.2.6, D.2.7) we have used the template from Figure 4.16. To build the fault trees that have the top event *Denial of host operating system availability* (Figures D.2.8, D.2.9, D.2.10) we have used the template from Figure 4.17. To build the fault trees that have the top event *Denial of host hardware availability* (Figures D.2.11, D.2.12, D.2.13) we have used the template from Figure 4.18.

In the risk analysis sub-process the predefined set of consequence and frequency tables (Figures A.2...A.9 in Appendix A) facilitated quick construction and documentation of consequence and frequency values. In the risk evaluation sub-process we identified quickly the risk treatment categories (Table D.4.3) with the help of the Possible risk treatment categories table (Table 5.48).

In the risk treatment sub-process we identified quickly the risk treatment options and risk treatment actions with the help of templates shown in Appendix B. The templates from figures B.4, B.5, and B.6 were used to identify the risk treatment options and actions for the risk treatment category *Host operating system availability risks* (Risk treatment table in Table D.5.1). The templates shown in figures B.8, B.9, and B.10 were used to identify the risk treatment options and actions for the risk treatment category *Host hardware availability risks* (Risk treatment table in Table D.5.2). The template shown in Figure B.16 was used to identify the risk treatment options and actions for the risk treatment category *Host authorization availability risks* (Risk treatment table in Table D.5.3). The risk treatment options and actions for the risk treatment categories *Host security service availability risks (firewall)* and *Host security service availability risks (antivirus software)* were identified with the help of templates shown in figures B.14 and B.15.

6.2.3 Conclusion

In this chapter we evaluated how MODA meets its second success criterion. The case study of the chat service shows that MODA targets time efficiency with the help of templates, guidelines and the predefined set of tables. The specification of the range of consequence and frequency values can be done quickly with the help of the predefined set of frequency and consequence values (Table 5.7, 5.9-5.11, Figure 5.3). In the risk identification sub-process the construction of fault trees can be done rapidly with the help of the templates for availability risk analysis (Figures 4.15…4.19). In the risk analysis sub-process the predefined set of consequence and frequency tables (Figures A.2…A.9 in Appendix A) supports the quick construction and documentation of consequence and frequency values. In the risk evaluation sub-process the risk treatment categories can be quickly identified with the help of the Possible risk treatment categories table (Table 5.48). In the risk treatment sub-process the risk treatment options and risk treatment actions can be identified rapidly with the help of the templates for risk treatment (Figures B.1…B.20 in Appendix B).

These conclusions are all rather subjective, based on the authors experiences and opinions. It is beyond the scope of this thesis to conduct a scientifically satisfactory empirical evaluation.

6.3 How MODA meets its third success criterion

In this section we discuss how MODA meets its third success criterion. This section is structured into three sub-sections. Sub-section 6.3.1 presents how MODA supports the fulfilment of the third success criterion. Sub-section 6.3.2 shows how it worked out in the risk assessment of the chat service. The conclusion is presented in sub-section 6.3.3.

Success criterion 3	**MODA should be cost effective from a reusability perspective**

6.3.1 MODA support

We address cost efficiency in MODA by means of reuse of tables and graphical models. All tables and templates have a clear defined structure and this makes it possible to use modelling tools that may automate some parts of availability assessment. For instance, it is enough to define once the headings of assessment roles and assessment methods tables (Tables 5.3, 5.5), and then produce with the help of modelling tools partially filled assessment methods and assessment roles tables that may be reused in the further availability risk assessments. The tables containing the proposed range of frequency and consequence values (Tables 5.7, 5.9…5.11) may be reused directly. Further, the Risk Matrix (Table 5.13) and the Risk treatment action priority matrix (Table 5.15) may be reused directly to compute the risk values and the priority of treatment actions. We construct the templates for availability risk analysis (Figures 4.15…4.19) in a general manner to support their reusability. We also formulate the risk treatment actions (Figures B.1…B.20 in Appendix B) in a general manner to assist the reuse of the risk treatment tables.

6.3.2 How it worked out

In all sub-processes the availability risk assessment results were documented in tables and graphical models and many of them may be reused in new or current availability risk assessment. In the context identification sub-process the consequence values were documented in the Consequence values table (Table D.1.2) and the frequency values were documented in the Frequency values table (Table D.1.1). These tables as well as the Risk Matrix (Table D.1.4) and the Risk treatment action priority matrix (Table D.1.5) may be reused directly in new or current availability risk assessment.

In the risk identification sub-process the most of templates for availability risk analysis were used directly without changes to construct fault trees. To reuse them in new availability risk analysis we only have to change the name of hardware and software components that were analysed. For example, the fault trees with the top events *Denial of host node availability* (Figure D.2.4) and *Denial of host security service availability* (Figure D.2.14) may be reused without changes, while the fault trees with the top events *Denial of host (PDA) application software availability* (Figure D.2.5) and *Denial of host (PDA) operating system availability* (Figure D.2.8) may be reused by changing the name of host and software components.

In the risk treatment sub-process the risk treatment tables may be reused effectively with possible small changes. To reuse them in new availability risk analysis we only have to decide if we need to change the treatment actions documented in the relevant risk treatment table. Those treatment actions that we decide to keep may be preserved in the risk treatment table along with their benefits and costs. The same approach can be applied to the reuse of treatment priority tables.

6.3.3 Conclusion

In this chapter we evaluated how MODA meets its third success criterion. The case study of the chat service shows that MODA targets cost efficiency by supporting reusability of tables and graphical models. In the context identification sub-process the frequency and consequence tables (Tables D.1.1 and D.1.2) document the agreed range of frequency and consequence values that may be reused in new availability risk analysis. The Risk Matrix (Table 5.13) and the Risk treatment action priority matrix (Table 5.15) also may be reused directly. In the risk identification sub-process the most of templates for availability risk analysis (Figures 4.15…4.19) may be reused directly without changes. Those templates that need changes, may be reused by changing the name of hardware and software components. In the risk treatment sub-process the risk treatment tables and the risk treatment priority tables may be reused with possible small changes.

Along with these positive experiences, the case study has shown that we need means to extract, save and define reusable elements. A database of reusable elements and a computerized tool that manages the construction, extraction and reuse of these elements would be very helpful.

6.4 How MODA meets its fourth success criterion

In this section we discuss how MODA meets its fourth success criterion. This section is structured into three sub-sections. Sub-section 6.4.1 presents how MODA supports the fulfilment of the fourth success criterion. Sub-section 6.4.2 shows how it worked out in the risk assessment of the chat service. The conclusion is presented in sub-section 6.4.3.

Success criterion 4	**MODA should be user friendly assisting its users by providing guidelines, templates and checklists**

6.4.1 MODA support

We address user friendliness in MODA by providing guidelines, templates and checklists. In the context identification sub-process the identification of applied value categories is supported by guidelines and the predefined set of consequence and frequency values (Tables 5.7, 5.9…5.11, Figure 5.3). Further, graphical models (e.g. Domain picture, Use case diagram) should support the communication between people with different background. We support the identification of actors, use cases, assets and the risk acceptance criteria by guidelines and checklists (Figure 5.10). In the risk identification sub-process we support the identification of availability aspect risks and the construction of fault trees by guidelines and templates (Figures 4.15…4.19). In the risk analysis sub-process we support the identification and documentation of consequence and frequency values by guidelines and the predefined set of consequence and frequency tables (Figures A.1…A.10 in Appendix A). In the risk evaluation sub-process we support the identification and update of risk values by guidelines. Further, the Possible risk treatment categories table (Table 5.48) should support the categorisation of risks into risk treatment categories, and the specification of their priorities is supported by guidelines. In the risk treatment sub-process we support the identification of risk treatment actions by graphical templates (Figures B.1…B.20 in Appendix B). The Risk treatment action priority matrix (Table 5.15) should support the identification of priorities of risk treatment actions.

6.4.2 How it worked out

In all sub-processes we were assisted by the set of guidelines, templates and checklists. In the context identification sub-process the range chosen for frequency and consequence values was easily defined with the help of guidelines and the predefined set of consequence and frequency values (Tables 5.7, 5.11, Figure 5.3). Graphical models depicted in Figure D.1.5 (Domain picture) and Figure D.1.6 (Use cases) supported the communication between people with different background participating in the availability risk assessment. In Activity 1.2 we used guidelines to define actors and use cases. The identified actors helped us to define stakeholders of the target system (Table D.1.8). In Activity 1.4 we identified assets with the help of questionnaires (Figure 5.7) and we specified the risk acceptance criteria with the help of checklist (Figure 5.10).

In the risk identification sub-process we identified availability aspects risks with the help of guidelines and documented them in the availability risks tables (Tables D.2.1, D.2.2, D.2.3, D.2.4). The fault tree analysis activity was done easily and quickly with the help of guidelines and templates for availability risk analysis (Figures 4.15, 4.16, 4.17, 4.18, 4.19).

In the risk analysis sub-process the frequency and consequence values were defined with the help of guidelines. The partially filled consequence and frequency tables (Figures A.1, … A.10) facilitated correct and quick construction of these tables for the documentation of results from Activity 3.1 and Activity 3.2.

In the risk evaluation sub-process we defined the risk values (Table D.4.1) with the help of the Risk Matrix (Table 5.13). Further, we updated the risk values (Table D.4.2) with the help of guidelines. The categorisation of risks into risk treatment categories (Table D.4.3) was done easily with the help of the Possible risk treatment categories table (Table 5.48). The specification of priorities of risk treatment categories was performed effectively with the help of guidelines (Table D.4.4).

In the risk treatment sub-process we identified the risk treatment options and risk treatment actions with the help of templates for risk treatment (Figures B.1, …B.20 in Appendix B). These templates are graphical and present the risk treatment options and risk treatment actions in an easy to understand way. This facilitated the rapid and easy identification and documentation of risk treatment actions (Tables D.5.1, …D.5.5). Further, we identified the risk treatment actions priorities with the help of the Risk treatment action priority matrix (Table 5.15).

6.4.3 Conclusion

In this chapter we evaluated how MODA meets its fourth success criterion. The case study of the chat service shows that MODA targets user friendliness by providing in all sub-processes guidelines, templates and checklists. In the context identification sub-process guidelines and the predefined set of consequence and frequency values (Tables 5.7, 5.9…5.11, Figure 5.3) help in the identification of applied value categories. Graphical models (Figures D.1.5, D.1.6) support the communication between stakeholders with different background. Further, the identification of actors, use cases, assets and the risk acceptance criteria is supported by guidelines and checklists (Figure 5.10). In the risk identification sub-process the identification of availability aspects risks and the construction of fault trees are supported by guidelines and templates (Figures 4.15…4.19). In the risk analysis sub-process the identification and documentation of consequence and frequency values is supported by guidelines and the predefined set of consequence and frequency values (Figures A.1…A.10 in Appendix A). In the risk evaluation sub-process the identification and update of risk values as well as the identification of priorities of risk treatment categories are supported by guidelines. The categorization of risks into risk treatment categories is supported by the predefined set of risk treatment categories suggested in the Possible risk treatment categories table (Table 5.48). In the risk treatment sub-process the identification of risk treatment actions is supported by the graphical templates for risk treatment (Figures B.1…B.20 in Appendix B). The Risk treatment action priority matrix (Table 5.15) supports the identification of priorities of risk treatment actions.

Conducting this case study we also felt that we need more help on the practical side with regard to the construction of tables and graphical models and documentation of results.
The use of a specialized computerized tool that effectively manages the construction of tables and diagrams as well as documentation of results would be very helpful.

7 Discussion

During the project work, we faced different challenges that could be solved in different ways. In this chapter we will discuss them and show what could be done different.

Availability aspects

In our project we defined four sub classes of availability:

- Network availability
- Software availability
- Human availability
- Hardware availability

Considering each of the above sub-classes of availability to be one of the links in the availability chain, it is obvious that each of these links must contribute to the overall availability of the system. To insure that important areas are not missed, in the template for Host node availability (Figure 4.15) we also considered aspects that do not belong to any of sub-classes of availability, but in the same time are important for the availability of Host node:

- Power supply service availability
- Host security service availability
- Host authorization availability

We could organise these aspects into fifth sub-class of availability – Environment availability. This sub-class of availability could also contain other aspects such as Lighting service availability, Air Conditioning service availability, and Heating service availability. In the template for Host node availability, all aspects that belong to the Environment service availability could be considered in the fault tree for the Environment service availability. The practicality of this idea is an issue for further research. Figures 7.1 and 7.2 show relevant templates for Environment service availability and Host node availability.

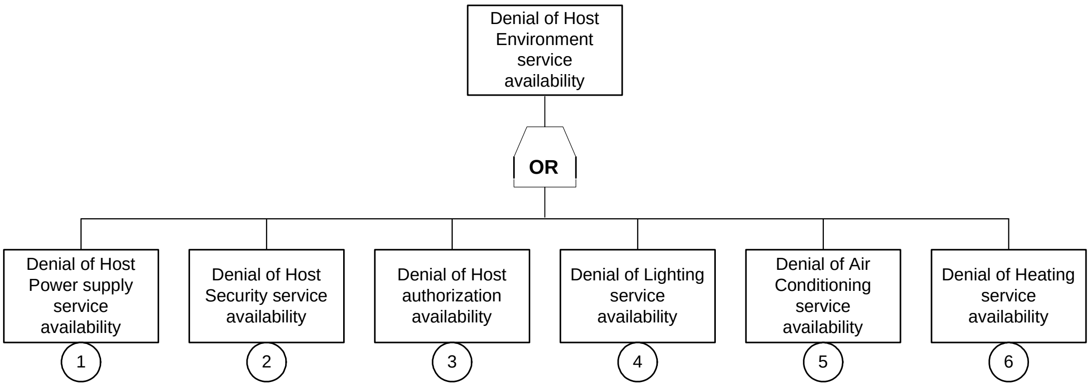

Denial of Host Environment service availability
OR
Denial of Host Power supply service availability
Denial of Host Security service availability
Denial of Host authorization availability
Denial of Lighting service availability
Denial of Air Conditioning service availability
Denial of Heating service availability
1
2
3
4
5
6

Figure 7.1: Template for the assessment of Host Environment service availability

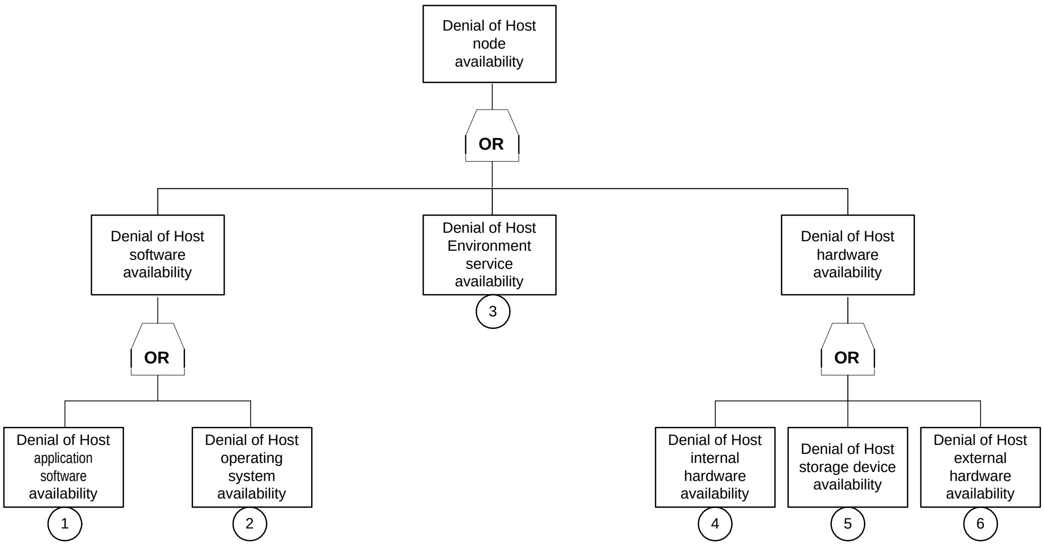

Denial of Host node availability
OR
Denial of Host software availability
Denial of Host Environment service availability
3
Denial of Host hardware availability
OR
OR
Denial of Host application software availability
1
Denial of Host operating system availability
2
Denial of Host internal hardware availability
4
Denial of Host storage device availability
5
Denial of Host external hardware availability
6

Figure 7.2: Template for the assessment of Host node availability

Specification of risk assessment objectives

The objective of this sub-activity of Activity 1.1 is to describe why the risk assessment is undertaken. To facilitate the description of risk assessment objectives we could consider a risk assessment benefits on a system and organization levels and think over how these benefits contribute to the achievement of organization high-level goal. Figure 7.3 shows these ideas.

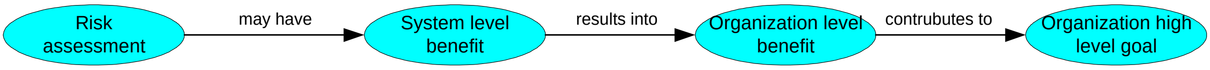


Figure 7.3: Risk assessment contribution to the achievement of high-level goal

The checklists provided in figures 7.4 and 7.5 could be helpful in the identification of system and organization level benefits as well as organization high-level goal. The most of organization level benefits cannot be easily measured in terms of dollars and are called by Hoffer [29] as intangible benefits. The Figure 7.5 shows that an organization level benefit is a sub-class of organization high-level goal. It means that some of organization level benefits can be the organization high-level goal(s).

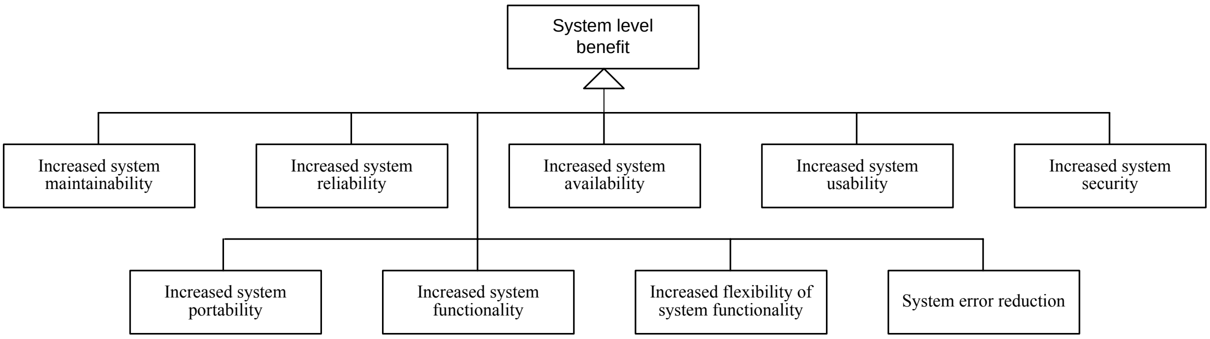

System level benefit
Increased system maintainability
Increased system reliability
Increased system availability
Increased system usability
Increased system security
Increased system portability
Increased system functionality
Increased flexibility of system functionality
System error reduction

Figure 7.4: System level benefits

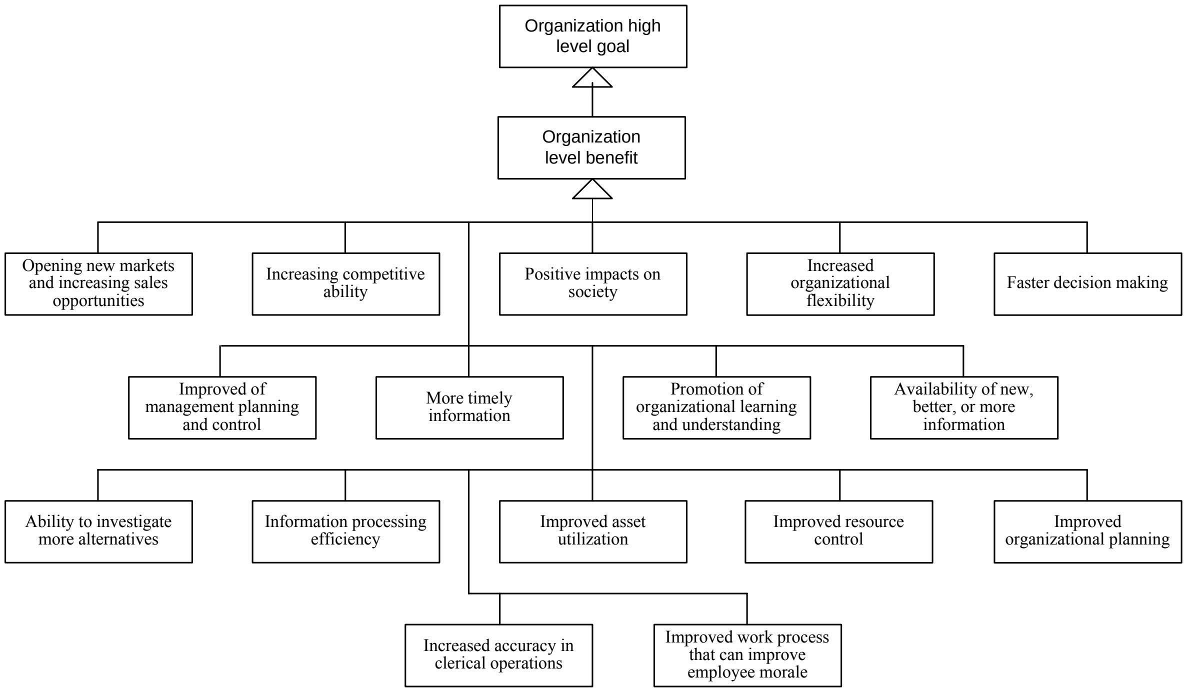

Organization high level goal
Organization level benefit
Opening new markets and increasing sales opportunities
Increasing competitive ability
Positive impacts on society
Increased organizational flexibility
Faster decision making
Improved of management planning and control
More timely information
Promotion of organizational learning and understanding
Availability of new, better, or more information
Ability to investigate more alternatives
Information processing efficiency
Improved asset utilization
Improved resource control
Improved organizational planning
Increased accuracy in clerical operations
Improved work process that can improve employee morale

Figure 7.5: Organization level benefits

The risk assessment objective, organization high level goal, system and organization level benefits could be documented in the Risk assessment objective table shown in Table 7.1. This approach of specification of the risk assessment objectives was not implemented in MODA for two reasons. Firstly, such a detailed guideline is mainly useful for the assessment of data systems that have not assessed so far. For the periodical assessment of information systems these detailed guidelines will be unnecessary. Secondly, in the context identification sub-process we tried to be compatible with CORAS that does not specify risk assessment objectives on a detailed level.

Table 7.1: Risk assessment objective table

Risk assessment objective	System level benefit	Organization level benefit	Organization high level goal
<objective>	<benefit>	<benefit>	<goal>

Risk evaluation

In the activity 4.1 of Risk evaluation sub-process we document identified risks values in the Risk levels table. In the activity 4.2 we document updated risks values in the Updated risk levels table. Instead of using two tables for the documentation of identified risk values and updated risk values, we could add one column in the Risk levels table (Table 7.2) for the documentation of updated risks values. On the one hand the use of one table may contribute to improved time efficiency of the risk assessment. On the other hand the use of two tables may facilitate improved reusability of the risk assessment results.

Table 7.2: Risks levels table (updated)

Stakeholder	Asset	Risk	Consequence Value	Frequency Value	Risk Value	Updated Risk Value
<..>	<..>	<..>	<..>	<..>	<..>	<..>

In the activity 4.3 we could make the categorisation of risks into risk treatment categories more explicit in the Risk treatment categories table shown in Table 7.3. This table could be used to document all identified risks along with their risk treatment categories. On the one hand this table could be quickly filled and on the other hand stakeholders would not have flexibility to define their own risk treatment categories. We decided that flexibility is more important and did not implement this table in MODA.

Table 7.3: Risk treatment categories table

Stakeholder	Asset	Risk			Risk treatment category
<Stakeholder>	<Asset>	Denial of Host (Node) Software availability	Denial of host operating system availability		Host (Node) operating system availability risks
			Denial of Host (Node) application software availability	Denial of availability of <application *n1*>	Host (Node) application software availability risks
				…	
				Denial of availability of <application *nn* >	
		Denial of Host (Node) Hardware availability	Denial of host storage device availability		Host (Node) storage device availability risks
			Denial of Host (Node) internal hardware availability	Denial of availability of <internal hardware *n1*>	Host (Node) hardware availability risks
				…	
				Denial of availability of <internal hardware *nn*>	
			Denial of Host (Node) external hardware availability	Denial of availability of <external hardware *n1*>	
				…	
				Denial of availability of <external hardware *nn*>	
		Denial of Host (Node) security service availability	Lack/Denial of firewall – host is attacked from the Internet		Host (Node) security service availability risks (firewall)
			Lack/Denial of antivirus software – host is attacked by computer virus		Host (Node) security service availability risks (antivirus software)
		Denial of Host (Node) power supply service availability			Host (Node) power supply service availability risks
		Denial of Host (Node) authorization availability			Host (Node) authorization availability risks
		Denial of Network availability (optional)			Network availability risks
		Denial of Human availability (optional)			Human availability risks

Risk treatment

In the Risk treatment sub-process the identification of treatment options could be supported by diagrams that show availability threats and treatment strategies. These diagrams could be a part of UML profile for availability risk assessment and their main purpose will be to facilitate communication and interaction between different groups of stakeholders involved in an availability risk analysis. We did not develop this UML profile because this extends the scope of our project. Figure 7.6 shows some of network threats and strategies to treat these threats.

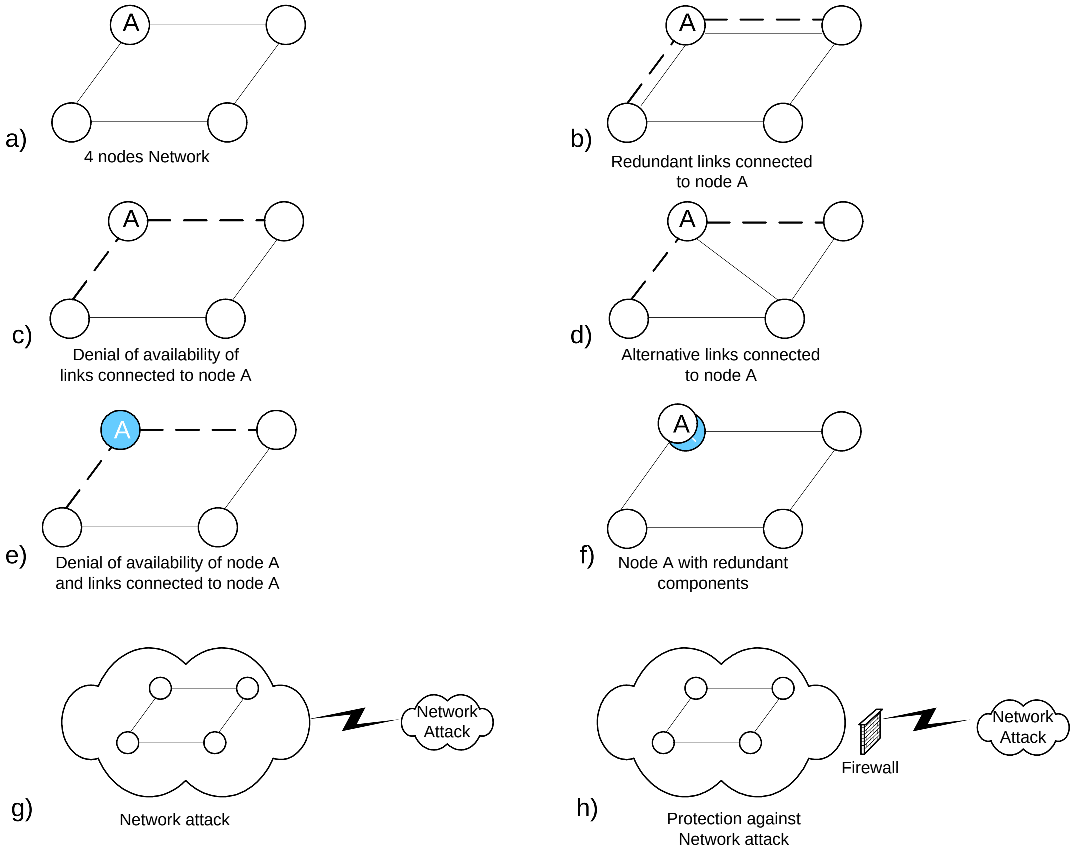

A
a)
4 nodes Network
A
b)
Redundant links connected to node A
A
c)
Denial of availability of links connected to node A
A
d)
Alternative links connected to node A
A
e)
Denial of availability of node A and links connected to node A
A
f)
Node A with redundant components
Network Attack
g)
Network attack
Firewall
Network Attack
h)
Protection against Network attack

Figure 7.6: Network threats and their treatment

As you can see from Figure 7.6, the network threats may be organized into threats that affect network components (Figures c and e) and threats that affect the whole network (Figure g). Among threats to network components we distinguish the denial of network node availability (Figure c) and denial of link connecting two network nodes (Figure e). These threats may be depicted graphically using a broken line to denote the denial of link and using a shadowed circle to denote the denial of network node. Using unbroken line and unpainted circle (Figure a) we depict network lines and nodes that functioning normally. By combing the different types of lines and nodes (Figures b, d, f) we can depict different treatment strategies. Further, we can define special symbols (Figures g, h) that may be used to depict network threats and the protection against these threats.

Figure 7.7 shows the categorisation of availability threats symbols. As you can see, threats to different availability aspects may be depicted using different symbols. Further, these symbols are organized into classes and sub-classes where sub-class inherits the main properties of its super class. For example, the symbols denoting the denial of host hardware availability and host external hardware availability are almost the same. The only difference is that the last one has letters ’EH’ denoting the denial of host external hardware availability.

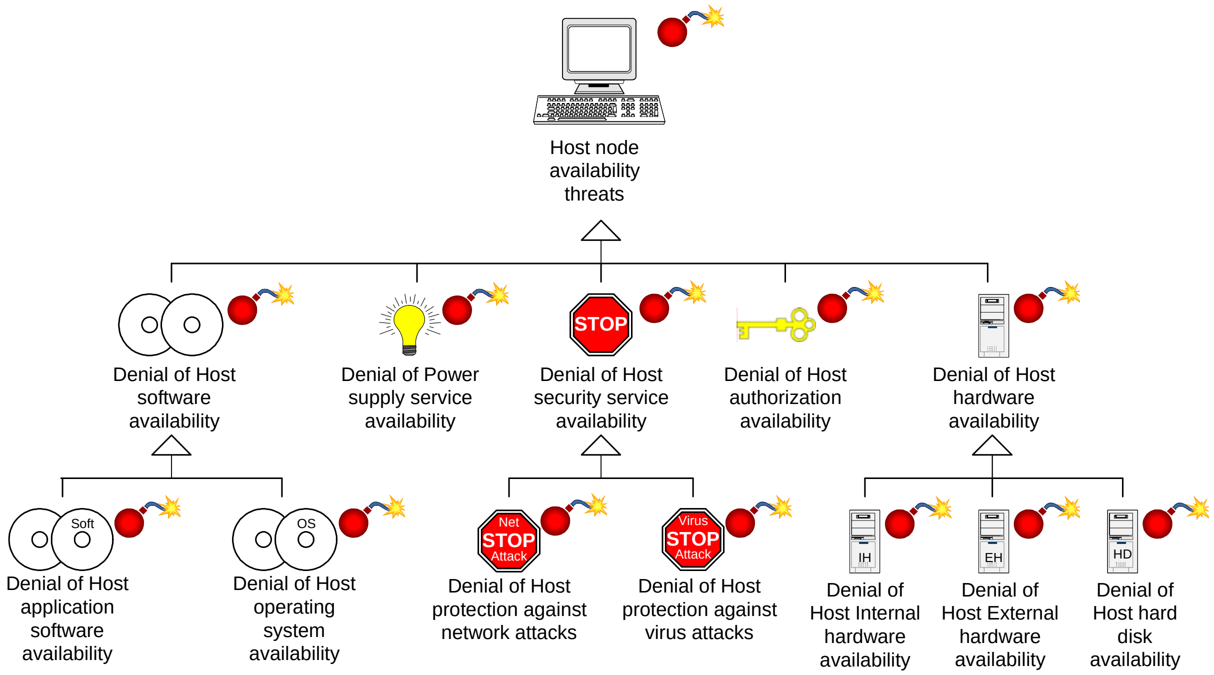

Host node availability threats
Denial of Host software availability
Denial of Power supply service availability
STOP
Denial of Host security service availability
Denial of Host authorization availability
Denial of Host hardware availability
Soft
Denial of Host application software availability
OS
Denial of Host operating system availability
Net STOP Attack
Denial of Host protection against network attacks
Virus STOP Attack
Denial of Host protection against virus attacks
IH
Denial of Host Internal hardware availability
EH
Denial of Host External hardware availability
HD
Denial of Host hard disk availability

Figure 7.7: Categorisation of availability threats symbols

Figures 7.8 and 7.9 illustrate how symbols depicted in Figure 7.10 may be used in use cases. Figure 7.8 shows two actors: a user and a mis-user who may be responsible for two threats that can cause the denial of host node availability. The treatment of a threat may be denoted by a red cross with lighting. Figure 7.9 shows how two threats from Figure 7.11 can be treated by installing a firewall and antivirus software.

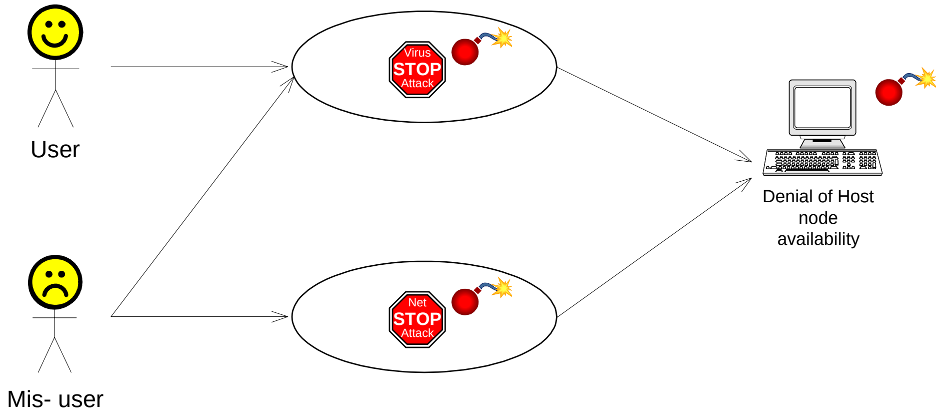


Figure 7.8: Security service availability threat use case

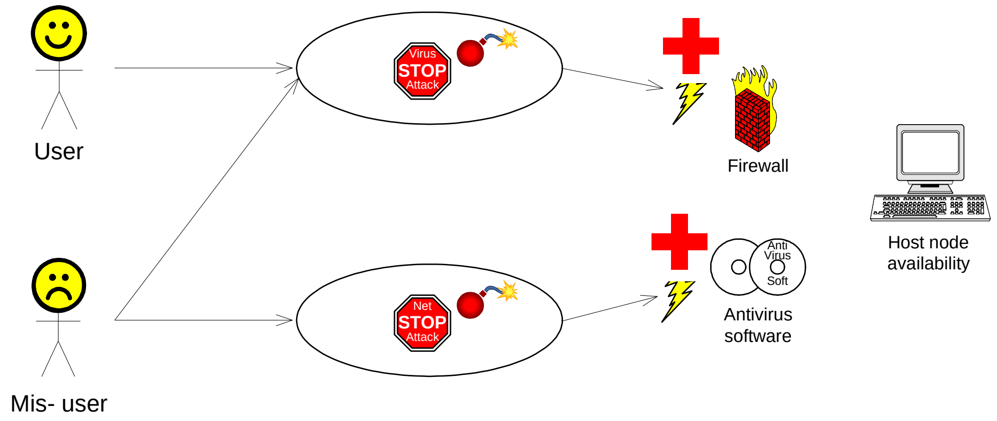


Figure 7.9: Security service availability treatment use case

8 Conclusion

We have presented MODA, a methodology for identifying, assessing and treating risks to availability. The MODA methodology is model driven and has been tested in two case studies: Private Lessons and Chat Service. The benefits of using MODA is a more efficient availability risk assessment due to extensive use of templates that contribute to high level of reusability and better communication among different stakeholders. MODA is characterised by the following:

- A risk management process based on AZ/NZS [6] and CORAS [5].
- Specialised templates and guidelines that support each sub-process of the MODA risk management process.
- Integration of techniques and features from risk assessment methods like FTA [12].
- Use of models to describe aspects that are relevant for availability risk assessment.

MODA meets the requirements of chapter 3 in the following sense:

1. MODA targets availability from a security perspective with the help of templates and guidelines:
   - Identification of security risks to host node availability is addressed in the templates for Host node availability (Figure 4.15) and Host security service availability (Figure 4.19).
   - Security risks are suggested to be categorised into three risk treatment categories: Host authorization availability risks, Host security service availability risks (firewall), Host security service availability risks (antivirus software) (Table 5.48).
   - Three templates for risk treatment support the identification of treatment strategies for host security risks (Figures B.14, B.15, B.16 in Appendix B).

2. Time effectiveness of MODA is achieved by means of guidelines, templates, check lists and a predefined set of tables and was validated in two case studies:
   - Predefined set of consequence and frequency categories helps in the quick identification of set of consequence and frequency values (Tables 5.7, 5.9…5.11, Figure 5.3).
   - Guidelines and templates assist to quick identification of risks and strategies for risk treatment (Figures 4.15… 4.19; B.1…B.20 in Appendix B).
   - Predefined set of consequence and frequency tables facilitates quick construction and documentation of consequence and frequency values (Figures A.1…A.10 in Appendix A).
   - Categorisation of risks into risk treatment categories can be done quickly according to the availability aspects categories (Table 5.48).

3. Cost effectiveness of MODA is achieved in the following way:
   - Availability risk assessment results are documented in tables and graphical models that can be reused in new or current availability risk assessment (e.g. fault trees in Activity 2.2; risk treatment tables in Activity 5.1).

   - Clear defined structure of templates and tables makes it possible to automate some parts of availability assessment (e.g. templates for the availability risk analysis from section 4.7; tables for risk analysis from Appendix A).
4. User friendliness of MODA is supported in the following way:
   - Graphical models support the communication between people with different background participating in availability risk assessment (e.g. Graphical templates for risk treatment in Activity 5.1).
   - In all sub-processes users are assisted by set of guidelines, templates and checklists.

8.1 Related work

MODA uses models to describe aspects that are relevant for availability risk assessment. The concept of model based risk assessment has been a research topic since 80-s [34] [35]. Recently CORAS [5] – a research and technological development project under the Information Society Technologies (IST) Programme (IST-2000-25031) developed a practical framework targeting risk analysis of security critical systems, which combines methods for risk analysis with methods for object-oriented modelling. Among other approaches to model-based risk assessment we can mention CRAMM [14], ATAM [36], Surety Analysis [37], and RSDS [38].

Some of the activities of the MODA risk management process are similar to the activities used in the CORAS risk management process, while others are completely different. This is due to the difference in goals of these two risk assessment methodologies. While CORAS addresses computer systems and security risks in a general manner, the main purpose of MODA is to target availability risks.

In the first sub-process – context identification, MODA's activities have more similarities with activities in CORAS then they do in other sub-processes. This is because in the first sub-process, both CORAS and MODA aim to clarify and define aspects that do not depend much on the kind of the risk assessment: scope of the risk assessment, participants of the risk assessment, target of evaluation, stakeholders, assets, risk evaluation criteria. This in turn explains why the most tables that MODA have borrowed from CORAS are used in this sub-process. At the same time MODA aims to be time effective and this explains why it does not have all the activities and sub-activities of CORAS. For example, the CORAS Activity 1.1 Identify areas of relevance has five sub-activities: the risk management context, the target of evaluation, the organisational context, the SWOT analysis, and the system description sub-activity. MODA does not have the three last ones and redefines only the first two sub-activities: Activity 1.1 Risk management context specification and Activity 1.2 Specification of the target of evaluation have the same purpose in MODA as the similar sub-activities of Activity 1.1 in CORAS.

Further, Activity 1.4 Identification of assets redefines in MODA the CORAS Activity 1.2 Identify and value assets, and Activity 1.5 Identification of the risk acceptance criteria redefines the risk evaluation criteria sub-activity of the CORAS Activity 1.3. MODA does not have an activity corresponding to the CORAS Activity 1.4 Approval.

In the context identification sub-process, MODA uses eleven CORAS tables and defines thirteen own tables and figures. Table 8.1 shows MODA and CORAS tables and figures used in this sub-process. Table 8.2 shows the most important MODA features in the context identification sub-process that are not part of the CORAS methodology.

Table 8.1: MODA and CORAS tables used in the context identification sub-process

CORAS	MODA
Table 5.3: Assessment methods table Table 5.4: Assessment restrictions table Table 5.5: Assessment roles table Table 5.6: Assessment plan table Table 5.7: Qualitative and quantitative frequency values Table 5.13: Risk Matrix Table 5.17: Target-of-evaluation table Table 5.19: Stakeholders table Table 5.21: Generic asset value domains Figure 5.8: Asset diagram Table 5.22: Asset table	Table 5.2: Assessment objectives table Table 5.8: Frequency values table Figure 5.3: Categorization of consequences of system unavailability Table 5.9: Asset consequence values table Table 5.10: Target system consequence values table Table 5.11: Total income consequence values table Table 5.12: Consequence values table Table 5.14: Risk values table Table 5.15: Risk treatment action priority matrix Table 5.16: Treatment action values table Figure 5.7: Questionnaire guide Figure 5.10: Risk acceptance criteria alternatives Table 5.24: Risk acceptance table

Table 8.2: The most important MODA features in the context identification sub-process

MODA features
• Guidelines for the definition of a risk assessment plan. • Predefined set of consequence categories (Figure 5.3, Tables 5.9..5.11). • Risk treatment action priority matrix (Table 5.15) for the specification of treatment action priorities. • Guidelines for the identification of actors and use cases.

In the risk identification sub-process CORAS targets the identification of all kinds of risks while MODA concentrates on the identification of risks to availability. That is why MODA in this sub-process redefines one of three CORAS activities: Activity 2.1 Identification of risks to availability aspects redefines in MODA the CORAS Activity 2.1 Identify threats to assets. MODA does not have activities that have the same purpose as the CORAS Acivity 2.2 Identify vulnerabilities of assets and Activity 2.3 Document unwanted incidents. Further, MODA supports this sub-process by specialized templates and guidelines. This explains why none of the CORAS tables were used in this sub-process. Table 8.3 shows the most important MODA features in the risk identification sub-process that are not part of the CORAS methodology.

Table 8.3: The most important MODA features in the risk identification sub-process

MODA features
• Guidelines for the identification of availability aspects risks and the construction of fault trees. • Availability risks table (Table 5.26) is constructed for each availability aspect. • Templates support the building of fault trees (Figures 4.15…4.19). • Guidelines for the detailed risk identification.

In the risk analysis sub-process MODA redefines both CORAS activities. Activity 3.1 Consequence evaluation and Activity 3.2 Frequency evaluation redefine the CORAS Activity 3.1 and Activity 3.2. CORAS targets the wide spectrum of risks by applying for the consequence evaluation the risk assessment methods like FMECA [13], Event trees [32], and Markov analysis [15]. The frequency evaluation is addressed in CORAS by applying FTA [12] and Markov analysis. MODA meets its success criteria by narrowing to FTA for frequency evaluation. In this sub-process MODA does not use the CORAS tables. Further, it uses the predefined set of consequence and frequency tables to support the effective construction and documentation of consequence and frequency values. Table 8.4 shows the most important MODA features in the risk analysis sub-process that are not part of the CORAS methodology.

Table 8.4: The most important MODA features in the risk analysis sub-process

MODA features
• Guidelines for the identification of consequence and frequency values. • Use of the predefined set of consequence and frequency tables (Figures A.1…A.10).

In the risk evaluation sub-process MODA redefines three of five CORAS activities. Activity 4.1 Identification of risks values, Activity 4.3 Categorization of risks into risk treatment categories, and Activity 4.4 Specification of priorities of risk treatment categories redefine the CORAS Activity 4.1, Activity 4.3, and Activity 4.5 respectively. MODA does not have activities that have the same purpose as the CORAS Acivity 4.2 Prioritise risks and Activity 4.4 Determine interrelationships among risk themes. In this sub-process MODA does not use the CORAS tables. Further, it defines five tables and suggests eleven risk treatment categories in the Possible risk treatment categories table (Table 5.48). Table 8.5 shows the most important MODA features in the risk evaluation sub-process that are not part of the CORAS methodology.

Table 8.5: The most important MODA features in the risk evaluation sub-process

MODA features
• Guidelines for the identification and update of risk values. • Use of the predefined set of risk treatment categories (Table 5.48). • Guidelines for the specification of priorities of risk treatment categories.

In the risk treatment sub-process MODA redefines both two CORAS activities. Activity 5.1 Identification of treatment options and Activity 5.2 Specification of risks treatment priorities redefine the CORAS Activity 5.1 and Activity 5.2. In this sub-process MODA does not use CORAS tables. While CORAS provides guidelines for the risk treatment in a general manner, MODA defines treatment actions for each predefined risk treatment category. Further, MODA applies its own Risk treatment action priority matrix for the specification of priorities of risk treatment actions. Table 8.6 shows the most important MODA features in the risk treatment sub-process that are not part of the CORAS methodology.

Table 8.6: The most important MODA features in the risk treatment sub-process

MODA features
• Guidelines for the identification of risk treatment options and risk treatment actions. • Use of graphical templates for the identification of treatment actions (Figures B.1…B.20). • Specification of priorities of risk treatment actions with the help of Risk treatment action priority matrix (Table 5.15).

8.2 Future work

One major challenge when performing an availability risk analysis is to establish a common understanding of the target of evaluation, availability risks and treatment strategies among the stakeholders participating in the availability analysis. An interesting area of research will be to develop a UML profile aiming to facilitate communication among stakeholders participating in availability assessment, by making the UML diagrams easier to understand for non-experts. Some elements of this profile we presented in Chapter 7. Dealing with the large volume of information, tables and diagrams is a non-trivial task. It will be interesting to develop computerised tool that effectively manages the construction of tables and diagrams as well as database of information relevant for availability risk assessment.

An essential part of the results of an availability risk analysis will typically have a certain general character. To avoid spending time and resources on starting from scratch for every new analysis, it is important to collect these general aspects. Documenting availability risk analysis results in UML-diagrams, tables and plain text opens for the collection of these general aspects through partially instantiated UML-diagrams, tables and check lists. CORAS organizes related general elements in so-called ’experience packages’ and has a computerised repository that manages the extraction, reuse and maintenance of experience packages [39]. An experience package is either constructive or supportive. Elements in the constructive experience package may be extended, instantiated or adjusted into concrete risk analysis documentation. Elements in the supportive package act as a helping hand during the instantiation of constructive elements or the making of new reusable elements.

It will be interesting to upgrade the CORAS repository to support the effective management of availability experience packages. Further, the availability experience packages may have sub-packages that contain elements specific for particular domain, e.g., telemedicine or e-commerce. These packages may be further decomposed into constructive and supportive. An important part of the work will be to define what kind of generic elements MODA has, and in what package they may be included.

References

[1] Computer Crime and Security Survey**,** retrieved February 10, 2003, from: http://www.gocsi.com/press/20020407.html (Computer Security Institute)

[2] Galatenko V., Doroshin I. "*Availability as an element of information security*" retrieved April 27, 2003, from: http://unixgems.jinr.ru/faq_guide/security/jet/acc_sec/article1.2.1997.html

[3] Visa SETs Security Standard for Online Shopping, retrieved February 25, 2003, from: http://www.acs.org.au/nsw/articles/2000061.htm

[4] Lukatski A.V. *Attacks identification*, BXV-Peterburg 2001

[5] Fredriksen R., Houmb S.H., Mork-Knudsen E., Wisløff E.D., Skipeens E., Lund M.S., Stølen K.: *The CORAS methodology for model-based risk assessment* vD2.4, IST-2000-25031

[6] Australian Standard (1999): *Risk management*, AS/NZS 4360:1999. Strathfield: StandardsAustralia

[7] Sommerville I. *Software Engineering*, 6.ed Addison-Wesley 2001

[8] Vose D. *Risk analysis. A quantitative guide* John Wiley & sons 2.ed 2001

[9] The CORAS Project. http://coras.sourceforge.net/

[10] ISO/IEC 10746:1995: Basic reference model for open distributed processing

[11] Redmill F., Chudleigh M., Catmur J. *Hazop and Software Hazop*, Wiley & sons 1999

[12] Andrews J.D., Moss T.R.: *Reliability and Risk Assessment*, 1st ed. Longman Group UK 1993

[13] Bouti A., Kadi A.D., *A state-of-the-art review of FMEA/FMECA International Journal of Reliability, Quality and Safety Engineering*, vol. 1, 1994, no. 4, pp 515-543

[14] Barber B., Davey J.: *The use of the CCTA risk analysis and management methodology CRAMM.* In: Proc. MEDINF. North Holland 1992, 1589-1593

[15] Littlewood B. *A Reliability Modell for Systems with Markov Structure* Applied Statistics, 24(2), 1975

[16] Booch G., Jacobson I., Rumbaugh J.: *Unified Software Development Process*, Addison-Wesley 1999

[17] World Wide Web Consortium: *Extensible Markup Language (XML)* v1.0, W3C Recommendation, Second Edition, 6 Oct. 2000

[18] ISO/IEC 17799-1:2000: Information technology – Code of Practice for information security management. http://www.iso.ch

[19] ISO/IEC TR 13335:2000 Information technology – Guidelines for the management of IT Security http://www.iso.ch

[20] IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related (E/E/PE) Systems

[21] IEEE610: IEEE Std 610.12 (1990): IEEE Standard Glossary of Software Engineering Terminology

[22] Avizienis A, Laprie J.C., Randell B.: *Dependability of computer systems: Fundamental concepts, terminology, and examples*. Technical report, LAAS-CNRS, October 2000.

[23] ISO/IEC TR 13335-1:2001 Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security

[24] OMG, *Unified Modelling Language Specification*, version 1.4, 2001

[25] Fowler M., Scott K., UML Distilled: *Applying the Standard Object Modelling Language*, Addison-Wesley, 1997

[26] McGrath J.E.: *Groups: interaction and performance*, Prentice Hall, 1984

[27] Englander, Irv. *The architecture of computer hardware and system software: An information technology approach,* 2.ed, John Wiley & Sons, Inc 2000

[28] Webopedia - *Internet online encyclopaedia,* retrieved May, 12, 2003, from: http://www.webopedia.com

[29] Hoffer J.A., George J., Valacich J. *Modern systems analysis and design*, 2.ed Addison-Wesley 1999

[30] Eeles P, Houston K, Kozaczynski W. *Building J2EE applications with the rational unified process*. Addison-Wesley 2003

[31] Berre A.J., B. Elvesæter B., Aagedal J.Ø., Solberg A., Oldevik J., Nordmoen B.: *COMET - Methodology Handbook with documentation of the COMET metamodels*, retrieved May, 27, 2003, from: http://www.ifi.uio.no/~mmo/generic/handbooks/COMET_v23.pdf

[32] Storey N.: *Safety-Critical Computer Systems*. Addison-Wesley 1996

[33] Husa K.E.: AMIGOS Case Study Requirement Specification 2003

[34] Garrett C.J., Guarro S.B., Apostolakis G.E.: *The dynamic flow graph methodology for assessing the dependability of embedded software systems*. IEEE Trans. on Systems, Man, and Cybernetics, Vol. 25, No.5, 1995, 824-840

[35] Kim I.S., Modarres M.: *Application of Goal Tree-Success Tree Model as The Knowledge-Base of Operator Advisory System*, Nuclear Engineering & Design Journal., 104, 1987, 67-81

[36] Clements P., Kazman R., Klein M.: *Evaluating software architectures: methods and case studies*. Addison-Wesley 2000

[37] Wyss G.D., Craft R.L., Funkhouser D.R.: *The use of object-oriented analysis methods in surety analysis*. SAND Report 99-1242. Sandia National Laboratories 1999

[38] Lano K., Androutsopoulos K., Clark D.: *Structuring and design of reactive systems using RSDS*. In: Proc. FASE 200, LNCS 1783. Springer 2000, 97-111

[39] Braber F., Gan C., Lund M.S., Stølen K., Vraalsen F.: *A UML Experience Repository Supporting Security Risk Analysis*

Appendix A.

This appendix is structured into two sections. Section A.1 presents consequence and frequency tables for the risk analysis sub-process. Section A.2 provides questionnaires for assets identification.

A.1 Tables for the risk analysis sub-process

This section is divided into two sub-sections. Sub-section A.1.1 presents consequence tables. Frequency tables are presented in sub-section A.1.2. Section A.2 provides questionnaires for assets identification.

A.1.1 Consequence tables

Table A.1: Consequence table (General form)

Stakeholder	Asset	Risk	Risk scenario	Consequence value	Consequence description
<stakeholder>	<asset>	<incident>	<scenario>	<consequence value>	<consequence description>

Table A.2: Consequence table for host software availability risks

Stakeholder	Asset	Risk			Risk scenario	Consequence value	Consequence description
<Stake holder>	<Asset>	Denial of host software availability	Denial of host operating system availability		<scenario>	<value>	<description>
			Denial of host application software availability	Denial of <entity *n1*>	<scenario>	<value>	<description>
				…	<scenario>	<value>	<description>
				<entity *nn*>	<scenario>	<value>	<description>

Table A.3: Consequence table for host hardware availability risks

Stakeholder	Asset	Risk			Risk scenario	Consequence value	Consequence description
<Stake holder>	<Asset>	Denial of host hardware availability	Denial of host storage device availability		<scenario>	<value>	<description>
			Denial of host internal hardware availability	Denial of <entity *n1*>	<scenario>	<value>	<description>
				…	<scenario>	<value>	<description>
			Denial of host external hardware availability	…	<scenario>	<value>	<description>
				…	<scenario>	<value>	<description>
				Denial of <entity *nn*>	<scenario>	<value>	<description>

Table A.4: Consequence table for host security service availability risks

Stakeholder	Asset	Risk		Risk scenario	Consequence value	Consequence description
<Stake holder>	<Asset>	Denial of host security service availability	Lack of firewall – host is attacked from the Internet	<scenario>	<value>	<description>
			Lack of antivirus software – host is attacked by computer virus	<scenario>	<value>	<description>

Table A.5: Consequence table for host availability risks

Stakeholder	Asset	Risk		Risk scenario	Consequence value	Consequence description
<Stake holder>	<Asset>	Denial of host availability	Denial of host Software availability	<scenario>	<value>	<description>
			Denial of host Hardware availability	<scenario>	<value>	<description>
			Denial of power supply service availability	<scenario>	<value>	<description>
			Denial of host security service availability	<scenario>	<value>	<description>
			Denial of host authorization availability	<scenario>	<value>	<description>

A.1.2 Frequency tables

Table A.6: Frequency table (General form)

Stakeholder	Asset	Risk	Risk scenario	Frequency value	Frequency description
<stakeholder>	<asset>	<incident>	<scenario>	<Frequency value>	<Frequency description>

Table A.7: Frequency table for host software availability risks

Stakeholder	Asset	Risk			Risk scenario	Frequency value	Frequency description
<Stake holder>	<Asset>	Denial of host software availability	Denial of host operating system availability		<scenario>	<value>	<description>
			Denial of host application software availability	Denial of <entity *n1*>	<scenario>	<value>	<description>
				…	<scenario>	<value>	<description>
				<entity *nn*>	<scenario>	<value>	<description>

Table A.8: Frequency table for host hardware availability risks

Stakeholder	Asset	Risk			Risk scenario	Frequency value	Frequency description
<Stake holder>	<Asset>	Denial of host hardware availability	Denial of host storage device availability		<scenario>	<value>	<description>
			Denial of host internal hardware availability	Denial of <entity *n1*>	<scenario>	<value>	<description>
				…	<scenario>	<value>	<description>
			Denial of host external hardware availability	…	<scenario>	<value>	<description>
				…	<scenario>	<value>	<description>
				Denial of <entity *nn*>	<scenario>	<value>	<description>

Table A.9: Frequency table for host security service availability risks

Stakeholder	Asset	Risk		Risk scenario	Frequency value	Frequency description
<Stake holder>	<Asset>	Denial of host security service availability	Lack/Denial of firewall – host is attacked from the Internet	<scenario>	<value>	<description>
			Lack/Denial of antivirus software – host is attacked by computer virus	<scenario>	<value>	<description>

Table A.10: Frequency table for host availability risks

Stakeholder	Asset	Risk		Risk scenario	Frequency value	Frequency description
<Stake holder>	<Asset>	Denial of host availability	Denial of host Software availability	<scenario>	<value>	<description>
			Denial of host Hardware availability	<scenario>	<value>	<description>
			Denial of power supply service availability	<scenario>	<value>	<description>
			Denial of host security service availability	<scenario>	<value>	<description>
			Denial of host authorization availability	<scenario>	<value>	<description>

A.2 Questionnaires for assets identification

Asset category	Description	Questionnaire
Human assets	Assets related to human resources, special knowledge	Questionnaire 1
Physical assets	Includes all physical components in the system and system dependent components	Questionnaire 2
Information assets	All information in the system and system dependent information	Questionnaire 3
Software assets	All software used in the system or system dependent	Questionnaire 4
Organizational assets	Organizational concerns, organizational (system) internal regulations, routines etc.	Questionnaire 5
Law and regulation assets	External laws and regulations that influence the system	Questionnaire 6

Figure A.1: Questionnaire overview

Questionnaire 1: for identification of assets related to the asset category “Human”

Q1.1 Which personnel safety is important?
Q1.2 Which parts of the system is depending on special knowledge?
Q1.3 Which special knowledge is it important to keep the within organization ?
Q1.4 Which parts of the system is depending on single individuals?

Questionnaire 2: for identification of assets related to the asset category “Physical assets”

Q2.1 Which system components is the system functionality depending on?
Q2.2 Which system components is system critical?
Q2.3 Which system components are of highest value?
Q2.4 Which system components have the highest maintainability costs?
Q2.5 Which system components have the longest repair time?
Q2.6 Which system components have the highest repair costs?

Questionnaire 3: for identification of assets related to the asset category “Information assets”

Q3.1 Which parts of the system is transporting/containing confidential information?
Q3.2 Which parts of the system is transporting/containing personnel information?
Q3.3 Which parts of the system is transporting/containing credit card/account information?
Q3.4 Which parts of the system is transporting/containing customers information?
Q3.5 Which parts of the system is transporting/containing financial information?
Q3.6 Which parts of the system is transporting/containing business information?
Q3.7 Which parts of the system information is confidential?

Questionnaire 4: for identification of assets related to the asset category “Software assets”

Q4.1 Which system software is processing confidential information?
Q4.2 Which system software is processing personnel information?
Q4.3 Which system software is processing credit card/account information?
Q4.4 Which system software is processing customers information?
Q4.5 Which system software is processing financial information?
Q4.6 Which system software is processing business information?
Q4.7 Which parts of software are properly tested?
Q4.8 To which part of the system are QA applied?

Questionnaire 5: for identification of assets related to the asset category “Organizational assets”

Q5.1 How important is the system to the organization?
Q5.2 How much of value is the system to the organization related to other parts of the organization?
Q5.3 How critical is the system to the organization?

Questionnaire 6: for identification of assets related to the asset category “Law and regulation assets”

Q6.1 Which system stakeholders are aware of all the system relevant laws and regulations?
Q6.2 Which countermeasures are installed to avoid breach in laws and regulations that can lead to significant losses?

Appendix B.

This appendix provides templates for risk treatment. Table B.1 shows the overview of templates presented in this appendix. The middle column shows the risk treatment template. The left column shows the corresponding figure. The right column shows the page where the reader can find the template.

Table B.1: The overview of Appendix B

Figure	Template for the treatment of risk	Page
B.1	Denial of application software functionality	130
B.2	Incorrect installation and use of application software	131
B.3	Denial of application software authorization functionality	132
B.4	Denial of operating system functionality	133
B.5	Incorrect installation and use of operating system	134
B.6	Denial of operating system authorization functionality	135
B.7	Denial of hardware software functionality	136
B.8	Denial of hardware component functionality	137
B.9	Incorrect installation and use of hardware component	138
B.10	Denial of hardware component authorization functionality	139
B.11	Denial of storage device functionality	140
B.12	Incorrect installation and use of storage device	141
B.13	Denial of storage device authorization functionality	142
B.14	Lack of firewall/Attack from the network	143
B.15	Lack of antivirus software/Virus attack	144
B.16	Denial of Host authorization availability	145
B.17	Denial of power supply service availability	146
B.18	Denial of Human availability	147
B.19	Lack of quality of service in the network (Network consumer)	148
B.20	Lack of quality of service in the network (Network provider)	149

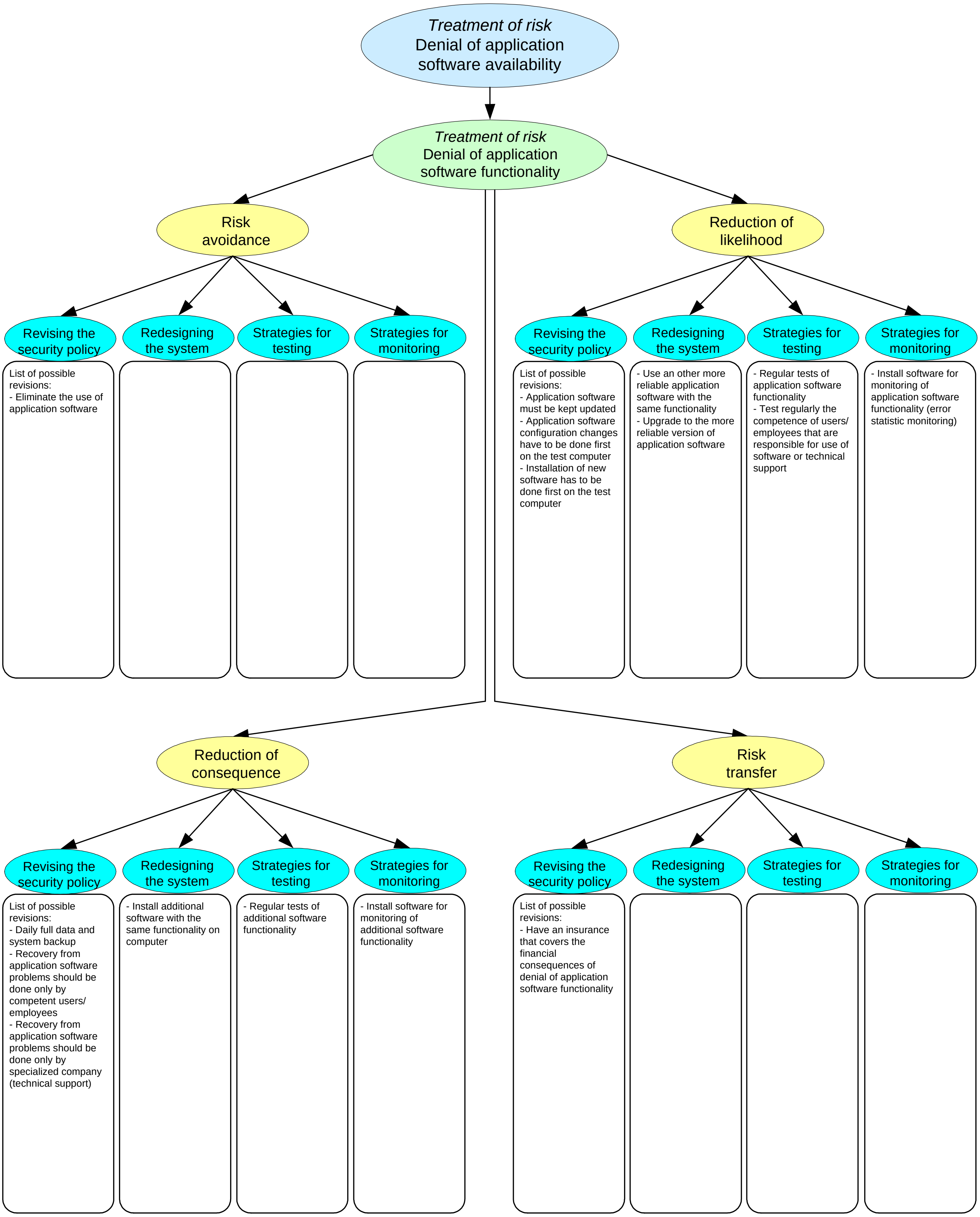
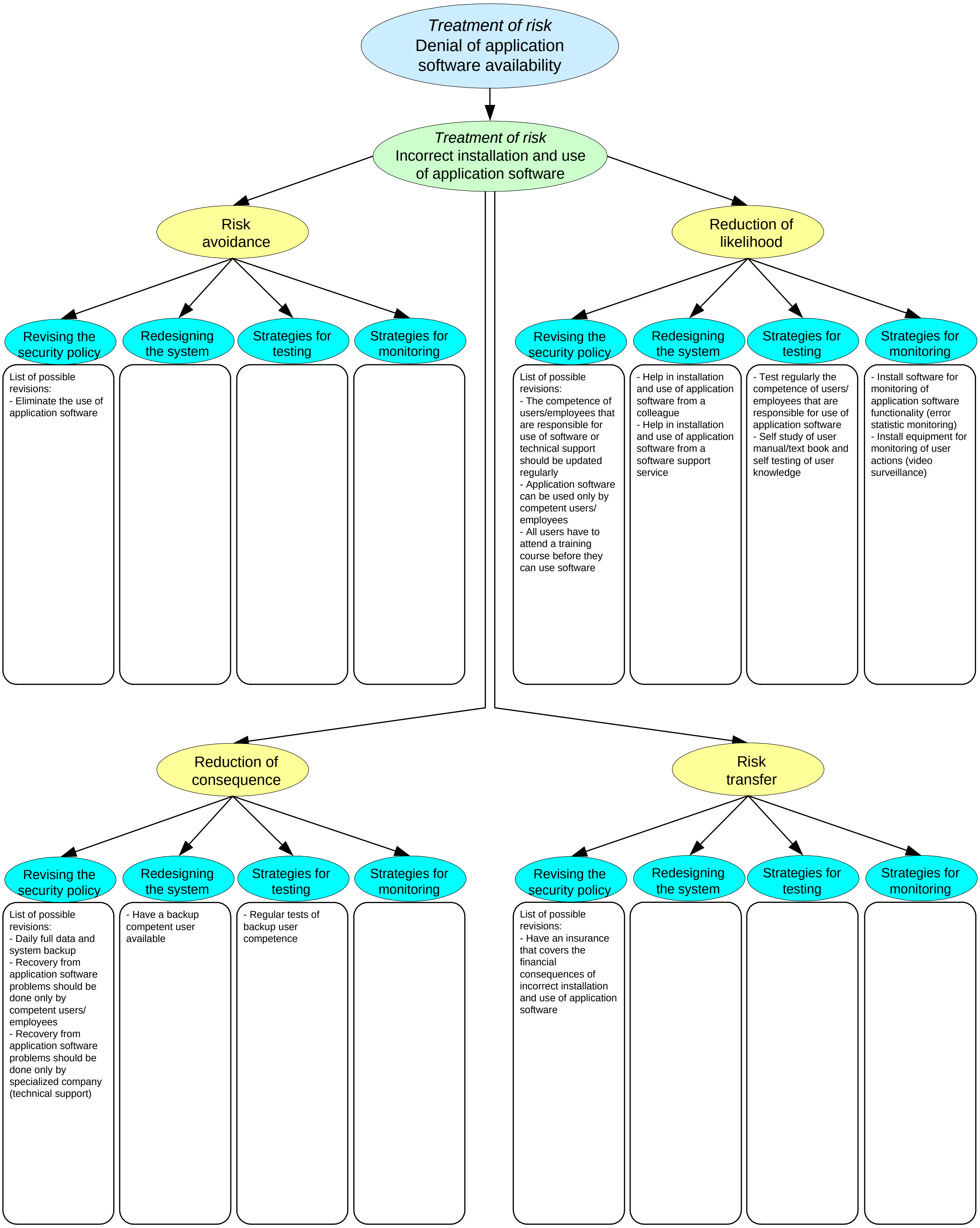

Treatment of risk
Denial of application software availability
Treatment of risk
Denial of application software functionality
Risk avoidance
Revising the security policy
List of possible revisions:
- Eliminate the use of application software
Redesigning the system
Strategies for testing
Strategies for monitoring
Reduction of likelihood
Revising the security policy
List of possible revisions:
- Application software must be kept updated
- Application software configuration changes have to be done first on the test computer
- Installation of new software has to be done first on the test computer
Redesigning the system
- Use an other more reliable application software with the same functionality
- Upgrade to the more reliable version of application software
Strategies for testing
- Regular tests of application software functionality
- Test regularly the competence of users/ employees that are responsible for use of software or technical support
Strategies for monitoring
- Install software for monitoring of application software functionality (error statistic monitoring)
Reduction of consequence
Revising the security policy
List of possible revisions:
- Daily full data and system backup
- Recovery from application software problems should be done only by competent users/ employees
- Recovery from application software problems should be done only by specialized company (technical support)
Redesigning the system
- Install additional software with the same functionality on computer
Strategies for testing
- Regular tests of additional software functionality
Strategies for monitoring
- Install software for monitoring of additional software functionality
Risk transfer
Revising the security policy
List of possible revisions:
- Have an insurance that covers the financial consequences of denial of application software functionality
Redesigning the system
Strategies for testing
Strategies for monitoring

Figure B.1: Template for treatment of risk Denial of application software functionality



Risk avoidance – Revising the security policy:
List of possible revisions:
- Eliminate the use of application software

Reduction of likelihood – Revising the security policy:
List of possible revisions:
- The competence of users/employees that are responsible for use of software or technical support should be updated regularly
- Application software can be used only by competent users/ employees
- All users have to attend a training course before they can use software

Reduction of likelihood – Redesigning the system:
- Help in installation and use of application software from a colleague
- Help in installation and use of application software from a software support service

Reduction of likelihood – Strategies for testing:
- Test regularly the competence of users/ employees that are responsible for use of application software
- Self study of user manual/text book and self testing of user knowledge

Reduction of likelihood – Strategies for monitoring:
- Install software for monitoring of application software functionality (error statistic monitoring)
- Install equipment for monitoring of user actions (video surveillance)

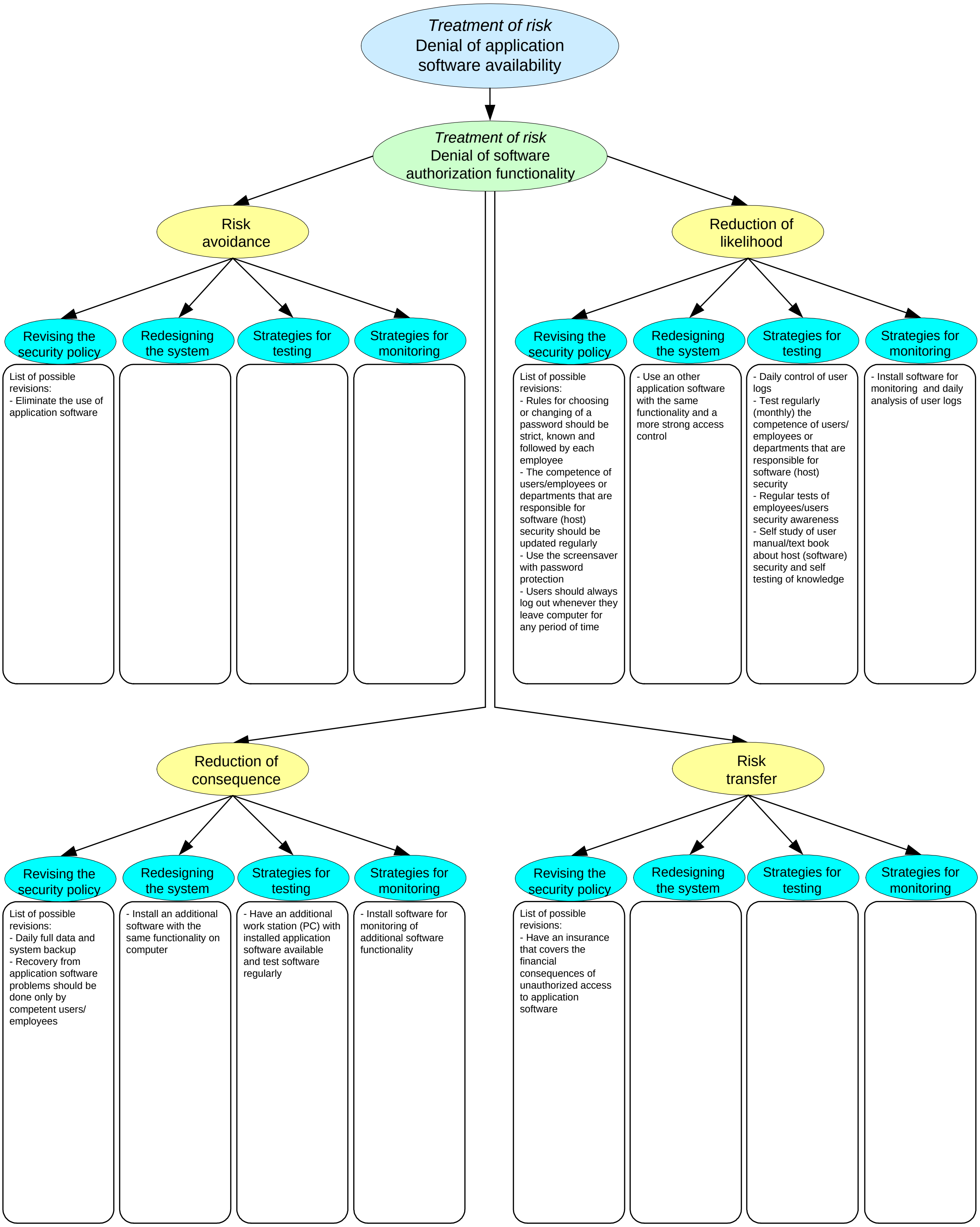
Reduction of consequence – Revising the security policy:
List of possible revisions:
- Daily full data and system backup
- Recovery from application software problems should be done only by competent users/ employees
- Recovery from application software problems should be done only by specialized company (technical support)

Reduction of consequence – Redesigning the system:
- Have a backup competent user available

Reduction of consequence – Strategies for testing:
- Regular tests of backup user competence

Risk transfer – Revising the security policy:
List of possible revisions:
- Have an insurance that covers the financial consequences of incorrect installation and use of application software

Figure B.2: Template for treatment of risk Incorrect installation and use of application software


Treatment of risk
Denial of application software availability
Treatment of risk
Denial of software authorization functionality
Risk avoidance
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Reduction of likelihood
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Reduction of consequence
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Risk transfer
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring

List of possible revisions:
- Eliminate the use of application software

List of possible revisions:
- Rules for choosing or changing of a password should be strict, known and followed by each employee
- The competence of users/employees or departments that are responsible for software (host) security should be updated regularly
- Use the screensaver with password protection
- Users should always log out whenever they leave computer for any period of time

- Use an other application software with the same functionality and a more strong access control

- Daily control of user logs
- Test regularly (monthly) the competence of users/ employees or departments that are responsible for software (host) security
- Regular tests of employees/users security awareness
- Self study of user manual/text book about host (software) security and self testing of knowledge

- Install software for monitoring and daily analysis of user logs

List of possible revisions:
- Daily full data and system backup
- Recovery from application software problems should be done only by competent users/ employees

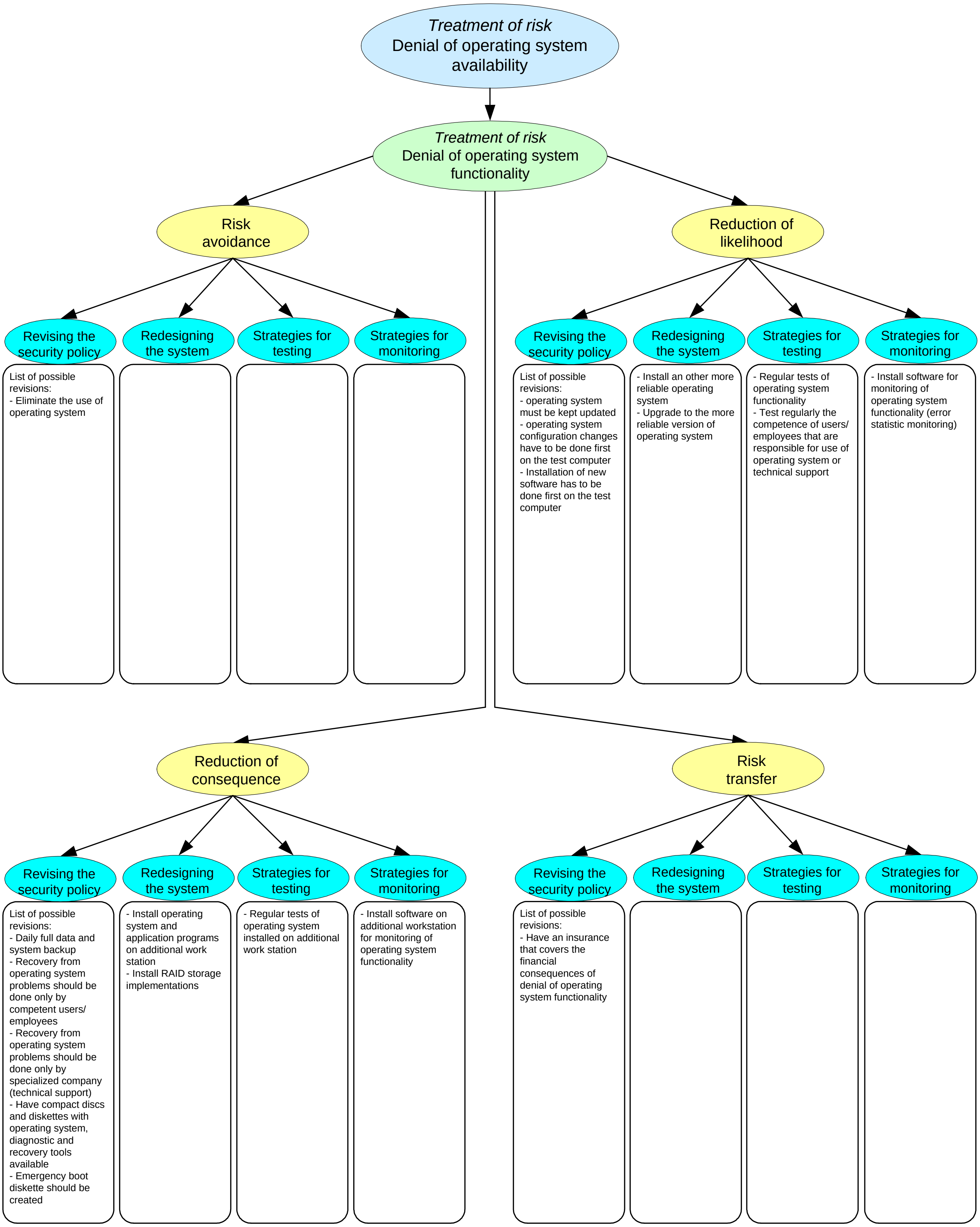
- Install an additional software with the same functionality on computer

- Have an additional work station (PC) with installed application software available and test software regularly

- Install software for monitoring of additional software functionality

List of possible revisions:
- Have an insurance that covers the financial consequences of unauthorized access to application software

Figure B.3: Template for treatment of risk Denial of application software authorization functionality


Treatment of risk
Denial of operating system availability
Treatment of risk
Denial of operating system functionality
Risk avoidance
Reduction of likelihood
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Reduction of consequence
Risk transfer
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring

List of possible revisions:
- Eliminate the use of operating system

List of possible revisions:
- operating system must be kept updated
- operating system configuration changes have to be done first on the test computer
- Installation of new software has to be done first on the test computer

- Install an other more reliable operating system
- Upgrade to the more reliable version of operating system

- Regular tests of operating system functionality
- Test regularly the competence of users/ employees that are responsible for use of operating system or technical support

- Install software for monitoring of operating system functionality (error statistic monitoring)

List of possible revisions:
- Daily full data and system backup
- Recovery from operating system problems should be done only by competent users/ employees
- Recovery from operating system problems should be done only by specialized company (technical support)
- Have compact discs and diskettes with operating system, diagnostic and recovery tools available
- Emergency boot diskette should be created

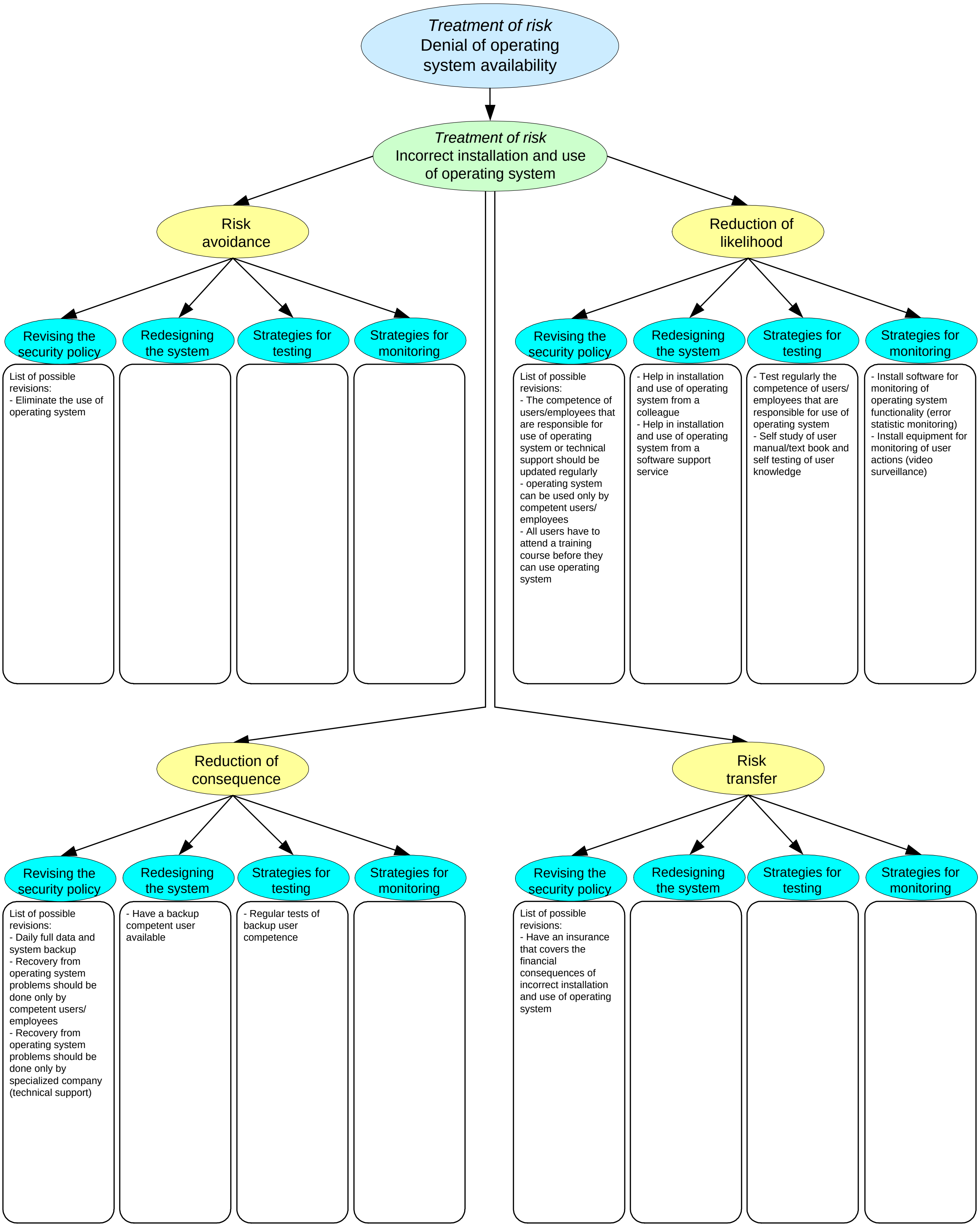
- Install operating system and application programs on additional work station
- Install RAID storage implementations

- Regular tests of operating system installed on additional work station

- Install software on additional workstation for monitoring of operating system functionality

List of possible revisions:
- Have an insurance that covers the financial consequences of denial of operating system functionality

Figure B.4: Template for treatment of risk Denial of operating system functionality



Risk avoidance – Revising the security policy:

List of possible revisions:
- Eliminate the use of operating system

Reduction of likelihood – Revising the security policy:

List of possible revisions:
- The competence of users/employees that are responsible for use of operating system or technical support should be updated regularly
- operating system can be used only by competent users/ employees
- All users have to attend a training course before they can use operating system

Reduction of likelihood – Redesigning the system:

- Help in installation and use of operating system from a colleague
- Help in installation and use of operating system from a software support service

Reduction of likelihood – Strategies for testing:

- Test regularly the competence of users/ employees that are responsible for use of operating system
- Self study of user manual/text book and self testing of user knowledge

Reduction of likelihood – Strategies for monitoring:

- Install software for monitoring of operating system functionality (error statistic monitoring)
- Install equipment for monitoring of user actions (video surveillance)

Reduction of consequence – Revising the security policy:

List of possible revisions:
- Daily full data and system backup
- Recovery from operating system problems should be done only by competent users/ employees
- Recovery from operating system problems should be done only by specialized company (technical support)

Reduction of consequence – Redesigning the system:

- Have a backup competent user available

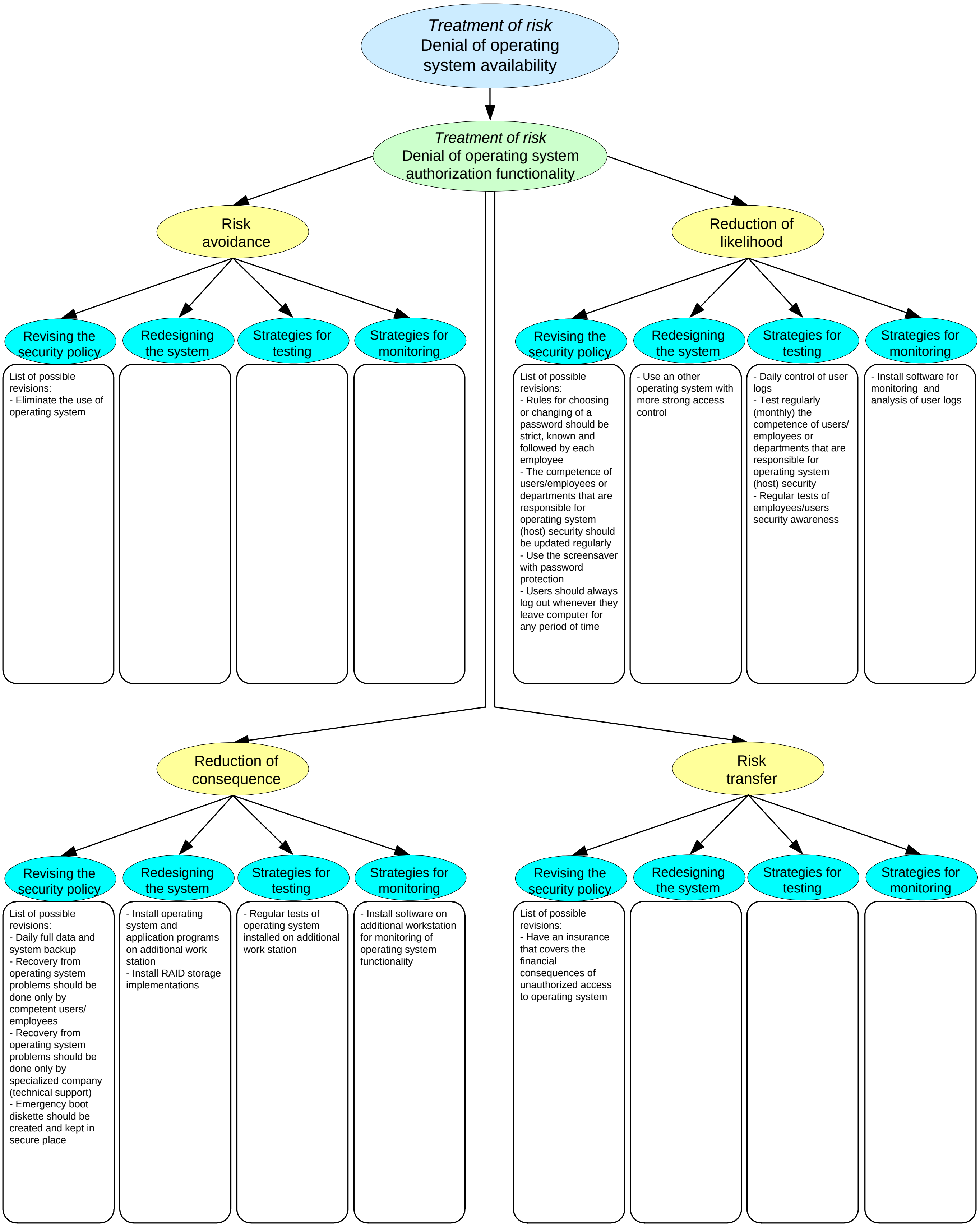
Reduction of consequence – Strategies for testing:

- Regular tests of backup user competence

Risk transfer – Revising the security policy:

List of possible revisions:
- Have an insurance that covers the financial consequences of incorrect installation and use of operating system

Figure B.5: Template for treatment of risk Incorrect installation and use of operating system



Risk avoidance – Revising the security policy:
List of possible revisions:
- Eliminate the use of operating system

Reduction of likelihood – Revising the security policy:
List of possible revisions:
- Rules for choosing or changing of a password should be strict, known and followed by each employee
- The competence of users/employees or departments that are responsible for operating system (host) security should be updated regularly
- Use the screensaver with password protection
- Users should always log out whenever they leave computer for any period of time

Reduction of likelihood – Redesigning the system:
- Use an other operating system with more strong access control

Reduction of likelihood – Strategies for testing:
- Daily control of user logs
- Test regularly (monthly) the competence of users/ employees or departments that are responsible for operating system (host) security
- Regular tests of employees/users security awareness

Reduction of likelihood – Strategies for monitoring:
- Install software for monitoring and analysis of user logs

Reduction of consequence – Revising the security policy:
List of possible revisions:
- Daily full data and system backup
- Recovery from operating system problems should be done only by competent users/ employees
- Recovery from operating system problems should be done only by specialized company (technical support)
- Emergency boot diskette should be created and kept in secure place

Reduction of consequence – Redesigning the system:
- Install operating system and application programs on additional work station
- Install RAID storage implementations

Reduction of consequence – Strategies for testing:
- Regular tests of operating system installed on additional work station

Reduction of consequence – Strategies for monitoring:
- Install software on additional workstation for monitoring of operating system functionality

Risk transfer – Revising the security policy:
List of possible revisions:
- Have an insurance that covers the financial consequences of unauthorized access to operating system

Figure B.6: Template for treatment of risk Denial of operating system authorization functionality

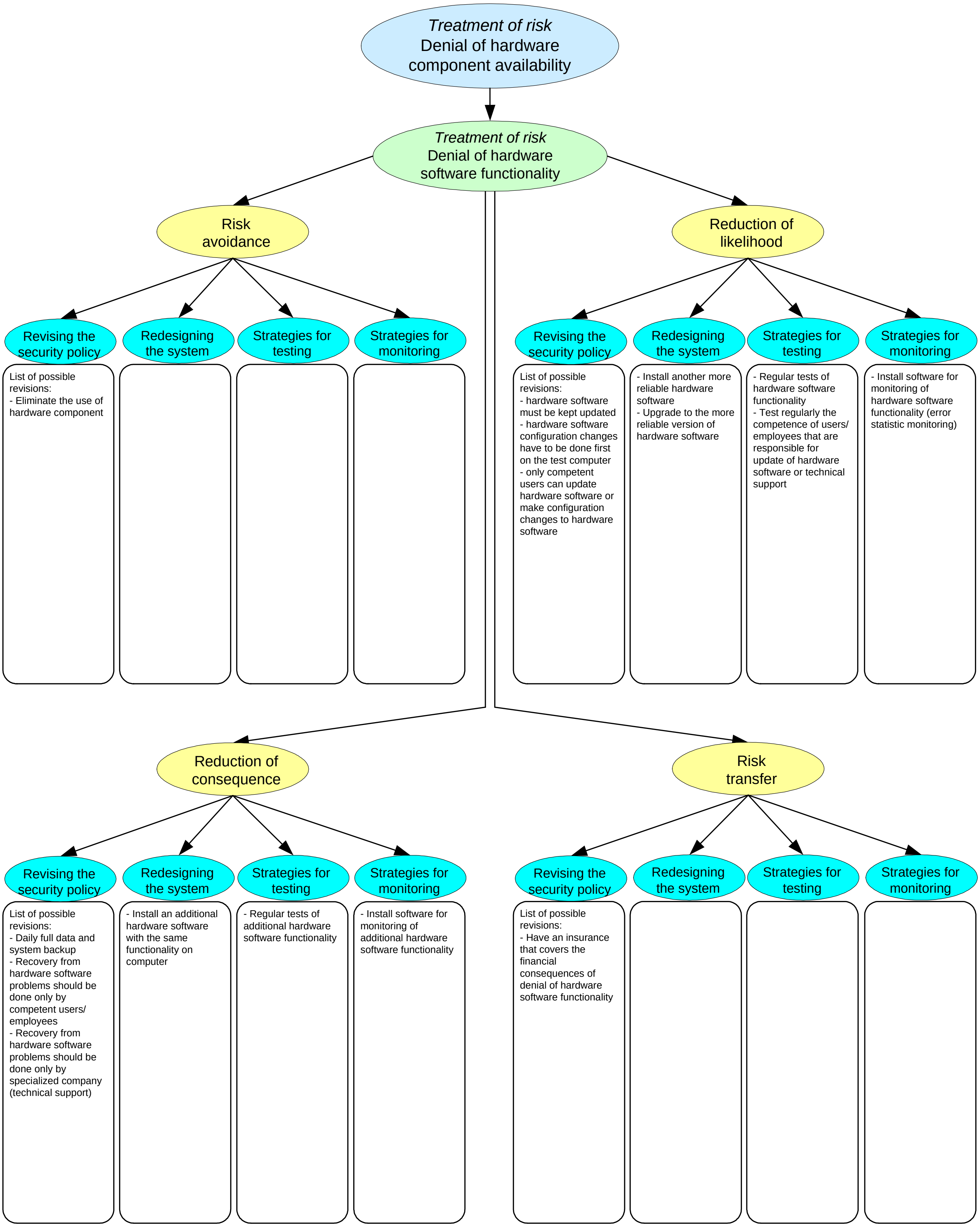

Treatment of risk
Denial of hardware component availability
Treatment of risk
Denial of hardware software functionality
Risk avoidance
Reduction of likelihood
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- Eliminate the use of hardware component
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- hardware software must be kept updated
- hardware software configuration changes have to be done first on the test computer
- only competent users can update hardware software or make configuration changes to hardware software
- Install another more reliable hardware software
- Upgrade to the more reliable version of hardware software
- Regular tests of hardware software functionality
- Test regularly the competence of users/ employees that are responsible for update of hardware software or technical support
- Install software for monitoring of hardware software functionality (error statistic monitoring)
Reduction of consequence
Risk transfer
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- Daily full data and system backup
- Recovery from hardware software problems should be done only by competent users/ employees
- Recovery from hardware software problems should be done only by specialized company (technical support)
- Install an additional hardware software with the same functionality on computer
- Regular tests of additional hardware software functionality
- Install software for monitoring of additional hardware software functionality
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- Have an insurance that covers the financial consequences of denial of hardware software functionality

Figure B.7: Template for treatment of risk Denial of hardware software functionality

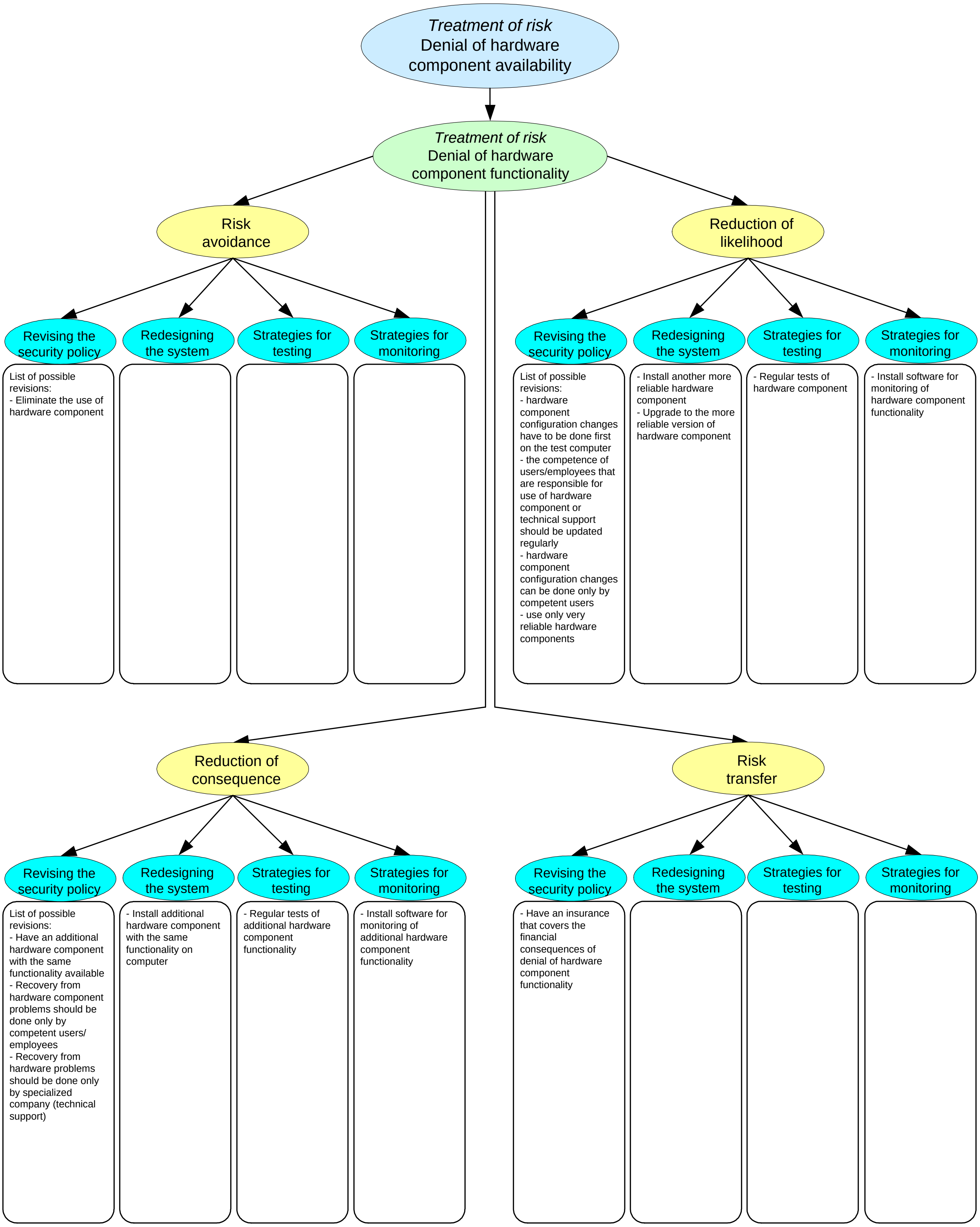
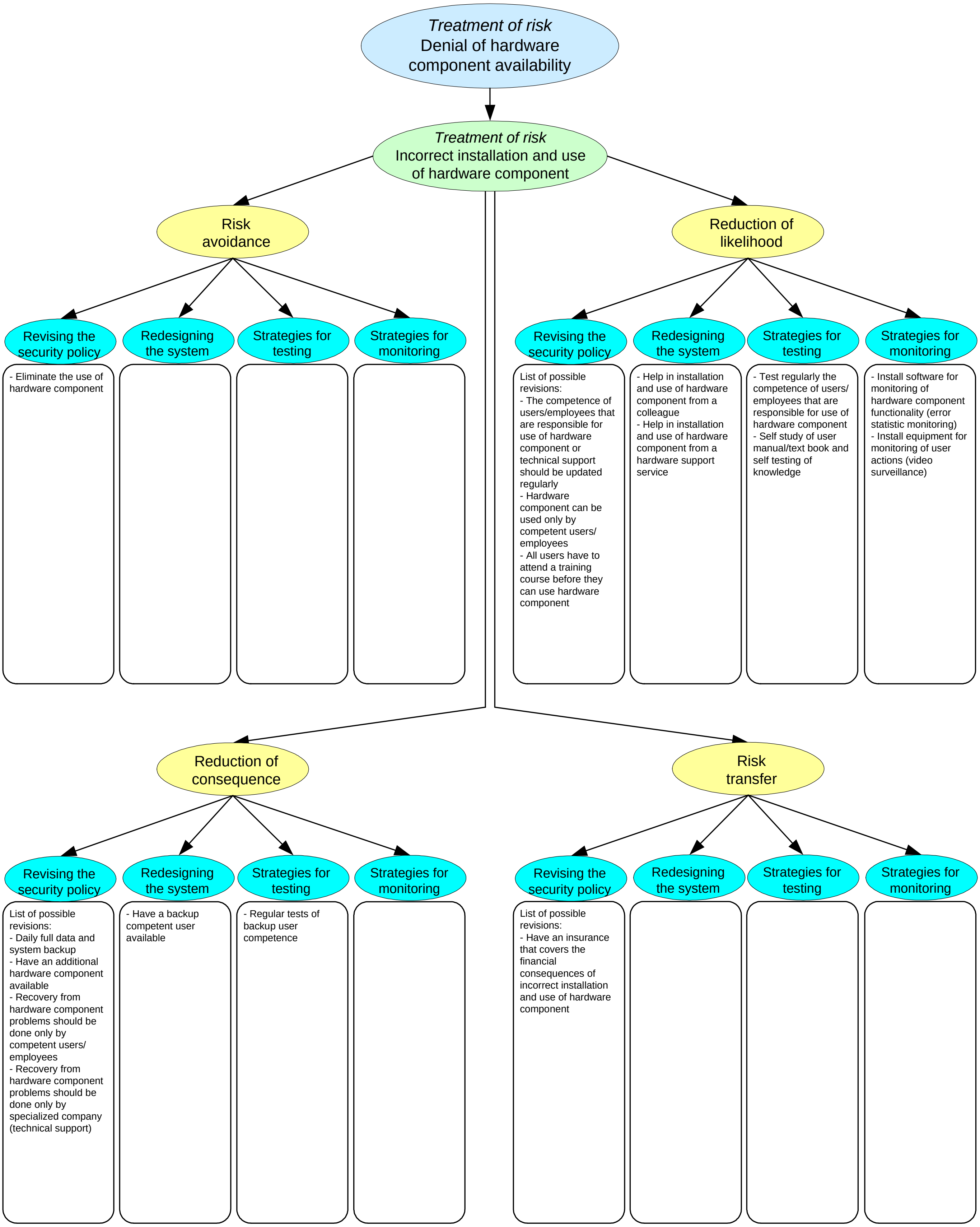

Treatment of risk Denial of hardware component availability
Treatment of risk Denial of hardware component functionality
Risk avoidance
Reduction of likelihood
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions: - Eliminate the use of hardware component
List of possible revisions: - hardware component configuration changes have to be done first on the test computer - the competence of users/employees that are responsible for use of hardware component or technical support should be updated regularly - hardware component configuration changes can be done only by competent users - use only very reliable hardware components
- Install another more reliable hardware component - Upgrade to the more reliable version of hardware component
- Regular tests of hardware component
- Install software for monitoring of hardware component functionality
Reduction of consequence
Risk transfer
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions: - Have an additional hardware component with the same functionality available - Recovery from hardware component problems should be done only by competent users/ employees - Recovery from hardware problems should be done only by specialized company (technical support)
- Install additional hardware component with the same functionality on computer
- Regular tests of additional hardware component functionality
- Install software for monitoring of additional hardware component functionality
- Have an insurance that covers the financial consequences of denial of hardware component functionality

Figure B.8: Template for treatment of risk Denial of hardware component functionality



Risk avoidance – Revising the security policy:

- Eliminate the use of hardware component

Reduction of likelihood – Revising the security policy:

List of possible revisions:
- The competence of users/employees that are responsible for use of hardware component or technical support should be updated regularly
- Hardware component can be used only by competent users/ employees
- All users have to attend a training course before they can use hardware component

Reduction of likelihood – Redesigning the system:

- Help in installation and use of hardware component from a colleague
- Help in installation and use of hardware component from a hardware support service

Reduction of likelihood – Strategies for testing:

- Test regularly the competence of users/ employees that are responsible for use of hardware component
- Self study of user manual/text book and self testing of knowledge

Reduction of likelihood – Strategies for monitoring:

- Install software for monitoring of hardware component functionality (error statistic monitoring)
- Install equipment for monitoring of user actions (video surveillance)

Reduction of consequence – Revising the security policy:

List of possible revisions:
- Daily full data and system backup
- Have an additional hardware component available
- Recovery from hardware component problems should be done only by competent users/ employees
- Recovery from hardware component problems should be done only by specialized company (technical support)

Reduction of consequence – Redesigning the system:

- Have a backup competent user available

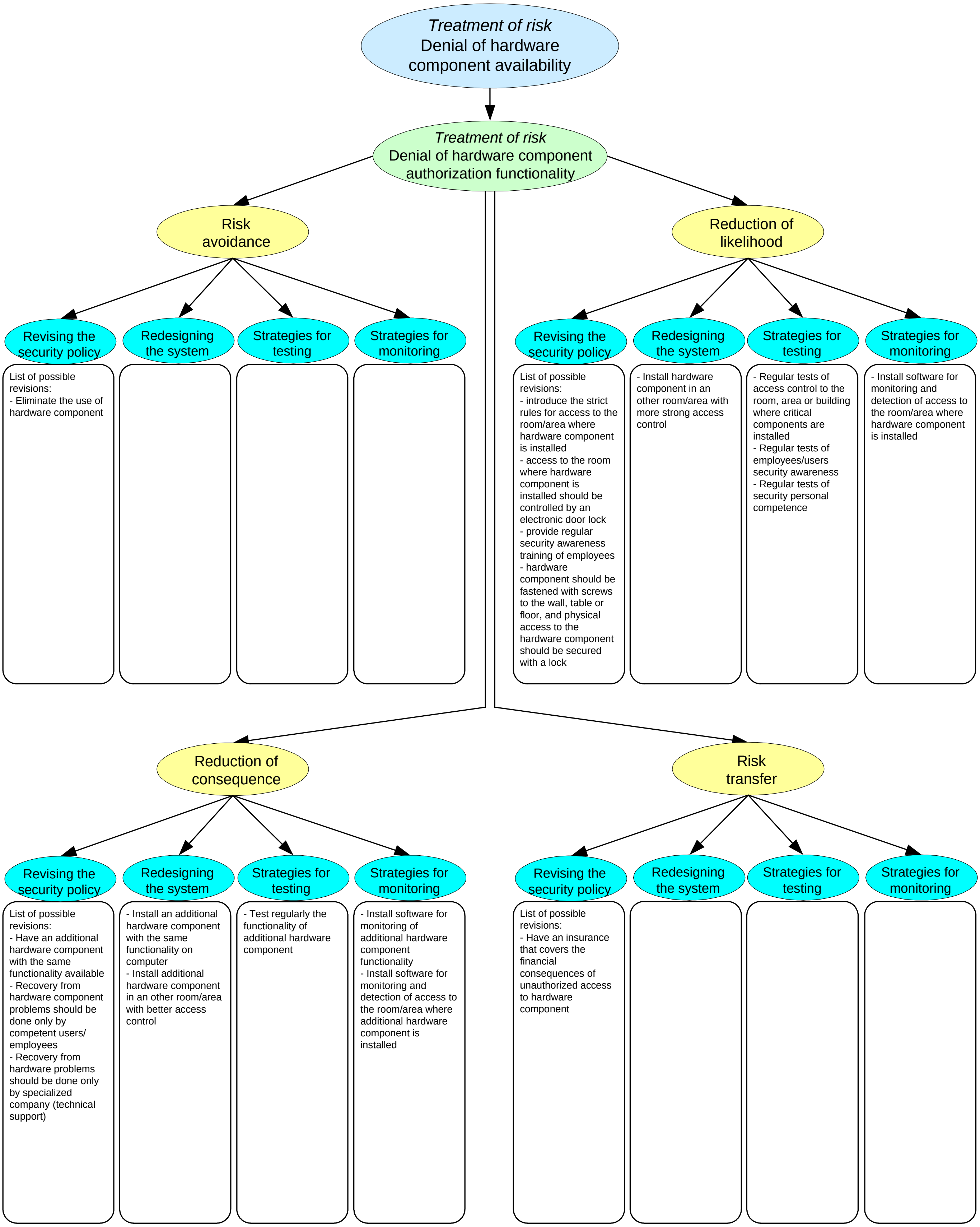
Reduction of consequence – Strategies for testing:

- Regular tests of backup user competence

Risk transfer – Revising the security policy:

List of possible revisions:
- Have an insurance that covers the financial consequences of incorrect installation and use of hardware component

Figure B.9: Template for treatment of risk Incorrect installation and use of hardware component


Treatment of risk
Denial of hardware component availability
Treatment of risk
Denial of hardware component authorization functionality
Risk avoidance
Reduction of likelihood
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Reduction of consequence
Risk transfer
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring

List of possible revisions:
- Eliminate the use of hardware component

List of possible revisions:
- introduce the strict rules for access to the room/area where hardware component is installed
- access to the room where hardware component is installed should be controlled by an electronic door lock
- provide regular security awareness training of employees
- hardware component should be fastened with screws to the wall, table or floor, and physical access to the hardware component should be secured with a lock

- Install hardware component in an other room/area with more strong access control

- Regular tests of access control to the room, area or building where critical components are installed
- Regular tests of employees/users security awareness
- Regular tests of security personal competence

- Install software for monitoring and detection of access to the room/area where hardware component is installed

List of possible revisions:
- Have an additional hardware component with the same functionality available
- Recovery from hardware component problems should be done only by competent users/ employees
- Recovery from hardware problems should be done only by specialized company (technical support)

- Install an additional hardware component with the same functionality on computer
- Install additional hardware component in an other room/area with better access control

- Test regularly the functionality of additional hardware component

- Install software for monitoring of additional hardware component functionality
- Install software for monitoring and detection of access to the room/area where additional hardware component is installed

List of possible revisions:
- Have an insurance that covers the financial consequences of unauthorized access to hardware component

Figure B.10: Template for treatment of risk Denial of hardware component authorization functionality

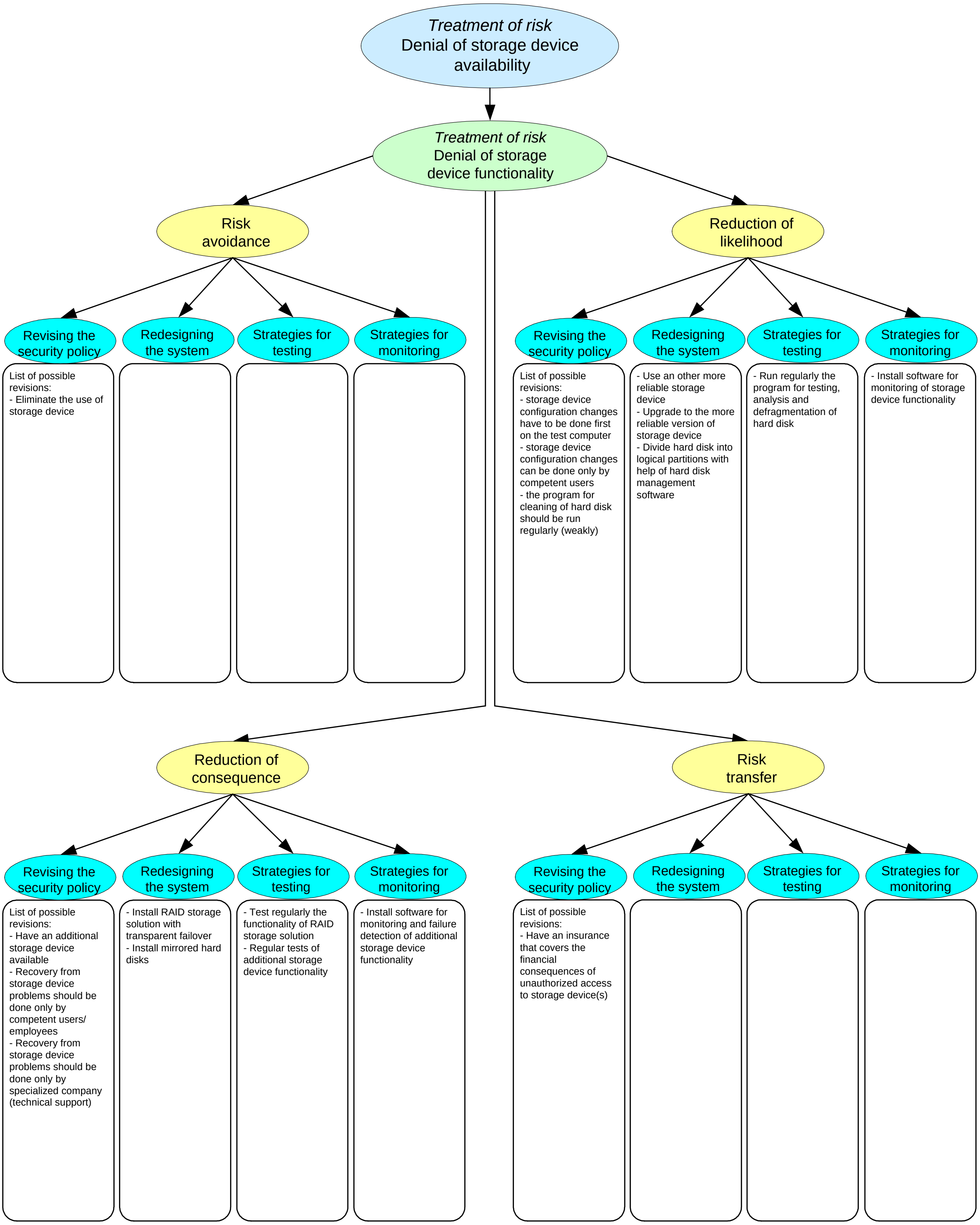
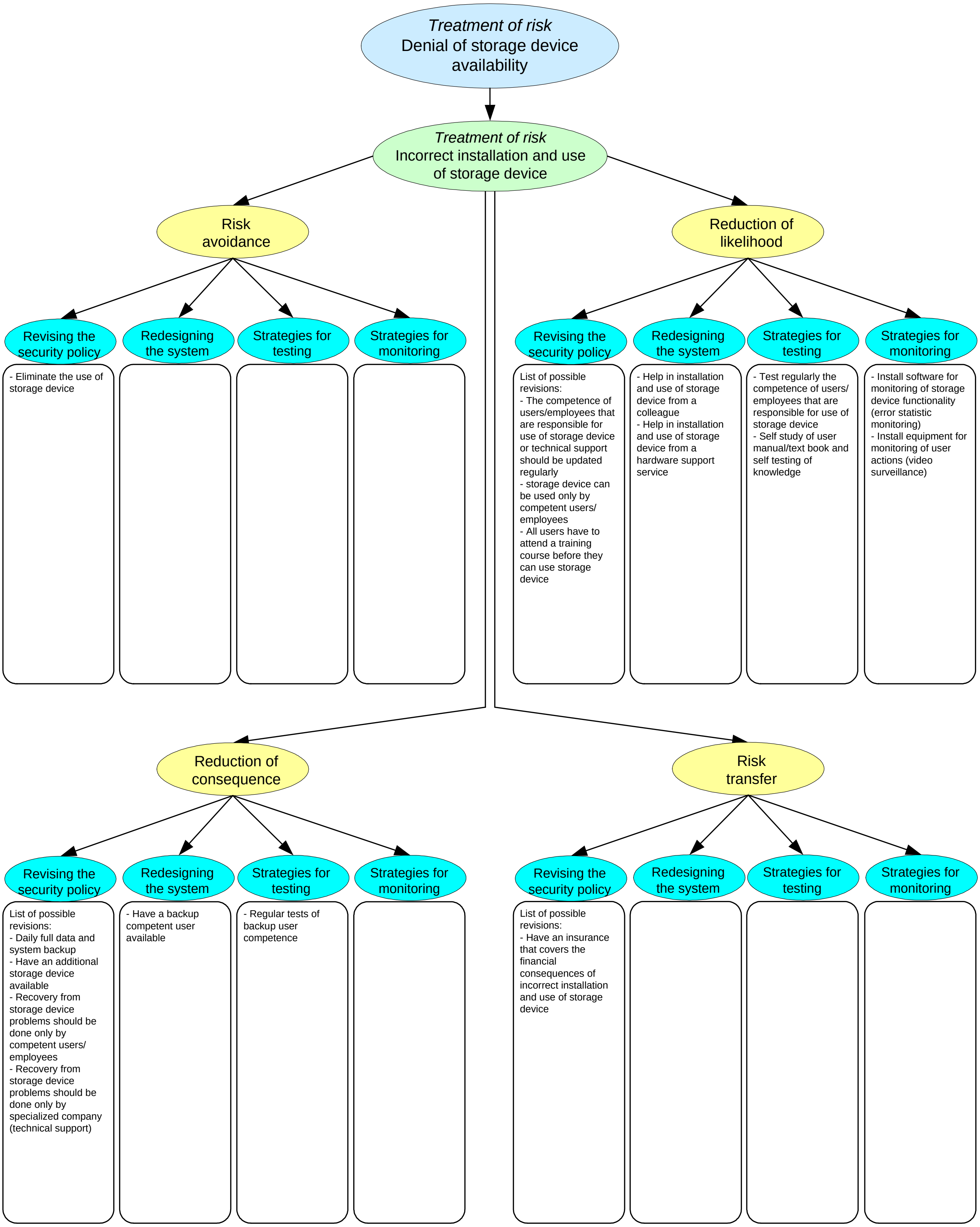

Treatment of risk
Denial of storage device availability
Treatment of risk
Denial of storage device functionality
Risk avoidance
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- Eliminate the use of storage device
Reduction of likelihood
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- storage device configuration changes have to be done first on the test computer
- storage device configuration changes can be done only by competent users
- the program for cleaning of hard disk should be run regularly (weakly)
- Use an other more reliable storage device
- Upgrade to the more reliable version of storage device
- Divide hard disk into logical partitions with help of hard disk management software
- Run regularly the program for testing, analysis and defragmentation of hard disk
- Install software for monitoring of storage device functionality
Reduction of consequence
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- Have an additional storage device available
- Recovery from storage device problems should be done only by competent users/ employees
- Recovery from storage device problems should be done only by specialized company (technical support)
- Install RAID storage solution with transparent failover
- Install mirrored hard disks
- Test regularly the functionality of RAID storage solution
- Regular tests of additional storage device functionality
- Install software for monitoring and failure detection of additional storage device functionality
Risk transfer
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- Have an insurance that covers the financial consequences of unauthorized access to storage device(s)

Figure B.11: Template for treatment of risk Denial of storage device functionality


Treatment of risk
Denial of storage device availability
Treatment of risk
Incorrect installation and use of storage device
Risk avoidance
Reduction of likelihood
Reduction of consequence
Risk transfer
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring

- Eliminate the use of storage device

List of possible revisions:
- The competence of users/employees that are responsible for use of storage device or technical support should be updated regularly
- storage device can be used only by competent users/ employees
- All users have to attend a training course before they can use storage device

- Help in installation and use of storage device from a colleague
- Help in installation and use of storage device from a hardware support service

- Test regularly the competence of users/ employees that are responsible for use of storage device
- Self study of user manual/text book and self testing of knowledge

- Install software for monitoring of storage device functionality (error statistic monitoring)
- Install equipment for monitoring of user actions (video surveillance)

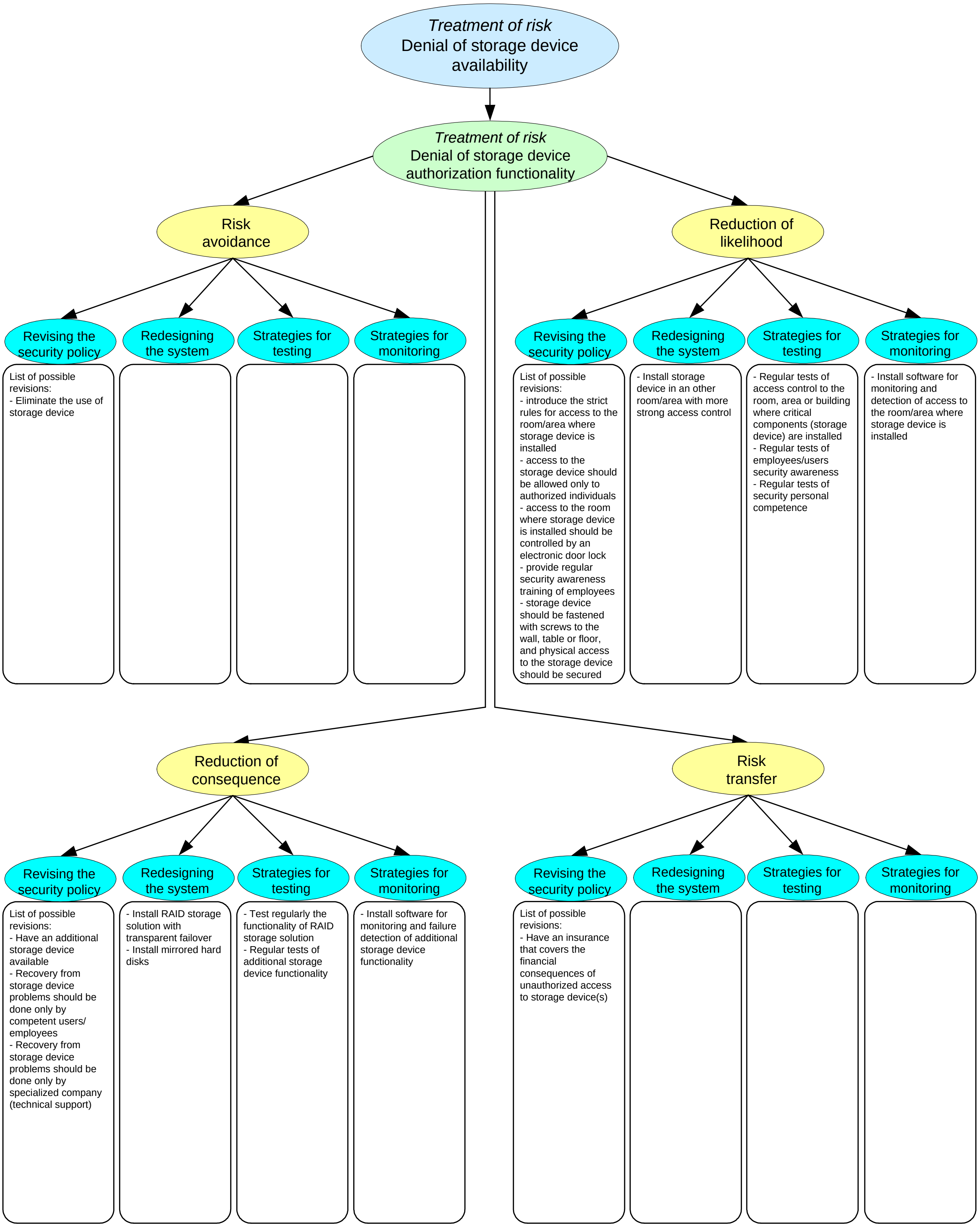
List of possible revisions:
- Daily full data and system backup
- Have an additional storage device available
- Recovery from storage device problems should be done only by competent users/ employees
- Recovery from storage device problems should be done only by specialized company (technical support)

- Have a backup competent user available

- Regular tests of backup user competence

List of possible revisions:
- Have an insurance that covers the financial consequences of incorrect installation and use of storage device

Figure B.12: Template for treatment of risk Incorrect installation and use of storage device



Risk avoidance – Revising the security policy:

List of possible revisions:
- Eliminate the use of storage device

Reduction of likelihood – Revising the security policy:

List of possible revisions:
- introduce the strict rules for access to the room/area where storage device is installed
- access to the storage device should be allowed only to authorized individuals
- access to the room where storage device is installed should be controlled by an electronic door lock
- provide regular security awareness training of employees
- storage device should be fastened with screws to the wall, table or floor, and physical access to the storage device should be secured

Reduction of likelihood – Redesigning the system:

- Install storage device in an other room/area with more strong access control

Reduction of likelihood – Strategies for testing:

- Regular tests of access control to the room, area or building where critical components (storage device) are installed
- Regular tests of employees/users security awareness
- Regular tests of security personal competence

Reduction of likelihood – Strategies for monitoring:

- Install software for monitoring and detection of access to the room/area where storage device is installed

Reduction of consequence – Revising the security policy:

List of possible revisions:
- Have an additional storage device available
- Recovery from storage device problems should be done only by competent users/ employees
- Recovery from storage device problems should be done only by specialized company (technical support)

Reduction of consequence – Redesigning the system:

- Install RAID storage solution with transparent failover
- Install mirrored hard disks

Reduction of consequence – Strategies for testing:

- Test regularly the functionality of RAID storage solution
- Regular tests of additional storage device functionality

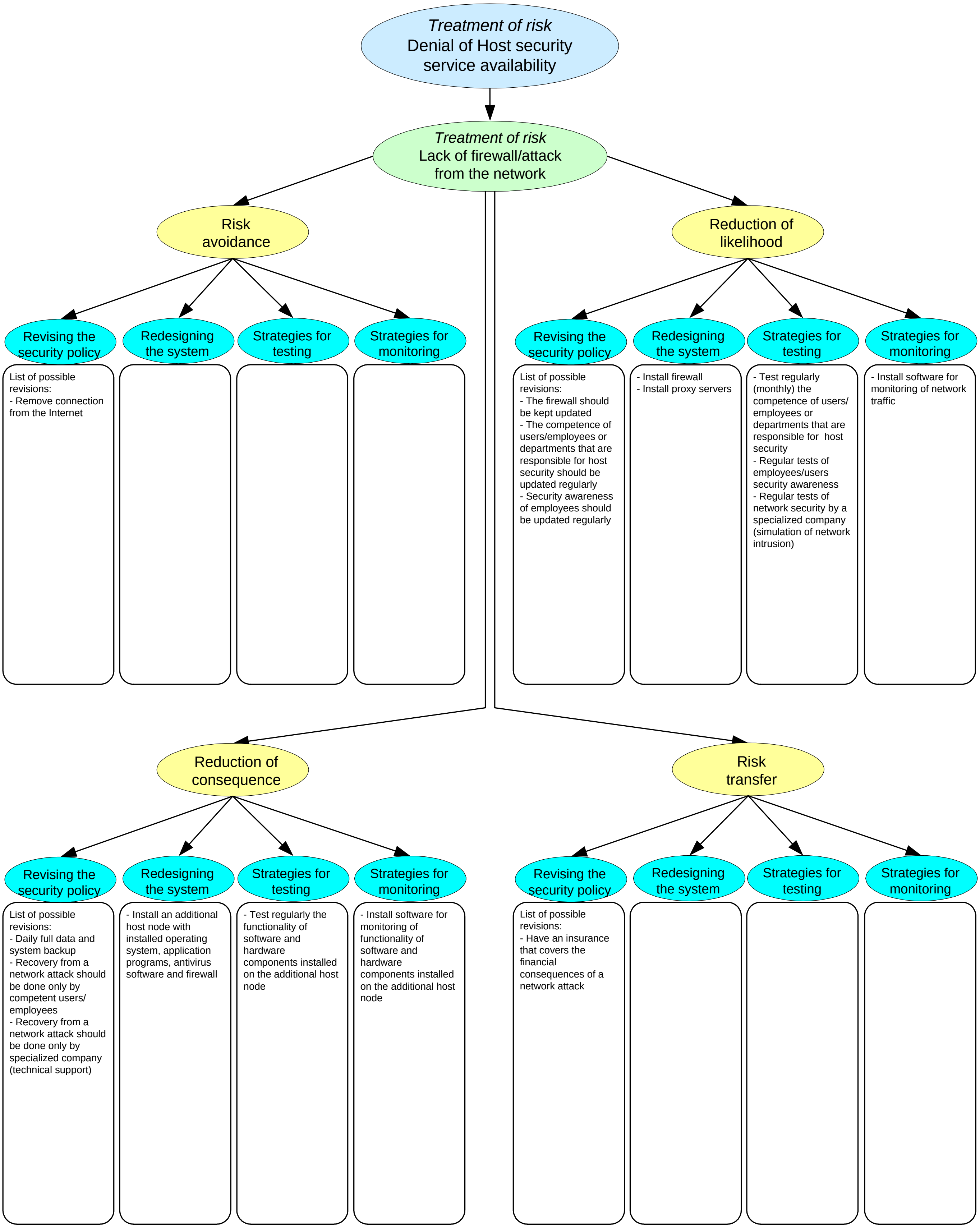
Reduction of consequence – Strategies for monitoring:

- Install software for monitoring and failure detection of additional storage device functionality

Risk transfer – Revising the security policy:

List of possible revisions:
- Have an insurance that covers the financial consequences of unauthorized access to storage device(s)

Figure B.13: Template for treatment of risk Denial of storage device authorization functionality



Risk avoidance – Revising the security policy:

List of possible revisions:
- Remove connection from the Internet

Reduction of likelihood – Revising the security policy:

List of possible revisions:
- The firewall should be kept updated
- The competence of users/employees or departments that are responsible for host security should be updated regularly
- Security awareness of employees should be updated regularly

Reduction of likelihood – Redesigning the system:

- Install firewall
- Install proxy servers

Reduction of likelihood – Strategies for testing:

- Test regularly (monthly) the competence of users/ employees or departments that are responsible for host security
- Regular tests of employees/users security awareness
- Regular tests of network security by a specialized company (simulation of network intrusion)

Reduction of likelihood – Strategies for monitoring:

- Install software for monitoring of network traffic

Reduction of consequence – Revising the security policy:

List of possible revisions:
- Daily full data and system backup
- Recovery from a network attack should be done only by competent users/ employees
- Recovery from a network attack should be done only by specialized company (technical support)

Reduction of consequence – Redesigning the system:

- Install an additional host node with installed operating system, application programs, antivirus software and firewall

Reduction of consequence – Strategies for testing:

- Test regularly the functionality of software and hardware components installed on the additional host node

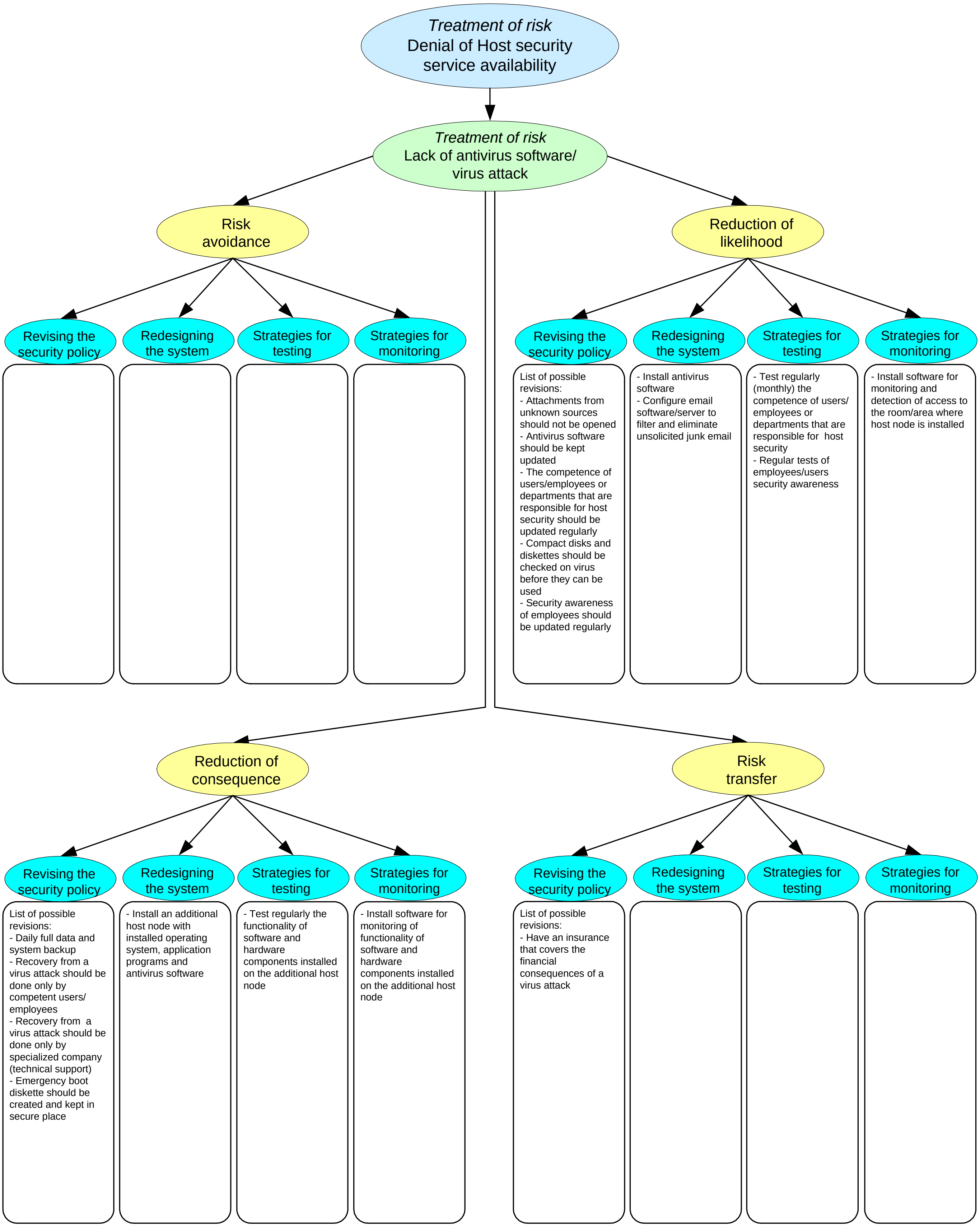
Reduction of consequence – Strategies for monitoring:

- Install software for monitoring of functionality of software and hardware components installed on the additional host node

Risk transfer – Revising the security policy:

List of possible revisions:
- Have an insurance that covers the financial consequences of a network attack

Figure B.14: Template for treatment of risk Lack of firewall/Attack from the network


Treatment of risk
Denial of Host security service availability
Treatment of risk
Lack of antivirus software/ virus attack
Risk avoidance
Reduction of likelihood
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Reduction of consequence
Risk transfer
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring

List of possible revisions:
- Attachments from unknown sources should not be opened
- Antivirus software should be kept updated
- The competence of users/employees or departments that are responsible for host security should be updated regularly
- Compact disks and diskettes should be checked on virus before they can be used
- Security awareness of employees should be updated regularly

- Install antivirus software
- Configure email software/server to filter and eliminate unsolicited junk email

- Test regularly (monthly) the competence of users/ employees or departments that are responsible for host security
- Regular tests of employees/users security awareness

- Install software for monitoring and detection of access to the room/area where host node is installed

List of possible revisions:
- Daily full data and system backup
- Recovery from a virus attack should be done only by competent users/ employees
- Recovery from a virus attack should be done only by specialized company (technical support)
- Emergency boot diskette should be created and kept in secure place

- Install an additional host node with installed operating system, application programs and antivirus software

- Test regularly the functionality of software and hardware components installed on the additional host node

- Install software for monitoring of functionality of software and hardware components installed on the additional host node

List of possible revisions:
- Have an insurance that covers the financial consequences of a virus attack

Figure B.15: Template for treatment of risk Lack of antivirus software/Virus attack

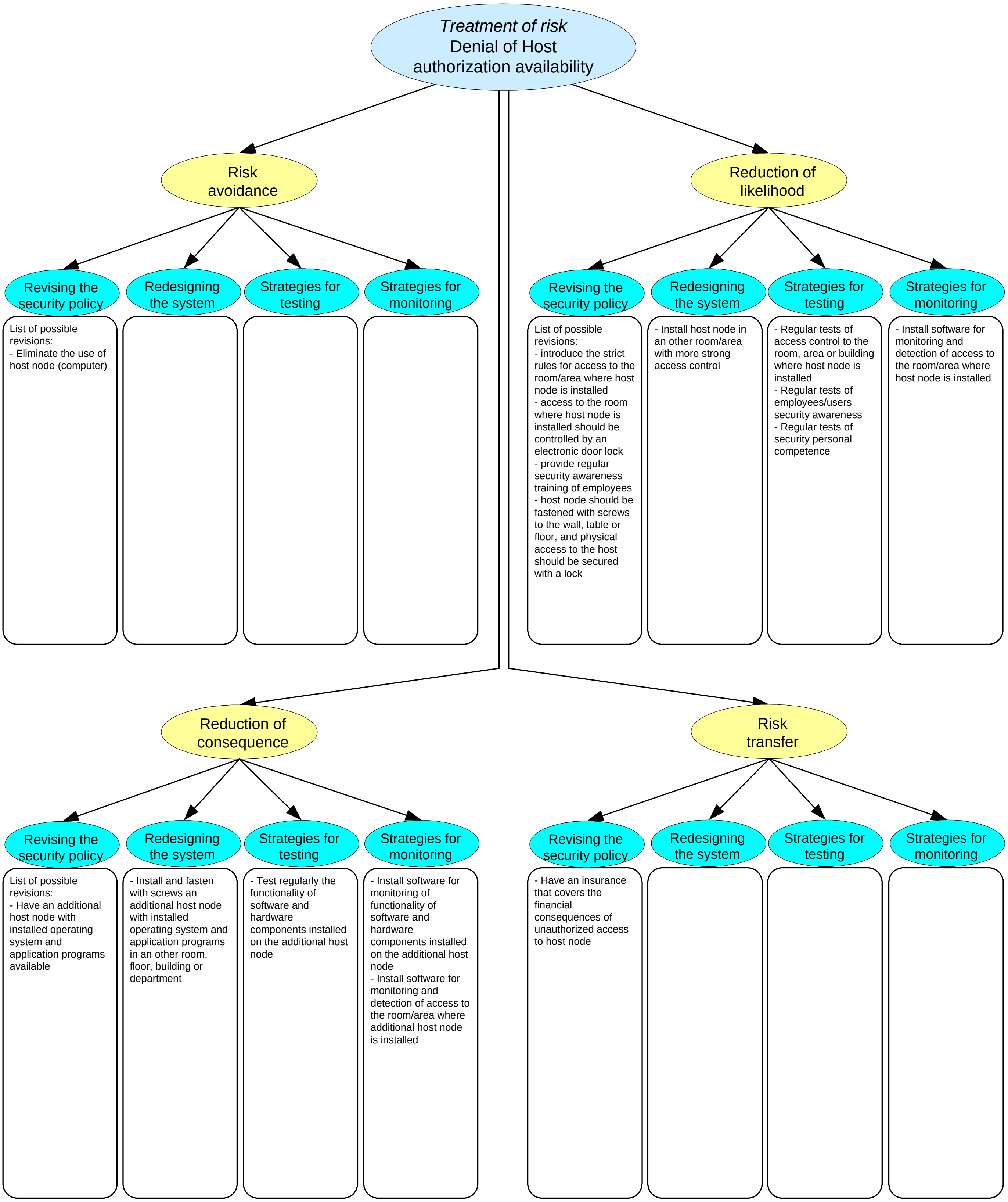


Figure B.16: Template for treatment of risk Denial of Host authorization availability

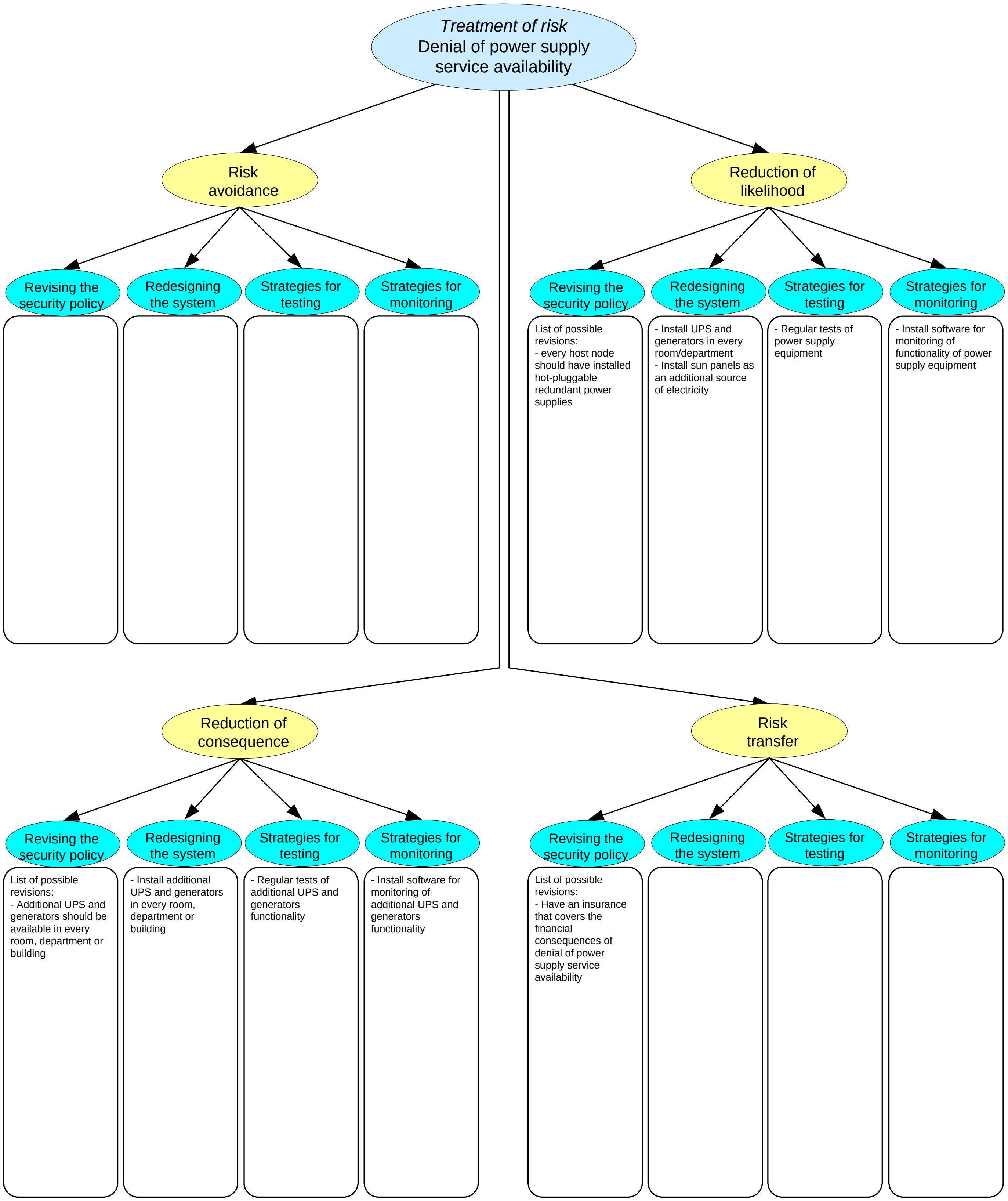

Treatment of risk
Denial of power supply service availability
Risk avoidance
Reduction of likelihood
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- every host node should have installed hot-pluggable redundant power supplies
- Install UPS and generators in every room/department
- Install sun panels as an additional source of electricity
- Regular tests of power supply equipment
- Install software for monitoring of functionality of power supply equipment
Reduction of consequence
Risk transfer
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- Additional UPS and generators should be available in every room, department or building
- Install additional UPS and generators in every room, department or building
- Regular tests of additional UPS and generators functionality
- Install software for monitoring of additional UPS and generators functionality
List of possible revisions:
- Have an insurance that covers the financial consequences of denial of power supply service availability

Figure B.17: Template for treatment of risk Denial of power supply service availability

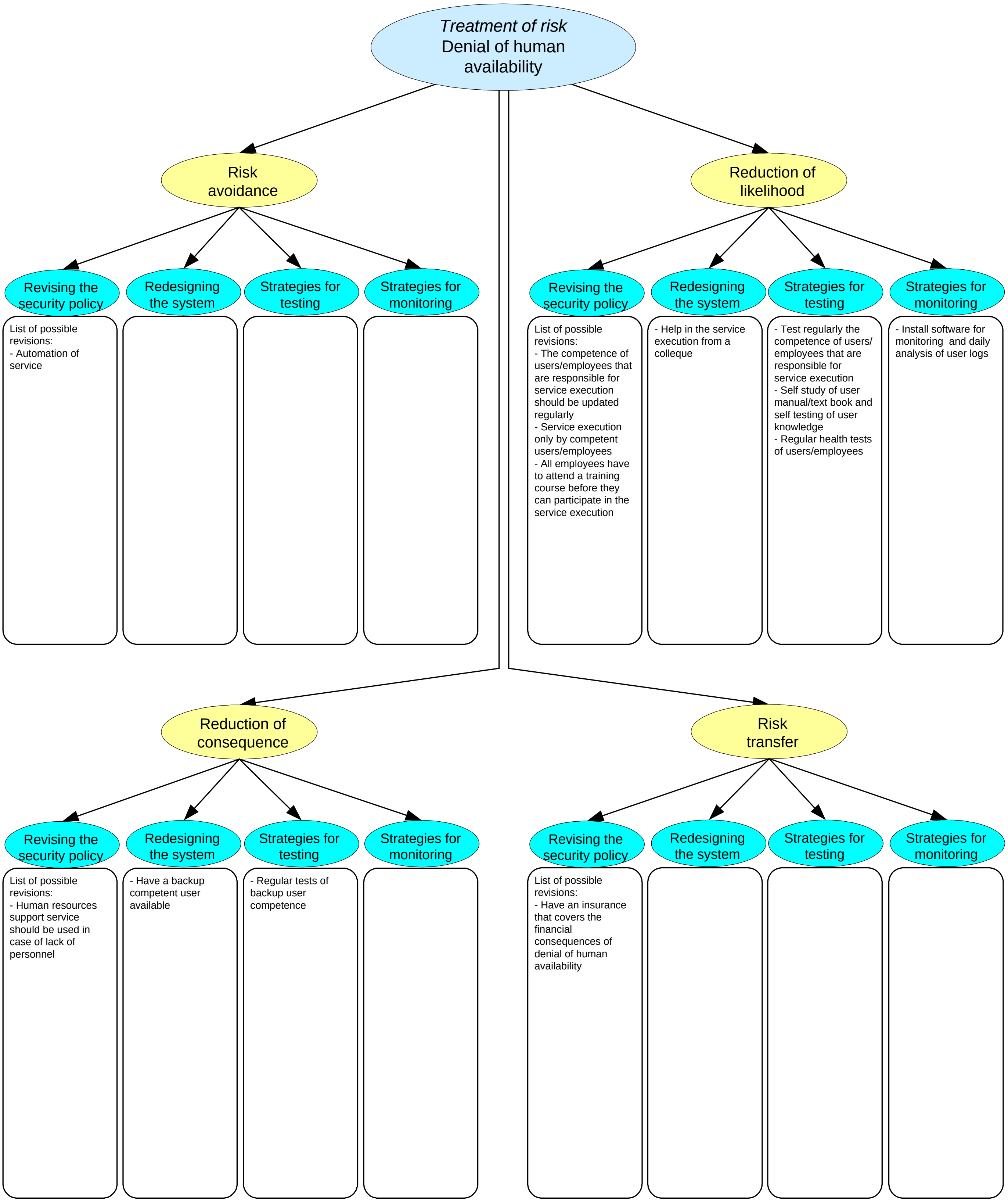
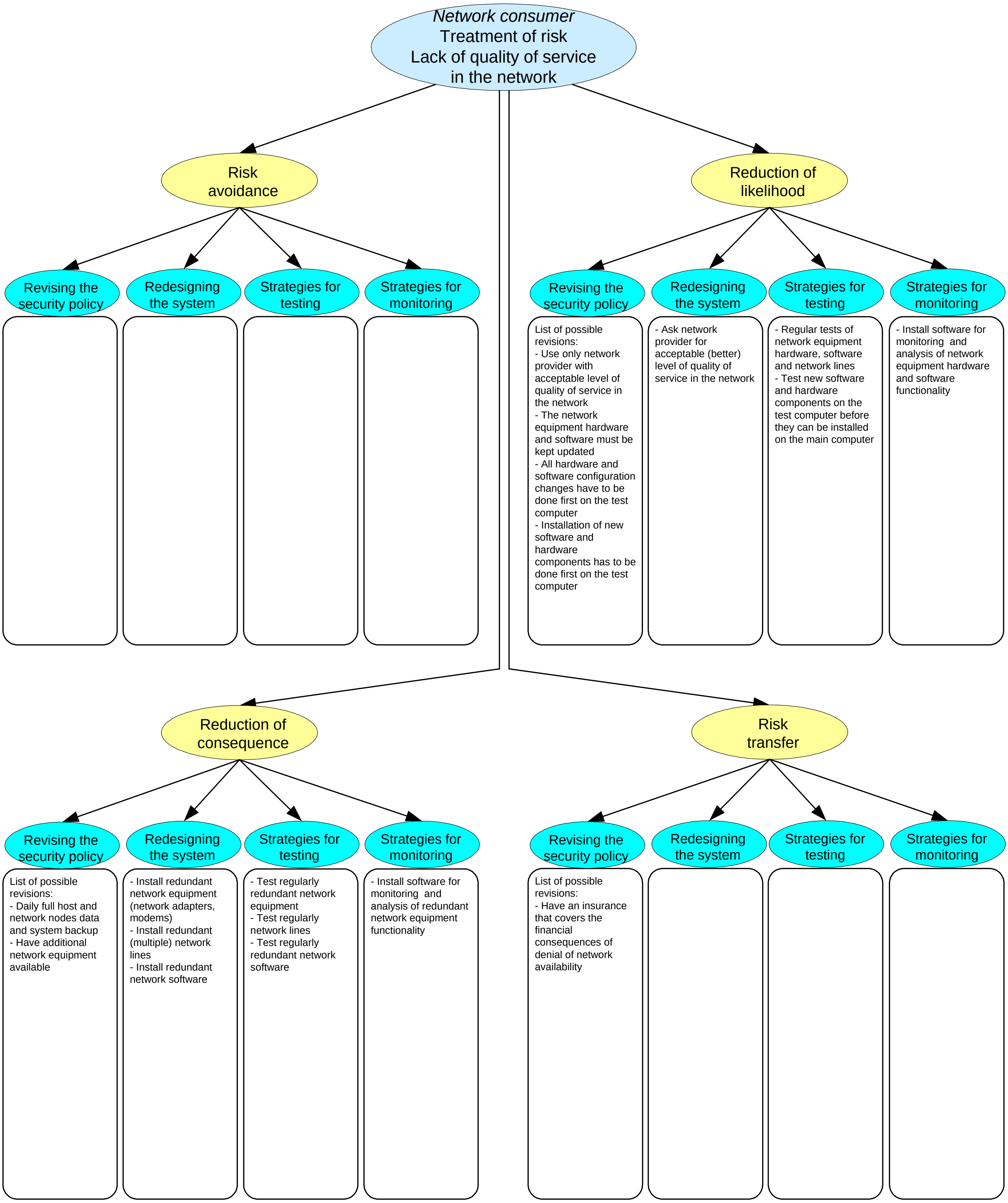

Treatment of risk
Denial of human availability
Risk avoidance
Reduction of likelihood
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- Automation of service
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- The competence of users/employees that are responsible for service execution should be updated regularly
- Service execution only by competent users/employees
- All employees have to attend a training course before they can participate in the service execution
- Help in the service execution from a colleque
- Test regularly the competence of users/ employees that are responsible for service execution
- Self study of user manual/text book and self testing of user knowledge
- Regular health tests of users/employees
- Install software for monitoring and daily analysis of user logs
Reduction of consequence
Risk transfer
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- Human resources support service should be used in case of lack of personnel
- Have a backup competent user available
- Regular tests of backup user competence
Revising the security policy
Redesigning the system
Strategies for testing
Strategies for monitoring
List of possible revisions:
- Have an insurance that covers the financial consequences of denial of human availability

Figure B.18: Template for treatment of risk Denial of Human availability



List of possible revisions:
- Use only network provider with acceptable level of quality of service in the network
- The network equipment hardware and software must be kept updated
- All hardware and software configuration changes have to be done first on the test computer
- Installation of new software and hardware components has to be done first on the test computer

- Ask network provider for acceptable (better) level of quality of service in the network

- Regular tests of network equipment hardware, software and network lines
- Test new software and hardware components on the test computer before they can be installed on the main computer

- Install software for monitoring and analysis of network equipment hardware and software functionality

List of possible revisions:
- Daily full host and network nodes data and system backup
- Have additional network equipment available

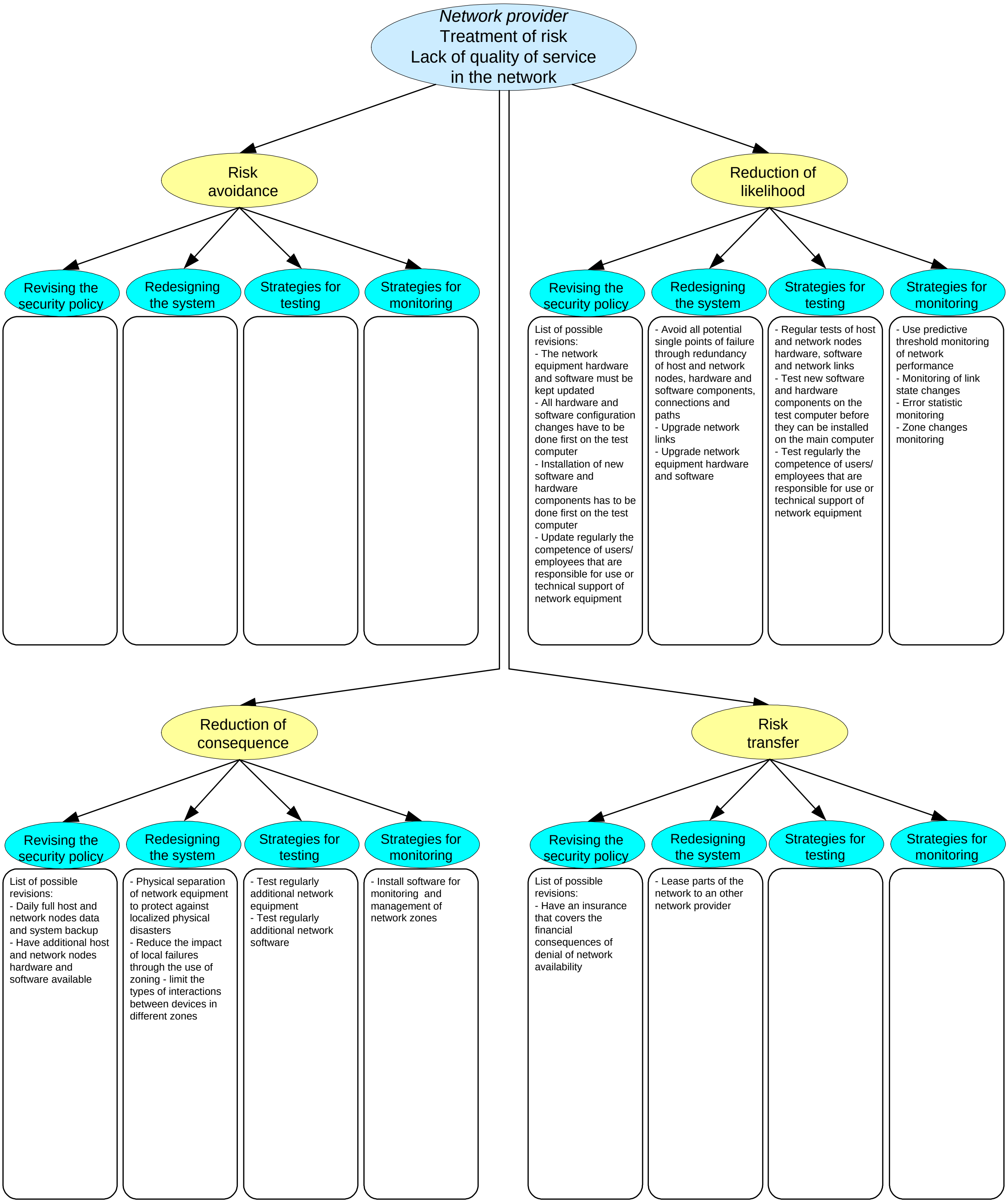
- Install redundant network equipment (network adapters, modems)
- Install redundant (multiple) network lines
- Install redundant network software

- Test regularly redundant network equipment
- Test regularly network lines
- Test regularly redundant network software

- Install software for monitoring and analysis of redundant network equipment functionality

List of possible revisions:
- Have an insurance that covers the financial consequences of denial of network availability

Figure B.19: Template for treatment of risk Lack of quality of service in the network (Network consumer)



Reduction of likelihood – Revising the security policy:

List of possible revisions:
- The network equipment hardware and software must be kept updated
- All hardware and software configuration changes have to be done first on the test computer
- Installation of new software and hardware components has to be done first on the test computer
- Update regularly the competence of users/ employees that are responsible for use or technical support of network equipment

Reduction of likelihood – Redesigning the system:

- Avoid all potential single points of failure through redundancy of host and network nodes, hardware and software components, connections and paths
- Upgrade network links
- Upgrade network equipment hardware and software

Reduction of likelihood – Strategies for testing:

- Regular tests of host and network nodes hardware, software and network links
- Test new software and hardware components on the test computer before they can be installed on the main computer
- Test regularly the competence of users/ employees that are responsible for use or technical support of network equipment

Reduction of likelihood – Strategies for monitoring:

- Use predictive threshold monitoring of network performance
- Monitoring of link state changes
- Error statistic monitoring
- Zone changes monitoring

Reduction of consequence – Revising the security policy:

List of possible revisions:
- Daily full host and network nodes data and system backup
- Have additional host and network nodes hardware and software available

Reduction of consequence – Redesigning the system:

- Physical separation of network equipment to protect against localized physical disasters
- Reduce the impact of local failures through the use of zoning - limit the types of interactions between devices in different zones

Reduction of consequence – Strategies for testing:

- Test regularly additional network equipment
- Test regularly additional network software

Reduction of consequence – Strategies for monitoring:

- Install software for monitoring and management of network zones

Risk transfer – Revising the security policy:

List of possible revisions:
- Have an insurance that covers the financial consequences of denial of network availability

Risk transfer – Redesigning the system:

- Lease parts of the network to an other network provider

Figure B.20: Template for treatment of risk Lack of quality of service in the network (Network provider)

Appendix C.

This appendix is structured into two sections. Section C.1 provides risk treatment tables for Private Lessons. Section C.2 provides risk treatment priorities tables for Private Lessons.

C.1 Private Lessons: Risk treatment tables

Table C.1: Private Lessons Treatment table for network availability risks (network consumer)

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Denial of network availability (Lack of quality of service in the network: bandwidth, timeliness, reliability/ stability)	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Use only network provider with acceptable level of quality of service in the network	Quality of Internet connection can usually be on the acceptable level	Cost of network access from the new network provider
				Network equipment hardware and software must be kept updated	Insure reliable functionality of network equipment hardware and software	Cost of work time of the teacher (updates) and cost of updates
			2)	Ask network provider for acceptable (better) level of quality of service in the network	Quality of Internet connection can usually be on the acceptable level	Cost of network access from the network provider
			3)	Regular tests of network equipment hardware and software	Early discovering and preventing of network equipment hardware and software problems	Cost of work time of the teacher (tests) and cost of tests
			4)	Install software for monitoring of network equipment hardware and software functionality	Early discovering and preventing of network equipment hardware and software problems	Cost of work time of the teacher (installation) and cost of software
		c)	**1)**	Have additional network equipment available	Quick change of failed network equipment	Cost of additional network equipment
			2)	Install redundant network equipment	Reduce the consequence of network equipment failure	Cost of additional network equipment
			3)	Test regularly redundant network equipment	Insure correct functionality of redundant network equipment – insure possibility for replacement of failed network equipment	Cost of work time of the teacher (tests) and cost of tests
			4)	Install software for monitoring and analysis of redundant network equipment functionality	Insure correct functionality of redundant network equipment – insure possibility for replacement of failed network equipment	Cost of installation (work hours), cost of hardware and software and cost of monitoring
		d)	**1)**	Have an insurance that covers the financial consequences of denial of network availability	Reduce the financial consequences of denial of network availability	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

Table C.2: Private Lessons Treatment table for host operating system availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Denial of operating system functionality	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Operating system must be kept updated	More stable and effective operating system	Cost of work time of the teacher (update) and cost of update
			2)	Install another more reliable operating system	More reliable and stable functionality of OS	Cost of work time of the teacher (installation) and cost of OS
				Upgrade to the more reliable version of OS	More reliable and stable functionality of OS	Cost of work time of the teacher (update) and cost of update
			3)	Regular tests of operating system	Early discovering and preventing of operating system problems	Cost of work time of the teacher (tests) and cost of tests
			4)	Install software for monitoring of operating system functionality	Early discovering and preventing of operating system problems	Cost of work time of the teacher (installation) and cost of software
		c)	**1)**	Daily full data and system backup	Insure possibility for recovery from operating system problems	Cost of work time of the teacher (backup) and cost of backup software and hardware
				Emergency boot diskette should be created	Insure possibility for recovery from operating system problems	Cost of diskette
			2)	Install OS and application programs on additional work station	Insure possibility for recovery from operating system problems – use of additional work station in case of denial of OS functionality on the main workstation	Cost of additional work station and cost of work time of the teacher (installation)
			3)	Regular tests of OS installed on additional work station	Insure correct functionality of OS on additional work station - use of additional work station in case of denial of OS functionality on the main workstation	Cost of work station, installation (the teacher work hours) and cost of tests
			4)	Install software on additional work station for monitoring of operating system functionality	Insure correct functionality of OS on additional work station - use of additional work station in case of denial of OS functionality on the main workstation	Cost of installation (the teacher work hours) and cost of software
		d)	**1)**	Have an insurance that covers the financial consequences of denial of operating system functionality	Reduce financial consequences of denial of operating system functionality	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

	Incorrect installation and use of operating system	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	The competence of users/employees responsible for use of OS should be updated regularly (regular training courses)	More correct use of operating system	Cost of training course
			2)	Help in installation and use of OS from a software support service	More correct and efficient use of operating system	Cost of software support service
			3)	Self study of user manual/text book and self testing of knowledge	More correct and efficient use of operating system	Cost of book/teaching program
			4)			
		c)	**1)**	Use software support service for recovery from OS problems	Quick recovery from OS problems	Cost of software support service
			2)	Have a backup competent user available	Possible more efficient use of operating system. OS user can always get quick help from competent user	Cost of work time of backup user
			3)			
			4)			
		d)	**1)**	Have an insurance that covers the financial consequences of incorrect use of OS	Reduce financial consequences of incorrect use of operating system.	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

	Denial of operating system authorization functionality	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Introduce the strict rules for choosing or changing of password	Insure strong protection against unauthorized access to OS	Cost of work time of the teacher/specialist to formulate the rules
				Use the screensaver with password protection	Better protection of OS against unauthorized access	Cost of time to change screensaver options
				Users should always logout whenever they leave computer for any period of time	Better protection of OS against unauthorized access	Cost of time to logout
			2)	Use another operating system with more strong access control	Insure effective OS access control	Cost of work time of the teacher (installation) and cost of OS
			3)	Self study of user manual/text book about host (OS) security and self testing of knowledge	Better protection of OS against unauthorized access	Cost of book/manual
			4)	Install software for monitoring and analysis of user logs	Insure access of only authorized users	Cost of software
		c)	**1)**	Daily full data and system backup	Quick recovery from OS problems	Cost of work time of the teacher and cost of backup software and hardware
			2)	Install OS and application programs on additional work station	Quick recovery from operating system problems - insure high service availability	Cost of additional work station and cost of work time of the teacher (installation)
			3)	Regular tests of OS installed on additional work station	Insure correct functionality of additional work station - insure high service availability	Cost of work station, installation (work hours) and cost of tests
			4)	Install software on additional work station for monitoring of OS functionality and analysis of user logs	Insure correct functionality of additional work station and access of only authorized users – better availability of service	Cost of work time of the teacher (installation) and cost of software
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to operating system	Reduce financial consequences of unauthorized access to operating system	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

Table C.3: Private Lessons Treatment table for host storage device availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Incorrect installation and use of hard disk	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Use of hard disc only by users that have completed training course	More correct use and installation of hard disc by user	Cost of arrangement or attendance of training course
			2)	Help in installation and use of hard disc from a colleague	More correct and efficient use of hard disc	Cost of colleague work time
			3)	User has to study a text book about installation and use of hard disc or study and test his knowledge with help of teaching interacting program	More correct and efficient use of hard disc	Cost of book/teaching program
			4)			
		c)	**1)**	Use hardware support service	Quick recovery from hard disc problems	Cost of hardware support service
			2)	Have a backup competent user available	Possible more efficient use of hard disc. Hard disk user can always get quick help from competent user	Cost of work time of backup user
			3)			
			4)			
		d)	**1)**	Have an insurance that covers the financial consequences of incorrect use of hardware component	Reduce financial consequences of incorrect use of hardware component	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

	Denial of hard disk functionality	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Run regularly (weakly) the program for cleaning of hard disk	More stable and effective hard disk functionality	Cost of work time of the teacher (cleaning) and cost of software
			2)	Divide hard disk into logical partitions with help of hard disk management software	Possible more stable and effective functionality of hard disk. Reduction of consequence of disk crash	Cost of work time of the teacher (installation) and cost of software
			3)	Run regularly (weakly) the program for analysis and defragmentation of hard disk	More stable and effective hard disk functionality	Cost of work time of the teacher and cost of analysis software
			4)	Install software for monitoring of hard disk functionality	Early discovering and preventing of hard disk problems	Cost of work time of the teacher (installation) and cost of software
		c)	**1)**	Have an additional hard disk available	The new hard disk can be quickly installed in case of denial of the old hard disk	Cost of additional hard disk
			2)	Install RAID storage solution with transparent failover	Higher availability of host hard disk	Cost of RAID system and cost of installation
			3)	Regular tests of additional hard disk functionality	Insure correct functionality of additional hard disk - insure possibility for its use in case of denial of main hard disk	Cost of tests
			4)	Install software for monitoring and failure detection of additional hard disk functionality	Insure correct functionality of additional hard disk - insure possibility for its use in case of denial of main hard disk	Cost of installation (work hours) and cost of software
		d)	**1)**	Have an insurance that covers the financial consequences of denial of hard disk functionality	Reduce financial consequences of denial of hard disk functionality	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

	Denial of hard disk authorization functionality	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Access to the room where hard disk is installed should be protected by a door with a lock	Insure protection against unauthorized access to hard disk	Cost of work time of the teacher/specialist to formulate the rules
				External hard disk should be fastened with screws to a wall, floor or table and physical access to the hard disk should be secured with a lock	Insure protection against unauthorized access to hard disk	Cost of work time of the teacher (installation) and cost of equipment (screws, lock)
			2)	Install hard disk in another room/area with more strong access control	Insure protection against unauthorized access to hard disk	Cost of work time of the teacher (installation)
			3)	Self study of user manual/text book about host security and self testing of knowledge	Better protection of hard disk against unauthorized access	Cost of book/manual
			4)	Install software for monitoring and detection of access to the room/area where hard disk is installed	Insure access to hard disk of only authorized users	Cost of work time of the teacher (installation) and cost of software
		c)	**1)**	Have an additional hard disk available	The new hard disk can be quickly installed in case of a damage of the old hard disk	Cost of additional hard disk
			2)			
			3)			
			4)			
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to hard disk	Reduce financial consequences of unauthorized access to hard disk	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

Table C.4: Private Lessons Treatment table for host authorization availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Denial of Host authorization availability	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Host node should be fastened with screws to a wall, floor or table and physical access to the host node should be secured with a lock	Improve protection against unauthorized access to host node	Cost of work time of the teacher (installation) and cost of equipment (screws, lock)
				Access to the room where host node is installed should be protected by door with a lock	Improve protection against unauthorized access to host node	Cost of work time of the teacher/specialist to formulate the rules
			2)	Install host node in another room/area with more strong access control	Improve protection against unauthorized access to host node	Cost of work time of the teacher (installation)
			3)	Self study of user manual/text book about host security and self testing of knowledge	Better protection of host node against unauthorized access	Cost of book/manual
			4)	Install software for monitoring and detection of access to the room/area where host node is installed	Insure access to the host node of only authorized users (The teacher)	Cost of work time of the teacher (installation) and cost of software
		c)	**1)**	Have an additional host node with installed operating system and application programs available	Better availability of service in case of damage (denial) of original host node	Cost of additional host node
			2)	Install and fasten with screws an additional host node with installed OS and application programs in another room with more strong access control	Improve protection against unauthorized access to additional host node – insure possibility of its use in case of denial of the main host node	Cost of work time of the teacher (installation) and cost of additional host node
			3)	Test regularly (monthly) the functionality of OS and application programs installed on additional host node	Insure correct and effective functionality of additional host node – denial of functionality of original host node will not affect service availability	Cost of work time of the teacher (tests)
			4)	Install software for monitoring and detection of access to the room/area where additional host node is installed	Insure access to additional host node of only authorized users – insure possibility of its use in case of denial of the main host node	Cost of work time of the teacher (installation) and cost of software
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to host node	Reduce financial consequences of unauthorized access to host node	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

Table C.5: Private Lessons Treatment table for host security service availability risks (antivirus software)

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Lack of antivirus software/virus attack	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Attachment from unknown sources should not be opened	Reduce the possibility for virus attack	No cost
				Compact disks and diskettes should be virus checked before they can be used	Reduce the possibility for virus attack	No cost
				Antivirus software should be regularly updated	Reduce the possibility for virus attack	Cost of update
			2)	Install antivirus software	Reduce the possibility for virus attack	Cost of software
			3)	Self study of user manual/text book about host security and self testing of knowledge	Better protection of host node against virus attack	Cost of book/manual
			4)	Secure physical access to the host and install video surveillance equipment for monitoring of access to the computer	Insure access to the host of only authorized users – reduction of possibility of virus attack caused by unauthorized physical access to the host	Cost of work time of the teacher (installation) and cost of video and access control equipment
		c)	**1)**	Daily full data and system backup	Higher availability of operating system, application programs and data –reduction of virus attack consequence	Cost of work time of the teacher (backup) and cost of backup software and hardware
			2)	Install OS, application programs and antivirus software on additional work station	Use of additional work station in case of denial of functionality of the main work station	Cost of additional work station and cost of work time of the teacher (installation)
			3)	Regular tests of OS and application programs installed on additional work station	Insure possibility for use of additional work station in case of denial of functionality of the main work station	Cost of work station, installation of OS and application programs (work hours) and cost of tests
			4)	Install software on additional work station for monitoring of OS functionality	Insure possibility for use of additional work station in case of denial of functionality of the main work station	Cost of work time of the teacher (installation) and cost of software
		d)	**1)**	Have an insurance that covers the financial consequences of virus attack	Reduce financial consequences of virus attack	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

Table C.6: Private Lessons Treatment table for host security service availability risks (firewall)

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Lack of firewall/attack from the network	**a)**	**1)**	Remove connection from the Internet	Eliminate the possibility of attack from the Internet	Possible reduction of service availability and revenue
			2)			
			3)			
			4)			
		b)	**1)**	Firewall should be regularly updated	Reduce the possibility for virus attack	Cost of update
			2)	Install firewall	Better protection of host node against network attacks	Cost of work time of the teacher (installation) and cost of software
			3)	Self study of user manual/text book about host security and self testing of knowledge	Better protection of host node against network attacks	Cost of book/manual
			4)	Install software for monitoring of network traffic	Early discovering and preventing of network problems – better protection against possible network attack	Cost of work time of the teacher (installation) and cost of software
		c)	**1)**	Daily full data and system backup	Higher availability of operating system, application programs and data –reduction of network attack consequence	Cost of work time of the teacher (backup) and cost of backup software and hardware
			2)	Install OS, application programs and antivirus software on additional work station	Use of additional work station in case of denial of functionality of the main work station	Cost of additional work station and cost of work time of the teacher (installation)
			3)	Regular tests of OS and application programs installed on additional work station	Insure possibility for use of additional work station in case of denial of functionality of the main work station	Cost of work station, installation of OS and application programs (work hours) and cost of tests
			4)	Install software on additional work station for monitoring of OS functionality	Insure possibility for use of additional work station in case of denial of functionality of the main work station	Cost of work time of the teacher (installation) and cost of software
		d)	**1)**	Have an insurance that covers the financial consequences of network attack	Reduction of financial consequences of network attack	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

C.2 Private Lessons: Risk treatment priorities tables

Table C.7: Private Lessons Treatment priority table for network availability risks (network consumer)

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost	Treatment action priority
	Denial of network availability (Lack of quality of service in the network bandwidth, timeliness, reliability/ stability)	**a)**	**1)**				
			2)				
			3)				
			4)				
		b)	**1)**	Use only network provider with acceptable level of quality of service in the network	High	Moderate	High
				Network equipment hardware and software must be kept updated	Moderate	Low	Moderate
			2)	Ask network provider for acceptable (better) level of quality of service in the network	High	Moderate	High
			3)	Regular tests of network equipment hardware and software	Moderate	Low	Moderate
			4)	Install software for monitoring of network equipment hardware and software functionality	Low	Moderate	Low
		c)	**1)**	Have additional network equipment available	High	Moderate	High
			2)	Install redundant network equipment	High	Moderate	High
			3)	Test regularly redundant network equipment	Low	Low	Low
			4)	Install software for monitoring and analysis of redundant network equipment functionality	Low	Moderate	Low
		d)	**1)**	Have an insurance that covers the financial consequences of denial of network availability	Moderate	Very High	Low
			2)				
			3)				
			4)				
		e)	**1)**				
			2)				
			3)				
			4)				

Table C.8: Private Lessons Treatment priority table for host operating system availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost	Treatment action priority
	Denial of operating system functionality	**a)**	**1)**				
			2)				
			3)				
			4)				
		b)	**1)**	Operating system must be kept updated	High	Very Low	Very High
			2)	Install another more reliable operating system	High	High	Moderate
				Upgrade to the more reliable version of OS	High	Moderate	High
			3)	Regular tests of operating system	Moderate	Low	Moderate
			4)	Install software for monitoring of operating system functionality	Moderate	Moderate	Moderate
		c)	**1)**	Daily full data and system backup	High	Low	High
				Emergency boot diskette should be created	High	Very Low	Very High
			2)	Install OS and application programs on additional work station	High	High	Moderate
			3)	Regular tests of OS installed on additional work station	Moderate	High	Low
			4)	Install software on additional work station for monitoring of operating system functionality	Moderate	High	Low
		d)	**1)**	Have an insurance that covers the financial consequences of denial of operating system functionality	Moderate	Very High	Low
			2)				
			3)				
			4)				
		e)	**1)**				
			2)				
			3)				
			4)				

	Incorrect installation and use of operating system	**a)**	**1)**				
			2)				
			3)				
			4)				
		b)	**1)**	The competence of users/employees responsible for use of OS should be updated regularly (regular training courses)	High	Moderate	High
			2)	Help in installation and use of OS from a software support service	High	High	Moderate
			3)	Self study of user manual/text book and self testing of knowledge	High	Very Low	Very High
			4)				
		c)	**1)**	Use software support service for recovery from OS problems	High	High	Moderate
			2)	Have a backup competent user available	Moderate	High	Low
			3)				
			4)				
		d)	**1)**	Have an insurance that covers the financial consequences of incorrect use of OS	Moderate	Very High	Low
			2)				
			3)				
			4)				
		e)	**1)**				
			2)				
			3)				
			4)				

	Denial of operating system authorization functionality	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Introduce the strict rules for choosing or changing of password	High	Very Low	Very High
				Use the screensaver with password protection	High	Very Low	Very High
				Users should always logout whenever they leave computer for any period of time	High	Very Low	Very High
			2)	Use another operating system with more strong access control	Moderate	High	Low
			3)	Self study of user manual/text book about host (OS) security and self testing of knowledge	High	Very Low	Very High
			4)	Install software for monitoring and analysis of user logs	Moderate	Moderate	Moderate
		c)	**1)**	Daily full data and system backup	High	Low	High
			2)	Install OS and application programs on additional work station	High	High	Moderate
			3)	Regular tests of OS installed on additional work station	Moderate	High	Low
			4)	Install software on additional work station for monitoring of OS functionality and analysis of user logs	Moderate	High	Low
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to operating system	Moderate	Very High	Low
			2)				
			3)				
			4)				
		e)	**1)**				
			2)				
			3)				
			4)				

Table C.9: Private Lessons Treatment priority table for host storage device availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost	Treatment action priority
	Incorrect installation and use of hard disk	**a)**	**1)**				
			2)				
			3)				
			4)				
		b)	**1)**	Use of hard disc only by users that have completed training course	High	Moderate	High
			2)	Help in installation and use of hard disc from a colleague	High	High	Moderate
			3)	User has to study a text book about installation and use of hard disc or study and test his knowledge with help of teaching interacting program	High	Very Low	Very High
			4)				
		c)	**1)**	Use hardware support service	High	High	Moderate
			2)	Have a backup competent user available	Moderate	High	Low
			3)				
			4)				
		d)	**1)**	Have an insurance that covers the financial consequences of incorrect use of hardware component	Moderate	Very High	Low
			2)				
			3)				
			4)				
		e)	**1)**				
			2)				
			3)				
			4)				

	Denial of hard disk functionality	**a)**	**1)**				
			2)				
			3)				
			4)				
		b)	**1)**	Run regularly (weakly) the program for cleaning of hard disk	High	Very Low	Very High
			2)	Divide hard disk into logical partitions with help of hard disk management software	High	Very Low	Very High
			3)	Run regularly (weakly) the program for analysis and defragmentation of hard disk	High	Very Low	Very High
			4)	Install software for monitoring of hard disk functionality	High	Moderate	High
		c)	**1)**	Have an additional hard disk available	Moderate	Moderate	Moderate
			2)	Install RAID storage solution with transparent failover	High	Moderate	High
			3)	Regular tests of additional hard disk functionality	Moderate	Low	Moderate
			4)	Install software for monitoring and failure detection of additional hard disk functionality	Moderate	High	Low
		d)	**1)**	Have an insurance that covers the financial consequences of denial of hard disk functionality	Moderate	Very High	Low
			2)				
			3)				
			4)				
		e)	**1)**				
			2)				
			3)				
			4)				

	Denial of hard disk authorization functionality	**a)**	**1)**				
			2)				
			3)				
			4)				
		b)	**1)**	Access to the room where hard disk is installed should be protected by a door with a lock	High	Very Low	Very High
				External hard disk should be fastened with screws to a wall, floor or table and physical access to the hard disk should be secured with a lock	High	Very Low	Very High
			2)	Install hard disk in another room/area with more strong access control	Moderate	Moderate	Moderate
			3)	Self study of user manual/text book about host security and self testing of knowledge	High	Very Low	Very High
			4)	Install software for monitoring and detection of access to the room/area where hard disk is installed	Moderate	Moderate	Moderate
		c)	**1)**	Have an additional hard disk available	High	Moderate	High
			2)				
			3)				
			4)				
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to hard disk	Moderate	Very High	Low
			2)				
			3)				
			4)				
		e)	**1)**				
			2)				
			3)				
			4)				

Table C.10: Private Lessons Treatment priority table for host authorization availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost	Treatment action priority
	Denial of Host authorization availability	**a)**	**1)**				
			2)				
			3)				
			4)				
		b)	**1)**	Host node should be fastened with screws to a wall, floor or table and physical access to the host node should be secured with a lock	High	Very Low	Very High
				Access to the room where host node is installed should be protected by door with a lock	High	Very Low	Very High
			2)	Install host node in another room/area with more strong access control	Moderate	Moderate	Moderate
			3)	Self study of user manual/text book about host security and self testing of knowledge	High	Very Low	Very High
			4)	Install software for monitoring and detection of access to the room/area where host node is installed	Moderate	Moderate	Moderate
		c)	**1)**	Have an additional host node with installed operating system and application programs available	High	High	Moderate
			2)	Install and fasten with screws an additional host node with installed OS and application programs in another room with more strong access control	High	High	Moderate
			3)	Test regularly (monthly) the functionality of OS and application programs installed on additional host node	Moderate	Moderate	Moderate
			4)	Install software for monitoring and detection of access to the room/area where additional host node is installed	Moderate	Moderate	Moderate
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to host node	High	Very High	Moderate
			2)				
			3)				
			4)				
		e)	**1)**				
			2)				
			3)				
			4)				

Table C.11: Private Lessons Treatment priority table for host security service availability risks (antivirus software)

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost	Treatment action priority
	Lack of antivirus software/virus attack	**a)**	**1)**				
			2)				
			3)				
			4)				
		b)	**1)**	Attachment from unknown sources should not be opened	High	Very Low	Very High
				Compact disks and diskettes should be virus checked before they can be used	High	Very Low	Very High
				Antivirus software should be regularly updated	High	Very Low	Very High
			2)	Install antivirus software	Very High	Low	Very High
			3)	Self study of user manual/text book about host security and self testing of knowledge	High	Low	High
			4)	Secure physical access to the host and install video surveillance equipment for monitoring of access to the computer	Moderate	High	Low
		c)	**1)**	Daily full data and system backup	High	Low	High
			2)	Install OS, application programs and antivirus software on additional work station	High	High	Moderate
			3)	Regular tests of OS and application programs installed on additional work station	Moderate	High	Low
			4)	Install software on additional work station for monitoring of OS functionality	Moderate	High	Low
		d)	**1)**	Have an insurance that covers the financial consequences of virus attack	Moderate	Very High	Low
			2)				
			3)				
			4)				
		e)	**1)**				
			2)				
			3)				
			4)				

Table C.12: Private Lessons Treatment priority table for host security service availability risks (firewall)

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost	Treatment action priority
	Lack of firewall/attack from the network	a)	1)	Remove connection from the Internet	No benefit		
			2)				
			3)				
			4)				
		b)	1)	Firewall should be regularly updated	High	Low	High
			2)	Install firewall	Very High	Moderate	High
			3)	Self study of user manual/text book about host security and self testing of knowledge	Moderate	Low	Moderate
			4)	Install software for monitoring of network traffic	Moderate	Moderate	Moderate
		c)	1)	Daily full data and system backup	High	Low	High
			2)	Install OS, application programs and antivirus software on additional work station	High	High	Moderate
			3)	Regular tests of OS and application programs installed on additional work station	Moderate	High	Low
			4)	Install software on additional work station for monitoring of OS functionality	Moderate	High	Low
		d)	1)	Have an insurance that covers the financial consequences of network attack	Moderate	Very High	Low
			2)				
			3)				
			4)				
		e)	1)				
			2)				
			3)				
			4)				

Appendix D. Chat service case study

In this appendix we describe the practical use of MODA for the availability risk assessment of the chat service AMIGOS. The appendix is structured into six sections. The first five sections are decomposed into sub-sections that describe the results of activities of each sub-process of the MODA Risk management process. The last section presents the summary of main conclusions. Table D1 shows the overview of Appendix D. The left column shows sub-processes of the MODA Risk management process. The middle column shows sections in Appendix D that describe activities of MODA sub-processes. The right column shows the page where the reader can find corresponding section or sub-section.

The MODA sub-process	Section	Page
Sub-process 1: **Context identification**	**D.1** Contest identification – overview of the section	172
	D.1.1 Activity 1.1 Risk management context specification	172
	D.1.2 Activity 1.2 Specification of the target of evaluation	174
	D.1.3 Activity 1.3 Identification of stakeholders of the target system	178
	D.1.4 Activity 1.4 Identification of assets	178
	D.1.5 Activity 1.5 Identification of the risk acceptance criteria	179
Sub-process 2: **Risk identification**	**D.2** Risk identification – overview of the section	180
	D.2.1 Activity 2.1 Identification of risks to availability aspects	180
	D.2.2 Activity 2.2 Fault tree analysis	181
Sub-process 3: **Risk analysis**	**D.3** Risk analysis – overview of the section	190
	D.3.1 Activity 3.1 Consequence evaluation	190
	D.3.2 Activity 3.2 Frequency evaluation	194
Sub-process 4: **Risk evaluation**	**D.4** Risk evaluation – overview of the section	207
	D.4.1 Activity 4.1 Identification of risks values	207
	D.4.2 Activity 4.2 Update of risks values	208
	D.4.3 Activity 4.3 Categorisation of risks into risk treatment categories	210
	D.4.4 Activity 4.4 Specification of priorities of risk treatment categories	210
Sub-process 5: **Risk treatment**	**D.5** Risk treatment – overview of the section	212
	D.5.1 Activity 5.1 Identification of treatment options	212
	D.5.2 Activity 5.2 Specification of risks treatment priorities	223
Summary of main conclusions	**D.6**	234

Table D.1: The overview of Appendix D

D.1 Context identification

This section documents the results from the Context identification of the chat service. The section is structured into five sub-sections. Sub-section D1.1 describes the Activity 1.1 Risk management context specification. Sub-section D1.2 describes the Activity 1.2 Specification of the target of evaluation. Activity 1.3 Identification of stakeholders of the target system is presented in sub-section D1.3. Sub-section D1.4 presents Activity 1.4 Identification of assets. Activity 1.5 Identification of the risk acceptance criteria is described in sub-section D1.5

D.1.1 Activity 1.1: Risk management context specification

Objective	Establish the risk assessment objectives and identify needed risk assessment processes, activities and resources as well as risk assessment records to be kept.

This activity consists of the following four sub-activities:

- Specification of risk assessment objectives and needed studies
- Identification of relevant roles for a risk assessment
- Specification of risk assessment plan
- Identification of applied value categories

Specification of risk assessment objectives and needed studies

During the meeting with the system owner, the risk assessment objectives were specified and different system and risk assessment aspects were discussed. It was decided that all sub-processes of the MODA risk management process should be applied. The risk assessment objectives are shown in the Figure D.1.1.

Risk assessment objectives
• The risk assessment should identify all possible risks to the system availability • The risk assessment should suggest possible treatment for identified availability risks

Figure D.1.1: Risk assessment objectives

Because of the little size of the system and the fact that the risk assessment should be done by one person we decided to skip the documentation of the risk assessment plan and the roles of participants of the risk assessment.

Identification of applied value categories

Prior to the risk assessment, we identified value categories that should be applied in the risk assessment. The set of frequency and consequence values agreed with the system owner is documented in tables D.1.1 and D.1.2. Frequency values were defined with the help of the

Qualitative and quantitative frequency values table (Table 5.7). It was decided that frequency values should be measured in terms of occurrences per month. We defined two categories of consequence values. In the first category the consequence is measured in the impact of service lost time on the PDA user. In the second category we use the Total income consequence values table (Table 5.11) to define the consequences of risks. The consequence is defined by comparing the lost income caused by a risk to the total income of organisation.

Table D.1.1: Frequency values table

	Frequency Values				
Category	Rare	Unlikely	Possible	Likely	Almost certain
Measured in terms of occurrences per month	0.00 – 0.01 less often then 1%	0.01 – 0.05 between 1% and 5%	0.05 – 0.20 between 5% and 20%	0.20 – 0.50 between 20% and 50%	0.50 – 1.00 between 50% and 100%

Table D.1.2: Consequence values table

	Consequence Values				
Category	Insignificant	Minor	Moderate	Major	Catastrophic
Lost hours of service usage Measured in the impact of service lost time (during 1 month) on the user	<1hour less than 1 hour	1 - 2 hours between 1 and 2 hours	2 - 4 hours between 2 and 4 hours	4 - 6 hours between 4 and 6 hours	>6 more than 6 hours
Lost income Lost income compared to the total income of organisation	0-01%	0.1-1%	1-2%	2-10%	10-100%

The agreed set of risk values and their mode of computation are documented in the Risk values table shown in Table D.1.3. We assigned risk values with the help of the Risk Matrix shown in Table D.1.4.

Table D.1.3: Risk values table

Chosen risk value category	**Computation mode**	**Level**	**Risk value**	**Risk value description**
Qualitative risk values	Risk Matrix	0	N	No risk
		1	L	Low risk
		2	M	Moderate risk
		3	H	High risk
		4	E	Extreme risk

Table D.1.4: Risk Matrix

	Frequency values				
Consequence Values	Rare	Unlikely	Possible	Likely	Certain
Insignificant	N	N	L	L	M
Minor	N	L	L	M	M
Moderate	L	L	M	M	H
Major	L	M	M	H	H
Catastrophic	M	M	H	H	E

We decided that the priority of a risk treatment action should be based on the level of treatment action value that should be assigned with the help of the Risk treatment action priority matrix shown in Table D.1.5. Identification of treatment action values implies an assignment of values to treatment action benefits and costs. The agreed scale for benefit, cost and action values is documented in the Treatment action values table shown in Table D.1.6.

Table D.1.5: Risk treatment action priority matrix

	Cost of risk treatment action				
Risk treatment action benefit	Very low	Low	Moderate	High	Very high
Very low	L	VL	VL	VL	VL
Low	L	L	L	VL	VL
Moderate	H	M	M	L	L
High	VH	H	H	M	M
Very high	VH	VH	H	H	M

Table D.1.6: Treatment action values table

Level	**Benefit Value**	**Benefit value description**	**Cost Value**	**Cost value description**	**Treatment Action Value**	**Treatment action value description**
0	VL	Very low	VL	Very low	VL	Very low
1	L	Low	L	Low	L	Low
2	M	Moderate	M	Moderate	M	Moderate
3	H	High	H	High	H	High
4	VH	Very high	VH	Very high	VH	Very high

D.1.2 Activity 1.2: Specification of the target of evaluation

Objective	Define boundaries of the system that has to be assessed.

The AMIGOS chat service users communicate with the service through the Internet and use PDA terminals with wireless Internet access to log into the service. We assume that PDA terminals have installed Windows for Pocket PC operating system and do not have installed antivirus software. A service user pays 1$ for each hour of service usage and the average use of service is 30000 hours per month. The chat service is implemented on two nodes: UnixSuper and UnixSuperDuper. These two nodes have similar hardware components and they do not have redundant hardware and software components that automatically can take over the activities of failed components. Operating system Unix and antivirus software are installed on both nodes. The UnixSuper node is connected to the Internet and has firewall and two network cards. The UnixSuperDuper node has one network card and is connected to the UnixSuper by a cable. The chat service is implemented on four software components: PDA component, UserAgent component, MeetingPlaceLogic component, and ChatLogic component. The PDA component is installed on PDA terminal and provides user interface. The UserAgent component is installed on UnixSuper and responsible for service access control. The MeetingPlaceLogic and ChatLogic components are installed on UnixSuperDuper and responsible for a chat room access control (MeetingPlaceLogic) and chat functionality of the service (ChatLogic).

Figures D.1.2, D.1.3 and D.1.4 show sequence diagrams of the chat service.

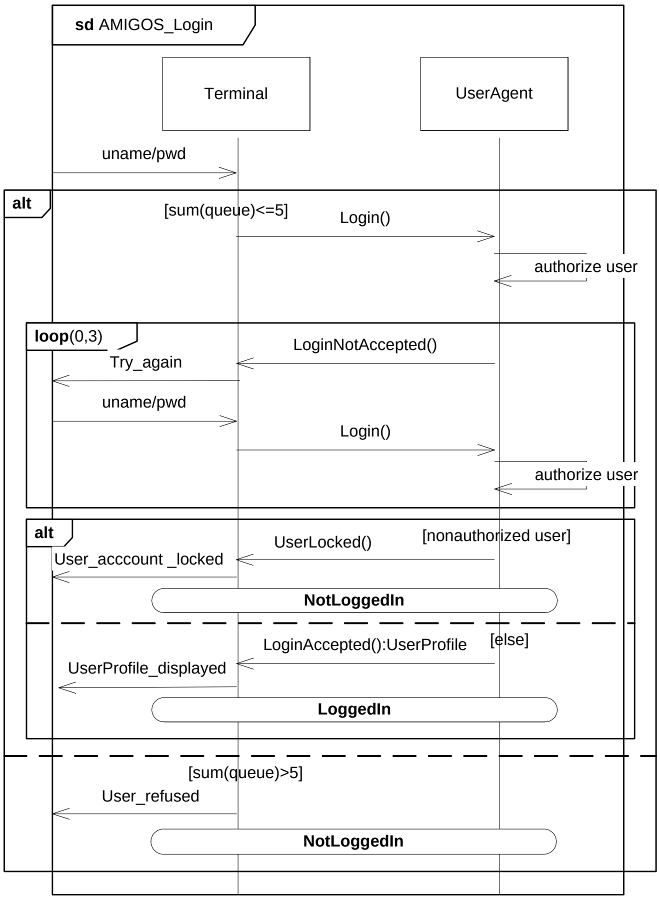


Figure D.1.2: AMIGOS login (sd1)

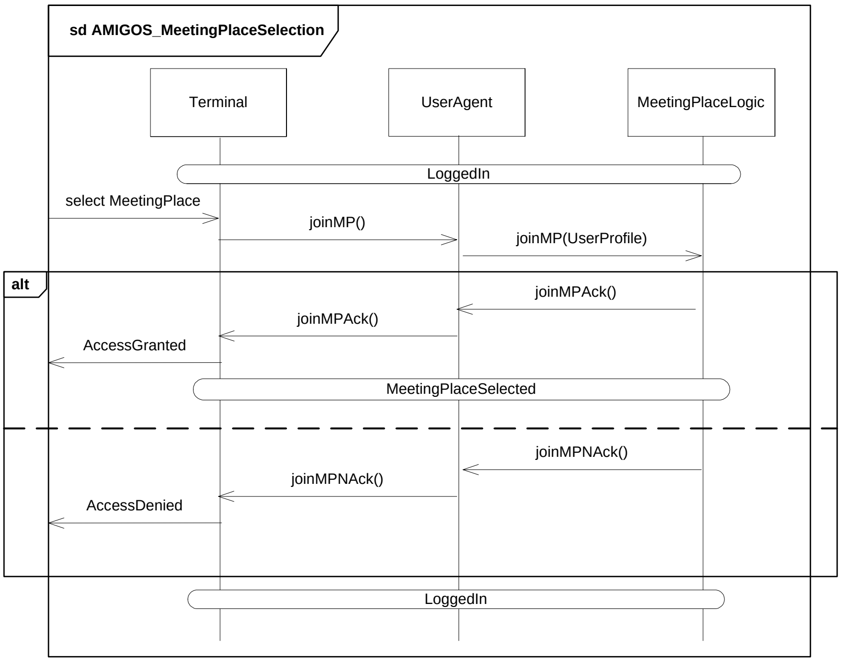


Figure D.1.3: AMIGOS Meeting place (chat room) selection (sd2)

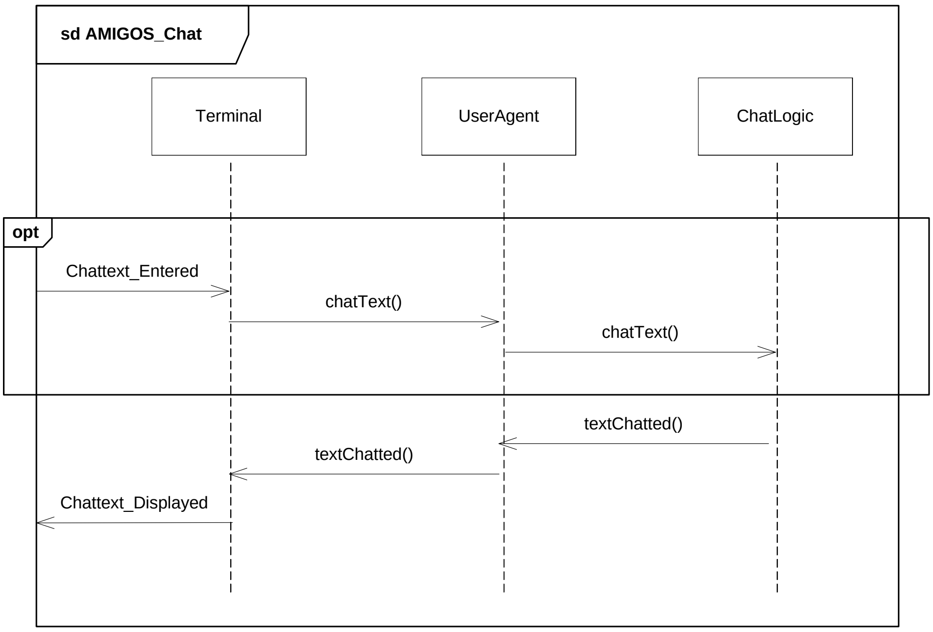


Figure D.1.4: AMIGOS chat (sd3)

Figure D.1.5 shows domain picture.

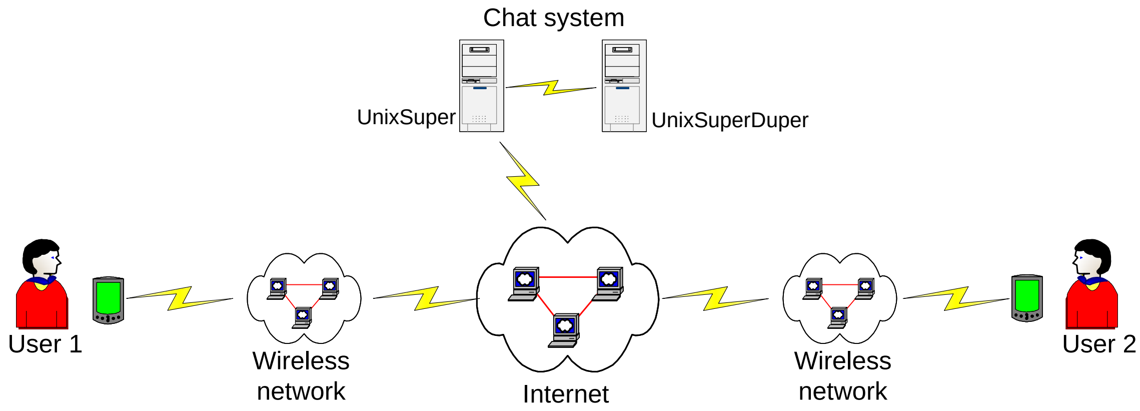


Figure D.1.5: Domain picture

The identified actors and use cases are shown in Figure D.1.6 and the Target of evaluation table is shown in Table D.1.7. We identified two main functions that should be provided by the chat service system:

- The chat service should provide the authentication control of users.
- The chat service should provide chat service functionality.

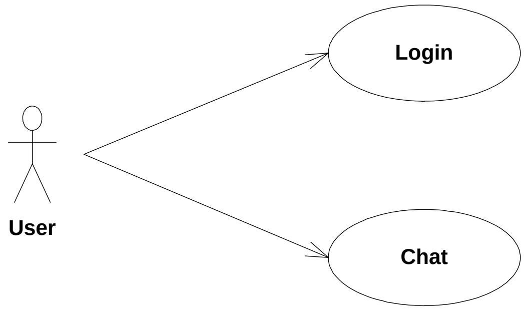


Figure D.1.6: Use cases

Table D.1.7: Target-of-evaluation table

Target:	Chat system & User PDA
Objective:	1. Online interactive chat service
Service/Function:	Chat service 1. Provide the authentication control of users 2. Provide chat service functionality PDA 1. Provide wireless access to the chat service
Security Aspects:	Availability should be the main concern

D.1.3 Activity 1.3: Identification of stakeholders of the target system

Objective	Identify stakeholders of the target system.

We identified two stakeholders – system owner and PDA user. The first owns the chat system and defines the business policy of the chat service; the second uses the chat service. The identified stakeholders are documented in the Stakeholder table that is shown in Table D.1.8 below.

Table D.1.8: Stakeholders table

Stakeholder ID	Stakeholder (Role)	Stakeholder (Name)	Description
01	System owner		Owns the chat system and defines business policy of the chat service
02	PDA user		Uses the chat service

D.1.4 Activity 1.4: Identification of assets

Objective	Identify and value assets.

The Asset diagram and the Asset table are shown in Figure D.1.7 and Table D.1.9. The Asset table documents stakeholders, asset categories and assets together with the description of assets and their values. The Asset diagram depicts stakeholders along with assets that they have. Both the system owner and the PDA user have availability of service as an asset that is very important to them. The PDA user pays 1$ for 1 hour of service usage and the system owner estimates that the system is used about 30000 hours per month.

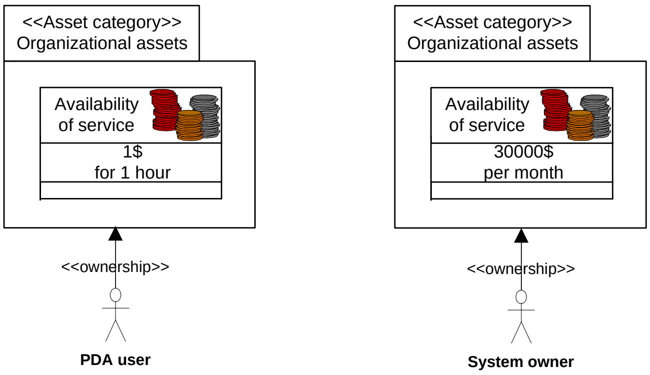


Figure D.1.7: Asset diagram

Table D.1.9: Asset table

ID	Stakeholder	Asset Category	Asset	Description	Value
01	System owner	Organizational	Availability of service	The highly available service is one of the main sources of income for the system owner	30000$ per month
02	PDA user	Organizational	Availability of service	The PDA user pays 1$ for each hour of service usage	1$ for 1 hour of service usage

D.1.5 Activity 1.5: Identification of the risk acceptance criteria

Objective	Identify the risk acceptance criteria that will be used to determine whether a given risk is acceptable or not.

The Risk acceptance table is shown in Table D.1.10 and documents stakeholders, asset categories and assets along with the description of the risk acceptance criteria. Both the system owner and the PDA user may accept risks that have the risk value equal or less than “Low”.

Table D.1.10: Risk acceptance table

Stakeholder	Asset category	Asset	Risk acceptance criteria
System owner	Organizational	Availability of service	No risks that have a risk value > Low
PDA user	Organizational	Availability of service	No risks that have a risk value > Low

D.2 Risk identification

This section describes the results from the Risk identification of the chat service. The section is structured into two sub-sections. Sub-section D2.1 describes the Activity 2.1 Identification of risks to availability aspects. Activity 2.2 Fault tree analysis is presented in sub-section D2.2.

D.2.1 Activity 2.1: Identification of risks to availability aspects

Objective	Identify availability aspects risks that are relevant for the target of evaluation.

The chat service is implemented on two nodes UnixSuper (US) and UnixSuperDuper (USD) that communicate with each other through a cable. PDA users are connected to a wireless network and communicate with the chat service (UnixSuper node) through the Internet. Table D.2.1 shows the Network availability risks table for the chat service.

Table D.2.1: Network availability risks table

Stakeholder	Asset	Availability aspect	Risk	Relevant entity
System owner	Availability of service	Network availability	Denial of Network availability	Internet connection Cable connecting two chat nodes
PDA user	Availability of service	Network availability	Denial of Network availability	Wireless network connection

Without the chat software component installed on a PDA terminal, the user will not be able to use the chat service. If software component UserAgent is not function or malfunction, the users will not be able to log into the service. Without MeetingPlaceLogic component the users will not be able to choose a chat room. If software component ChatLogic is not available, the users will not be able to chat with each other. Table D.2.2 shows the Software availability risks table for the chat service.

Table D.2.2: Software availability risks table

Stakeholder	Asset	Availability aspect	Risk	Relevant entity
System owner	Availability of service	Host (US) application software availability	Denial of Host (US) application software availability	UserAgent
		Host (USD) application software availability	Denial of Host (USD) application software availability	MeetingPlaceLogic ChatLogic
PDA user	Availability of service	Host (PDA) application software availability	Denial of Host (PDA) application software availability	PDA chat software

The chat service nodes UnixSuper and UnixSuperDuper are connected by a cable and have similar hardware components that are important for the chat service functionality: processor, network card and hard disk. The UnixSuper has two network cards: one is used to connect the node to the Internet, and another one is used to connect the node to the UnixSuperDuper. PDA terminal connects to the Internet with the help of network card and has removable flash memory card and lithium battery. Table D.2.3 shows the Hardware availability risks table for the chat service.

Table D.2.3: Hardware availability risks table

Stakeholder	Asset	Availability aspect	Risk	Relevant entity
System owner	Availability of service	Host (US) internal hardware availability	Denial of Host (US) internal hardware availability	Network card 1 Network card 2 Hard disk Processor
		Host (USD) internal hardware availability	Denial of Host (USD) internal hardware availability	Network card Hard disk Processor
PDA user	Availability of service	Host (PDA) internal hardware availability	Denial of Host (PDA) internal hardware	Network card Memory flash card Lithium battery

The chat service availability also depends on the availability of network administrator that is responsible for installation of new components, configuration and maintenance of chat service. Table D.2.4 shows the Human availability risks table for the chat service.

Table D.2.4: Human availability risks table

Stakeholder	Asset	Availability aspect	Risk	Relevant entity
System owner	Availability of service	Human availability	Denial of Human availability	Chat service network administrator

D.2.2 Activity 2.2: Fault tree analysis

Objective	Identify causes that may lead to the availability aspects risks identified in the Activity 2.1

The availability of chat service can be affected by the denial of availability of chat service nodes, availability of network and availability of network administrator. Figure D.2.1 shows fault tree that depicts risks that may lead to the denial of service availability.

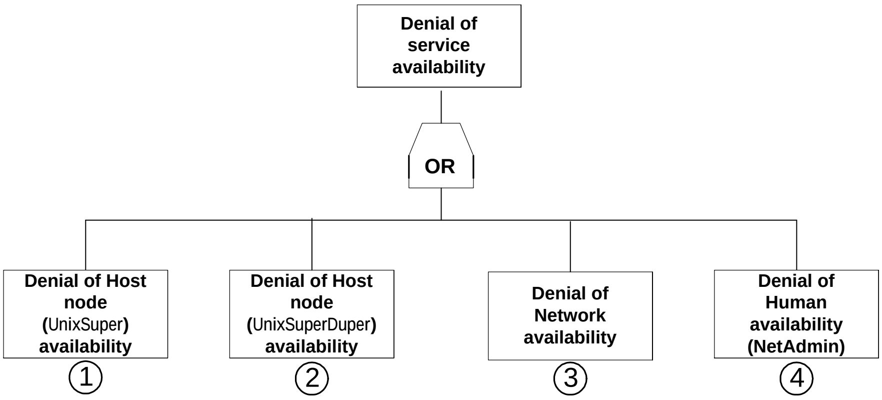

Denial of service availability
OR
Denial of Host node (UnixSuper) availability
1
Denial of Host node (UnixSuperDuper) availability
2
Denial of Network availability
3
Denial of Human availability (NetAdmin)
4

Figure D.2.1: Fault tree for Denial of service availability

The availability of wireless access to the chat service can be affected by the denial of availability of wireless network and availability of PDA. Figure D.2.2 shows fault tree that depicts risks that may lead to the denial of wireless access to the chat service.

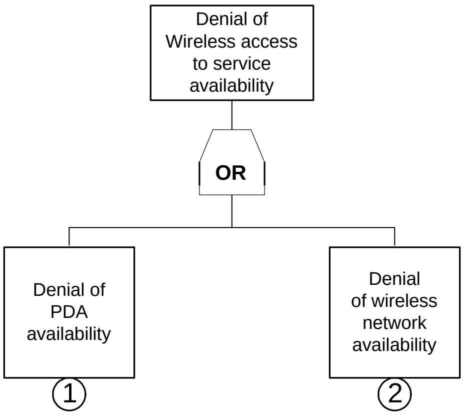

Denial of Wireless access to service availability
OR
Denial of PDA availability
1
Denial of wireless network availability
2

Figure D.2.2: Fault tree for Denial of wireless access to service

The network availability can be decomposed into the availability of Internet connection and availability of cable connecting the two chat service nodes. Figure D.2.3 shows fault tree that depicts risk that may lead to the denial of network availability.

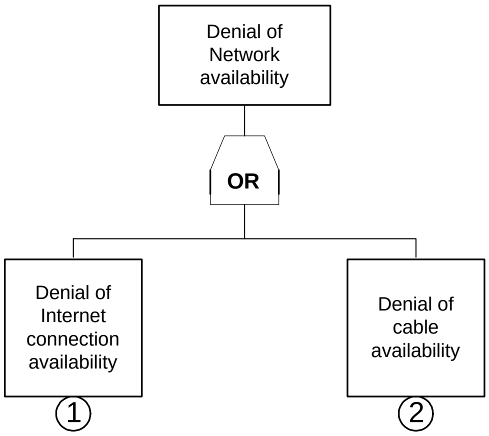

Denial of Network availability
OR
Denial of Internet connection availability
1
Denial of cable availability
2

Figure D.2.3: Fault tree for Denial of network availability

To build the fault trees that have the top events *Denial of Host node (PDA) availability*, *Denial of Host node (UnixSuper) availability*, and *Denial of Host node (UnixSuperDuper) availability*, we have used the template from Figure 4.15 (chapter 4.7). Figure D.2.4 shows fault tree that was build for each of top events.

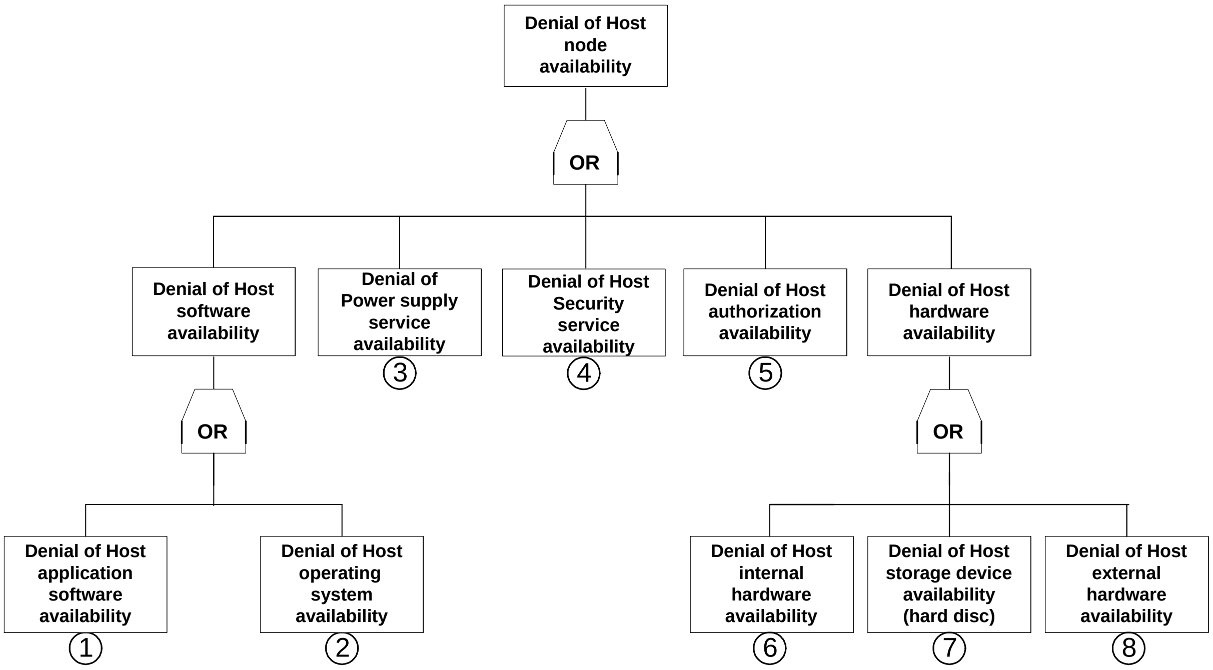

Denial of Host node availability
OR
Denial of Host software availability
Denial of Power supply service availability
3
Denial of Host Security service availability
4
Denial of Host authorization availability
5
Denial of Host hardware availability
OR
OR
Denial of Host application software availability
1
Denial of Host operating system availability
2
Denial of Host internal hardware availability
6
Denial of Host storage device availability (hard disc)
7
Denial of Host external hardware availability
8

Figure D.2.4: Fault tree for Denial of Host node (PDA, UnixSuper, UnixSuperDuper) availability

Figures D.2.5, D.2.6 and D.2.7 show fault trees for the availability risks *Denial of Host (PDA) application software availability*, *Denial of Host (UnixSuper) application software availability*, and *Denial of Host (UnixSuperDuper) application software availability*. These fault trees were constructed with the help of template from Figure 4.16.

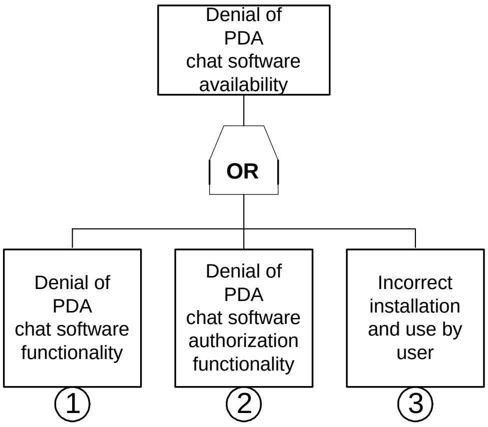

Denial of PDA chat software availability
OR
Denial of PDA chat software functionality
Denial of PDA chat software authorization functionality
Incorrect installation and use by user
1
2
3

Figure D.2.5: Fault tree for Denial of Host (PDA) application software availability

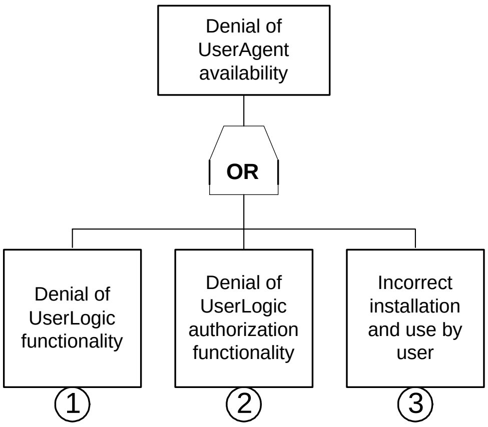

Denial of UserAgent availability
OR
Denial of UserLogic functionality
Denial of UserLogic authorization functionality
Incorrect installation and use by user
1
2
3

Figure D.2.6: Fault tree for Denial of Host (UnixSuper) application software availability

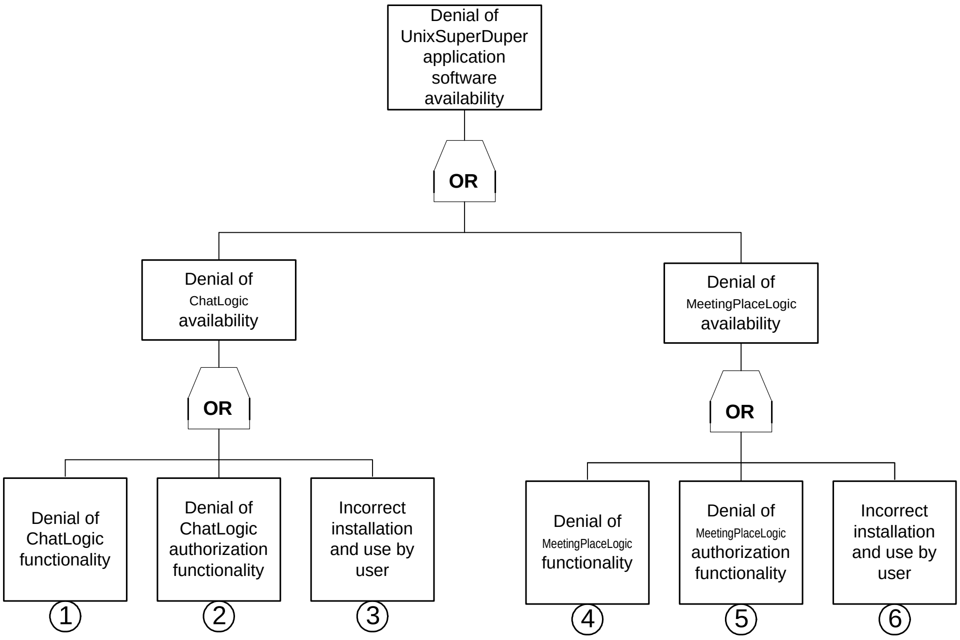

Denial of UnixSuperDuper application software availability
OR
Denial of ChatLogic availability
Denial of MeetingPlaceLogic availability
OR
OR
Denial of ChatLogic functionality
Denial of ChatLogic authorization functionality
Incorrect installation and use by user
Denial of MeetingPlaceLogic functionality
Denial of MeetingPlaceLogic authorization functionality
Incorrect installation and use by user
1
2
3
4
5
6

Figure D.2.7: Fault tree for Denial of Host (UnixSuperDuper) application software availability

Figures D.2.8, D.2.9 and D.2.10 show fault trees for the availability risks *Denial of Host (PDA) operating system availability*, *Denial of Host (UnixSuper) operating system availability*, and *Denial of Host (UnixSuperDuper) operating system availability*. These fault trees were constructed with the help of template from Figure 4.17.

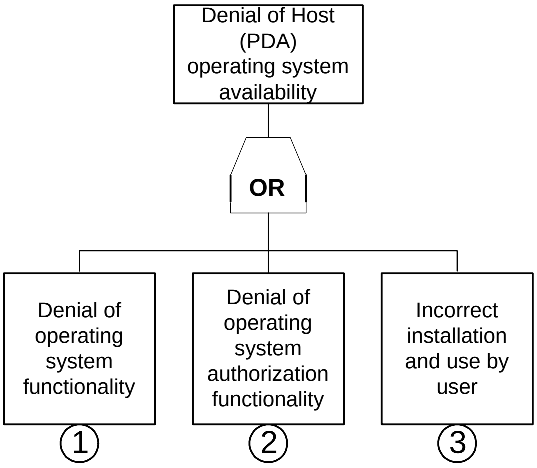

Denial of Host (PDA) operating system availability
OR
Denial of operating system functionality
Denial of operating system authorization functionality
Incorrect installation and use by user
1
2
3

Figure D.2.8: Fault tree for Denial of Host (PDA) operating system availability

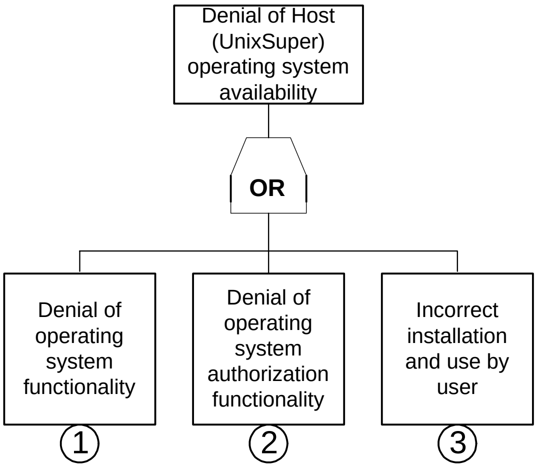

Denial of Host (UnixSuper) operating system availability
OR
Denial of operating system functionality
Denial of operating system authorization functionality
Incorrect installation and use by user
1
2
3

Figure D.2.9: Fault tree for Denial of Host (UnixSuper) operating system availability

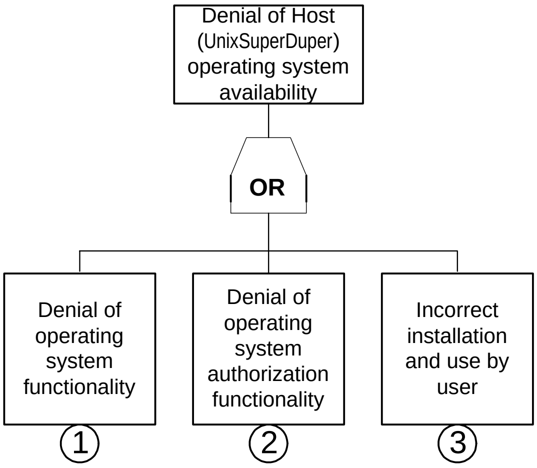

Denial of Host (UnixSuperDuper) operating system availability
OR
Denial of operating system functionality
Denial of operating system authorization functionality
Incorrect installation and use by user
1
2
3

Figure D.2.10: Fault tree for Denial of Host (UnixSuperDuper) operating system availability

Figure D.2.11 shows fault tree for the availability risk *Denial of Host (PDA) hardware availability*. The denial of PDA memory flash card availability will be considered under Denial of Host storage device availability in the fault tree for Denial of Host node (PDA) availability. Figures D.2.12 and D.2.13 show fault trees that are constructed for the availability risks *Denial of Host (UnixSuper) hardware availability*, and *Denial of Host (UnixSuperDuper) hardware availability*. We constructed hardware availability fault trees with the help of template from Figure 4.18.

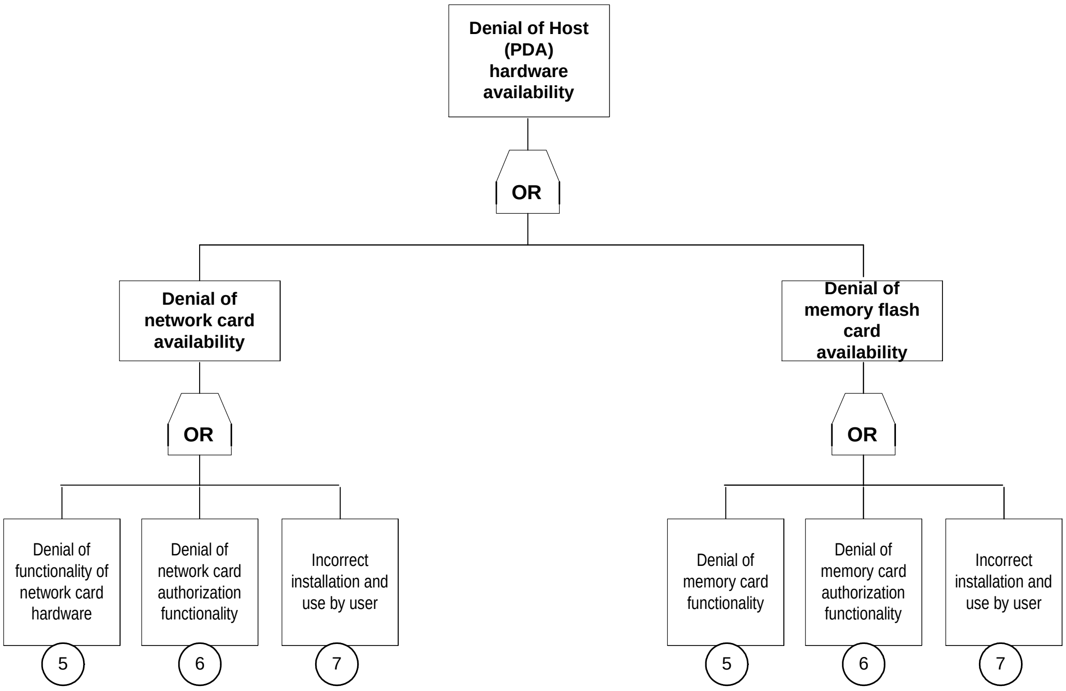

Denial of Host (PDA) hardware availability
OR
Denial of network card availability
Denial of memory flash card availability
OR
OR
Denial of functionality of network card hardware
Denial of network card authorization functionality
Incorrect installation and use by user
Denial of memory card functionality
Denial of memory card authorization functionality
Incorrect installation and use by user
5
6
7
5
6
7

Figure D.2.11: Fault tree for Denial of Host (PDA) hardware availability

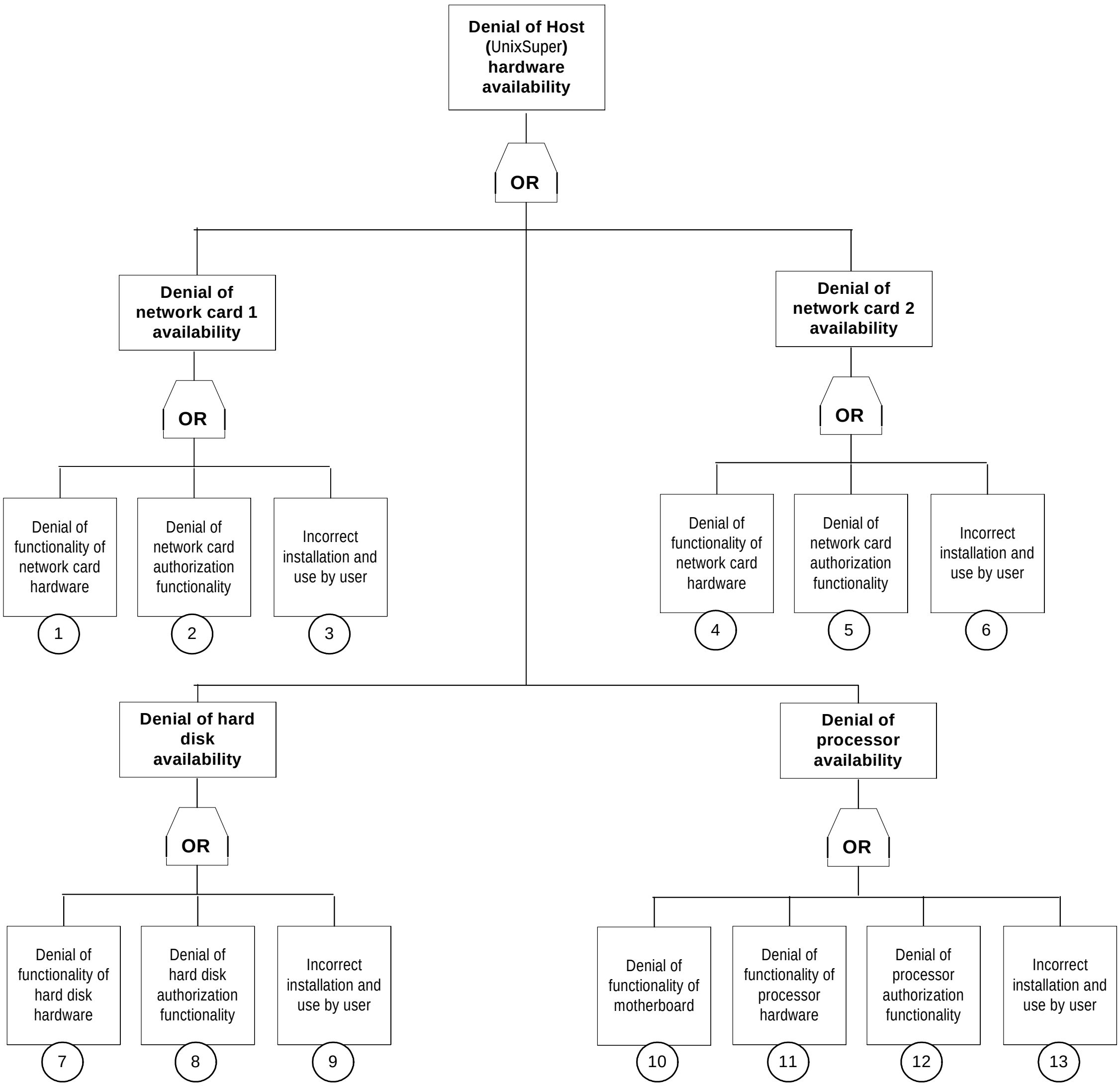

Denial of Host (UnixSuper) hardware availability
OR
Denial of network card 1 availability
Denial of network card 2 availability
OR
OR
Denial of functionality of network card hardware
Denial of network card authorization functionality
Incorrect installation and use by user
Denial of functionality of network card hardware
Denial of network card authorization functionality
Incorrect installation and use by user
1
2
3
4
5
6
Denial of hard disk availability
Denial of processor availability
OR
OR
Denial of functionality of hard disk hardware
Denial of hard disk authorization functionality
Incorrect installation and use by user
Denial of functionality of motherboard
Denial of functionality of processor hardware
Denial of processor authorization functionality
Incorrect installation and use by user
7
8
9
10
11
12
13

Figure D.2.12: Fault tree for Denial of Host (UnixSuper) hardware availability

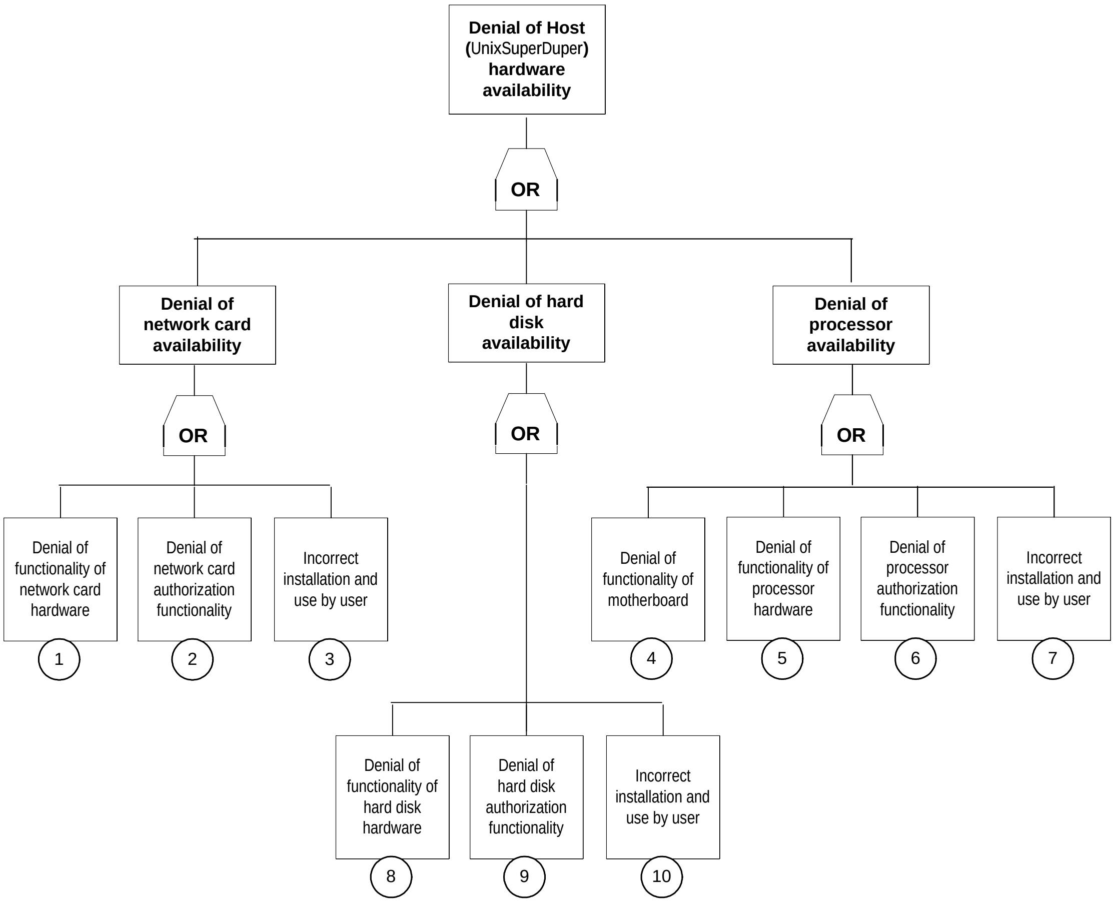

Denial of Host (UnixSuperDuper) hardware availability
OR
Denial of network card availability
Denial of hard disk availability
Denial of processor availability
OR
OR
OR
Denial of functionality of network card hardware
Denial of network card authorization functionality
Incorrect installation and use by user
Denial of functionality of motherboard
Denial of functionality of processor hardware
Denial of processor authorization functionality
Incorrect installation and use by user
1
2
3
4
5
6
7
Denial of functionality of hard disk hardware
Denial of hard disk authorization functionality
Incorrect installation and use by user
8
9
10

Figure D.2.13: Fault tree for Denial of Host (UnixSuperDuper) hardware availability

Figure D.2.14 shows fault tree that is constructed for the availability risk *Denial of Host (PDA) security service availability*. The similar trees were constructed for the risks *Denial of Host (UnixSuper) security service availability*, and *Denial of Host (UnixSuperDuper) security service availability*. We constructed fault tree with the help of template from Figure 4.19.

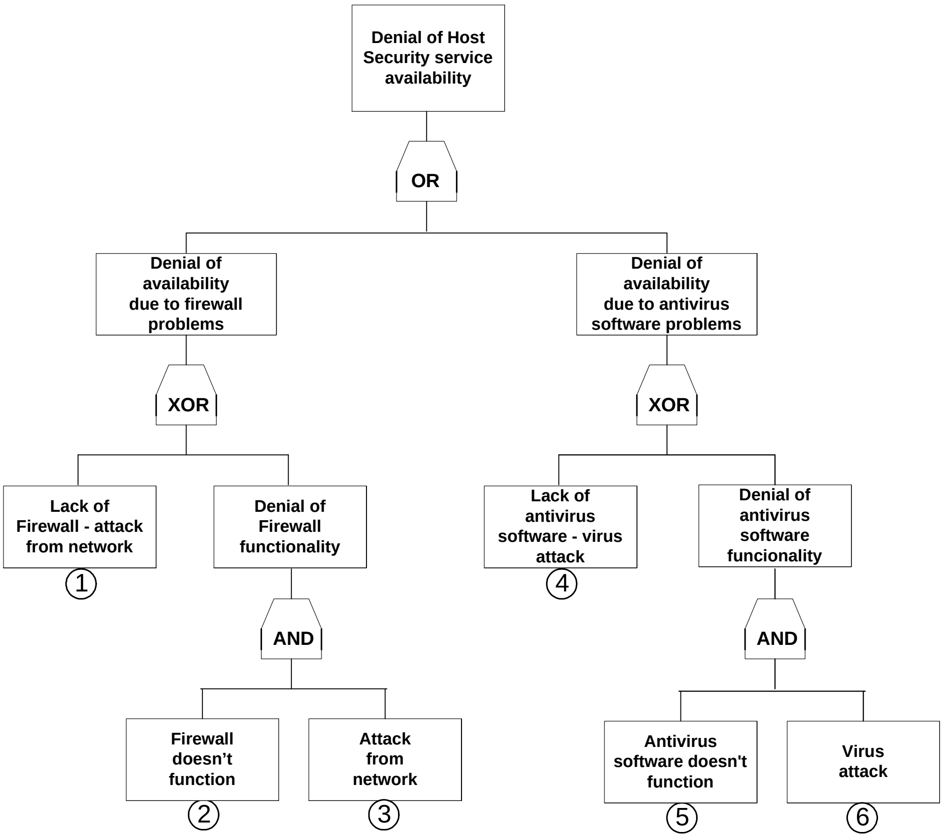

Denial of Host Security service availability
OR
Denial of availability due to firewall problems
Denial of availability due to antivirus software problems
XOR
XOR
Lack of Firewall - attack from network
Denial of Firewall functionality
Lack of antivirus software - virus attack
Denial of antivirus software funcionality
1
4
AND
AND
Firewall doesn't function
Attack from network
Antivirus software doesn't function
Virus attack
2
3
5
6

Figure D.2.14: Fault tree for Denial of Host (PDA) security service availability

D.3 Risk analysis

This section presents the results from the Risk analysis of the chat service. The section is structured into two sub-sections. Sub-section D3.1 describes the Activity 3.1 Consequence evaluation. Sub-section D3.2 presents the Activity 3.2 Frequency evaluation.

D.3.1 Activity 3.1: Consequence evaluation

Objective	Analyse risks consequences

In the activity 1.1 we decided that consequence values for the PDA user and the system owner should be determined with the help of the Consequence values table shown in Table D.1.2. Both PDA users and the system owner have agreements with service companies about software and hardware support. The consequence values for the system owner were determined in the following way:

- First we determined the hour income of the chat service (month income/number of hours in month): 30000/730 = 41$ per hour
- Then we determined the lost income (downtime*hour income)
- Then the lost income was compared to the monthly income of the chat service and the resulted percent was used to determine the consequence value with the help of the Consequence values table (Table D.1.2).

The consequence tables for the chat service are depicted below and show identified consequence values together with their description.

Table D.3.1: Consequence table for software availability risks

Stakeholder	Asset	Risk			Risk scenario	Consequence value	Consequence description
PDA user	Availability of service	Denial of host (PDA) software availability	Denial of host (PDA) operating system availability		The Host (PDA) operating system doesn’t function or malfunction	Major	Service company guarantees that it takes for company no longer than 5 hours to fix operating system problems
			Denial of Host (PDA) application software availability	Denial of PDA chat software functionality	PDA chat software doesn’t function or malfunction	Minor	Service company guarantees that it takes for company no longer than 2 hours to fix chat application software problems
System owner	Availability of service	Denial of host (US) software availability	Denial of host (US) operating system availability		The Host (US) operating system doesn’t function or malfunction	Moderate	Service company guarantees that it takes for company no longer than 8 hours to fix operating system problems ((41*8)/30000)*100 = 1,09%

			Denial of Host (US) application software availability	Denial of UserAgent software component functionality	UserAgent software component doesn't function or malfunction	Minor	Service company guarantees that it takes for company no longer than 5 hours to fix chat application software problems ((41*5)/30000)*100 = 0,68%
		Denial of host (USD) software availability	Denial of host (US) operating system availability		The Host (USD) operating system doesn't function or malfunction	Moderate	Service company guarantees that it takes for company no longer than 8 hours to fix operating system problems ((41*8)/30000)*100 = 1,09%
			Denial of Host (USD) application software availability	Denial of MeetingPlace Logic software component functionality	MeetingPlaceLogic software component doesn't function or malfunction	Minor	Service company guarantees that it takes for company no longer than 5 hours to fix chat application software problems ((41*5)/30000)*100 = 0,68%
				Denial of ChatLogic software component functionality	ChatLogic software component doesn't function or malfunction	Minor	Service company guarantees that it takes for company no longer than 5 hours to fix chat application software problems ((41*5)/30000)*100 = 0,68%

Table D.3.2: Consequence table for hardware availability risks

Stakeholder	Asset	Risk			Risk scenario	Consequence value	Consequence description
PDA user	Availability of service	Denial of host (PDA) hardware availability	Denial of host (PDA) memory flash card availability		The Host (PDA) memory flash card doesn't function or malfunction	Moderate	PDA user hasn't an additional memory flash card. It takes him no longer than 4 hours to get a new memory flash card and install it.
			Denial of Host (PDA) internal hardware availability	Denial of network card availability	Network card doesn't function or malfunction	Major	PDA user hasn't an additional network card. It takes him 5 hours to get a new memory flash card and install it.
System owner	Availability of service	Denial of host (US) and host (USD) hardware availability	Denial of host (US & USD) storage device availability		The host hard disk doesn't function or malfunction	Moderate	Service company guarantees that it takes for company no longer than 10 hours to fix hard disk problems ((41*10)/30000)*100 = 1,36%
			Denial of host (US & USD) internal hardware availability	Denial of network card availability	Network card doesn't function or malfunction	Major	Service company guarantees that it takes for company no longer than 15 hours to fix network card problems ((41*15)/30000)*100 = 2,05%

				Denial of processor availability	Processor doesn't function or malfunction	Major	Service company guarantees that it takes for company no longer than 18 hours to fix processor problems ((41*18)/30000)*100 = 2,46%

Table D.3.3: Consequence table for host security service availability risks

Stakeholder	Asset	Risk		Risk scenario	Consequence value	Consequence description
PDA user	Availability of service	Denial of host (PDA) security service availability	Lack of firewall – host is attacked from the Internet	The host node is attacked from the Internet	Catastrophic	Service company guarantees that it takes for company no longer than 8 hours to recover PDA from a network attack
			Lack of antivirus software – host is attacked by computer virus	The host node is attacked by computer virus	Major	Service company guarantees that it takes for company no longer than 6 hours to recover PDA from a virus attack
System owner	Availability of service	Denial of host (US & USD) security service availability	Host (US) is attacked from the Internet	The host node (US) is attacked from the Internet	Moderate	Service company guarantees that it takes for company no longer than 10 hours to recover host from network attack ((41*10)/30000)*100 = 1,36%
			Host (US & USD) is attacked by computer virus	The host node (US & USD) is attacked by computer virus	Major	Service company guarantees that it takes for company no longer than 15 hours to recover host from virus attack ((41*15)/30000)*100 = 2,05%

Table D.3.4: Consequence table for host availability risks

Stakeholder	Asset	Risk		Risk scenario	Consequence value	Consequence description
PDA user	Availability of service	Denial of host (PDA) availability	Denial of host software availability	The host software doesn't function or malfunction		The consequence of denial of availabilities of host operating system and chat software
			Denial of host hardware availability	The host hardware doesn't function or malfunction		The consequence of denial of availabilities of memory flash card and network card
			Denial of power supply service availability	Lithium battery doesn't function or malfunction	Moderate	PDA user has not an additional lithium battery. It takes him no longer than 4 hours to get a new lithium battery and install it.
			Denial of host security service availability	The host is attacked from the internet and/or by computer virus		The consequence of lack of firewall and antivirus software

			Denial of host authorization availability	PDA is stolen	Catastrophic	As a result of theft of PDA, user has to buy a new PDA and install operating system along with application programs. It takes him 1 day to buy a new PDA
System owner	Availability of service	Denial of host (US & USD) availability	Denial of host software availability	The host software doesn’t function or malfunction		The consequence of denial of availabilities of host (US & USD) operating system and chat software
			Denial of host hardware availability	The host hardware doesn’t function or malfunction		The consequence of denial of availabilities of host (US & USD) hard disc, network card and processor
			Denial of power supply service availability	The local provider of electricity has technical problems and can’t provide electricity	Moderate	Provider of electricity guarantees that it takes for company no longer than 10 hours to recover from electricity problems ((41*10)/30000)*100 = 1,36%
			Denial of host security service availability	The host is attacked from the internet and/or by computer virus		The consequence of attack from Internet or virus attack
			Denial of host authorization availability	The chat service nodes are stolen or damaged	Catastrophic	It takes the system owner 5 days to recover from theft/damage of service nodes

Table D.3.5: Consequence table for service availability risks

Stakeholder	Asset	Risk		Risk scenario	Consequence value	Consequence description
System owner	Availability of service	Denial of Service availability	Denial of host (US & USD) availability	The host (US & USD) is not available		The consequence of denial of availabilities of hosts software, hardware, power supply service, host authorization and security service
			Denial of Network availability	The local Internet provider has technical problems and can’t provide access to the Internet	Minor	Internet provider guarantees that it takes for company no longer than 3 hours to recover from network problems ((41*3)/30000)*100 = 0,41%
				The cable connecting two chat service nodes is damaged or doesn’t function	Minor	The chat company has an additional cable. It takes netadmin 2 hours to change the cable. ((41*2)/30000)*100 = 0,27%
			Denial of Human availability	The network administrator makes fail during maintenance of chat service	Minor	Usually it takes 1 hour for network administrator to recover the chat service from fail ((41*1)/30000)*100 = 0,13%

PDA user	Availability of service	Denial of wireless access to service availability	Denial of PDA availability	PDA is not available		The consequence of denial of availabilities of memory flash card, network card , lithium battery, host authorization and security service
			Denial of wireless network availability	Wireless network is not available	Minor	Wireless network provider guarantees that it takes for company no longer than 2 hours to recover from network problems

D.3.2 Activity 3.2: Frequency evaluation

Objective	Evaluate risks frequencies

Figure D.3.1 shows the fault tree with frequencies of risks that may lead to the *Denial of Host (PDA) security service availability*. The probabilities of basis events were defined with the help of information provided by the PDA user support company.

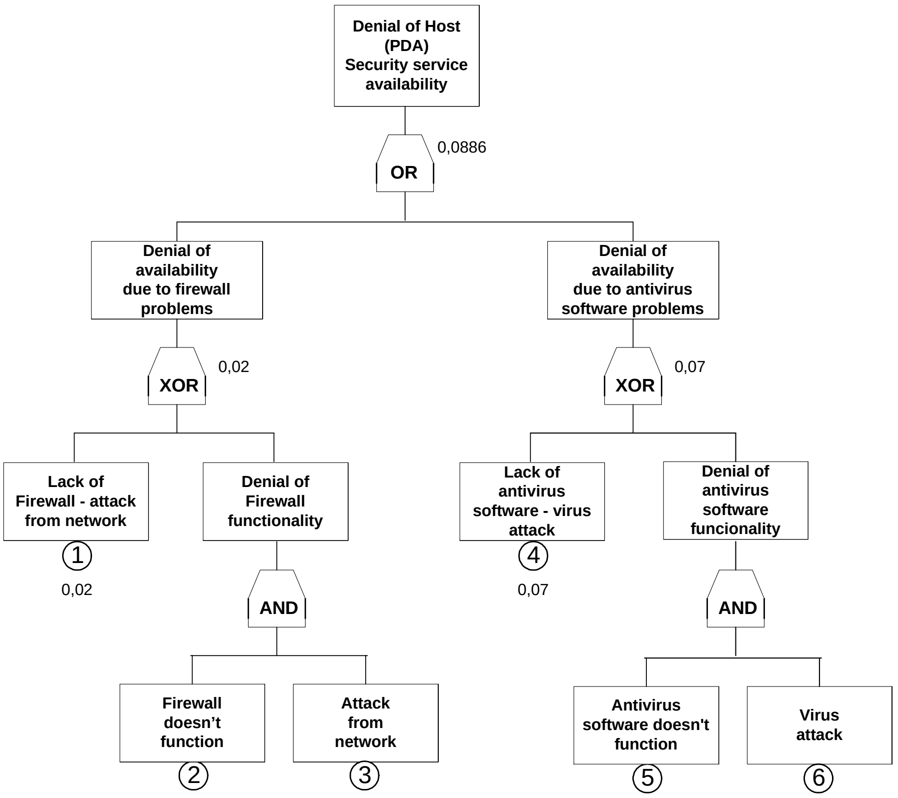

Denial of Host (PDA) Security service availability
0,0886
OR
Denial of availability due to firewall problems
Denial of availability due to antivirus software problems
XOR
0,02
XOR
0,07
Lack of Firewall - attack from network
1
0,02
Denial of Firewall functionality
AND
Lack of antivirus software - virus attack
4
0,07
Denial of antivirus software funcionality
AND
Firewall doesn't function
2
Attack from network
3
Antivirus software doesn't function
5
Virus attack
6

Figure D.3.1: Determination of frequency for Denial of PDA security service availability

Figures D.3.2, D.3.3 and D.3.4 show the fault trees with frequencies of risks that may lead to the *Denial of Host (PDA) software availability*, *Denial of Host (PDA) hardware availability* and

Denial of Host (PDA) availability. The probabilities of basis events were defined with help of information provided by the PDA user support company.

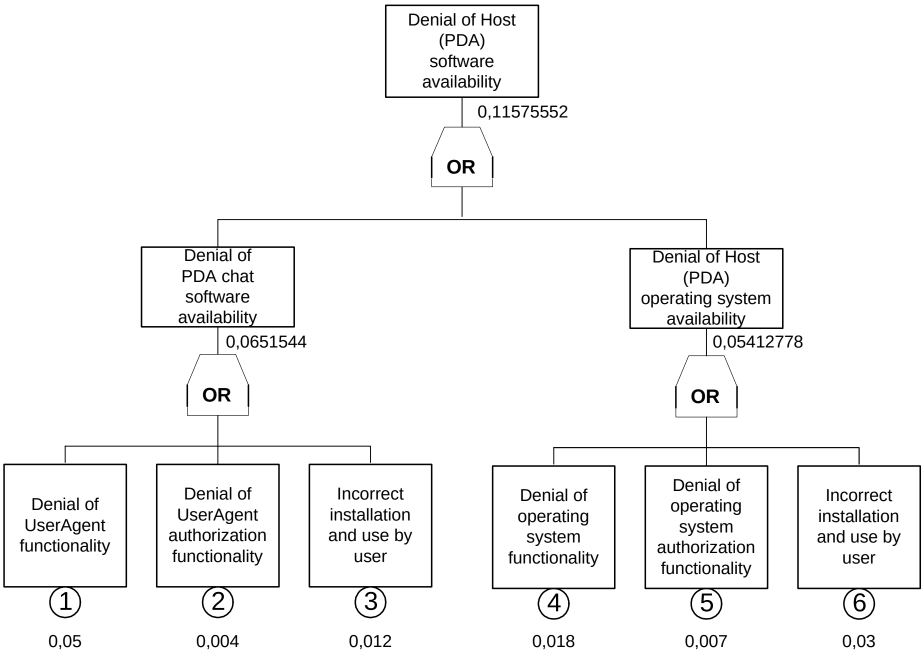

Denial of Host (PDA) software availability
0,11575552
OR
Denial of PDA chat software availability
0,0651544
OR
Denial of Host (PDA) operating system availability
0,05412778
OR
Denial of UserAgent functionality
Denial of UserAgent authorization functionality
Incorrect installation and use by user
Denial of operating system functionality
Denial of operating system authorization functionality
Incorrect installation and use by user
1
2
3
4
5
6
0,05
0,004
0,012
0,018
0,007
0,03

Figure D.3.2: Determination of frequency for Denial of PDA software availability

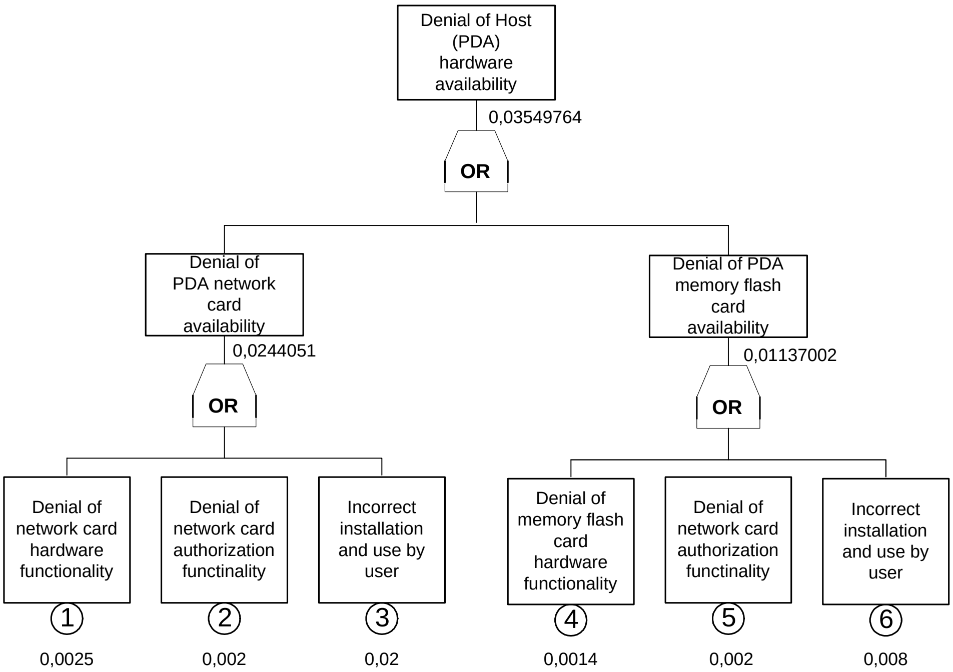

Denial of Host (PDA) hardware availability
0,03549764
OR
Denial of PDA network card availability
0,0244051
OR
Denial of PDA memory flash card availability
0,01137002
OR
Denial of network card hardware functionality
Denial of network card authorization functinality
Incorrect installation and use by user
Denial of memory flash card hardware functionality
Denial of network card authorization functinality
Incorrect installation and use by user
1
2
3
4
5
6
0,0025
0,002
0,02
0,0014
0,002
0,008

Figure D.3.3: Determination of frequency for Denial of PDA hardware availability

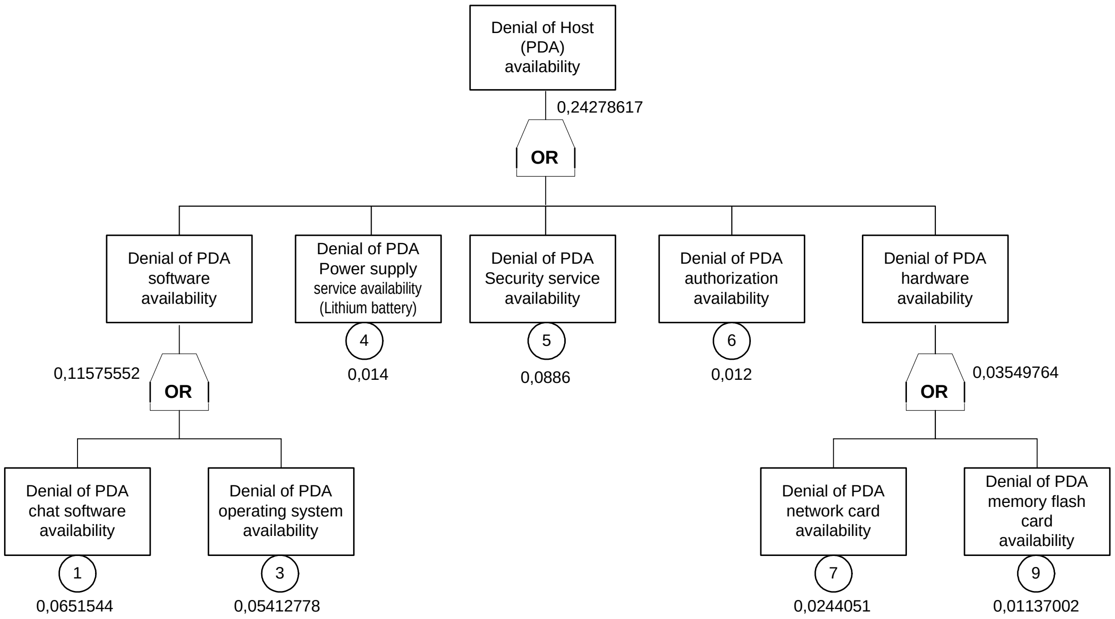

Denial of Host (PDA) availability
0,24278617
OR
Denial of PDA software availability
Denial of PDA Power supply service availability (Lithium battery)
Denial of PDA Security service availability
Denial of PDA authorization availability
Denial of PDA hardware availability
4
0,014
5
0,0886
6
0,012
0,11575552
OR
OR
0,03549764
Denial of PDA chat software availability
Denial of PDA operating system availability
Denial of PDA network card availability
Denial of PDA memory flash card availability
1
0,0651544
3
0,05412778
7
0,0244051
9
0,01137002

Figure D.3.4: Determination of frequency for Denial of PDA availability

Figures D.3.5 and D.3.6 show the fault trees with frequencies of risks that may lead to the *Denial of Host (US) security service availability* and *Denial of Host (USD) security service availability*. The probabilities of basis events were defined with the help of information provided by the software support company used by the chat service administration.

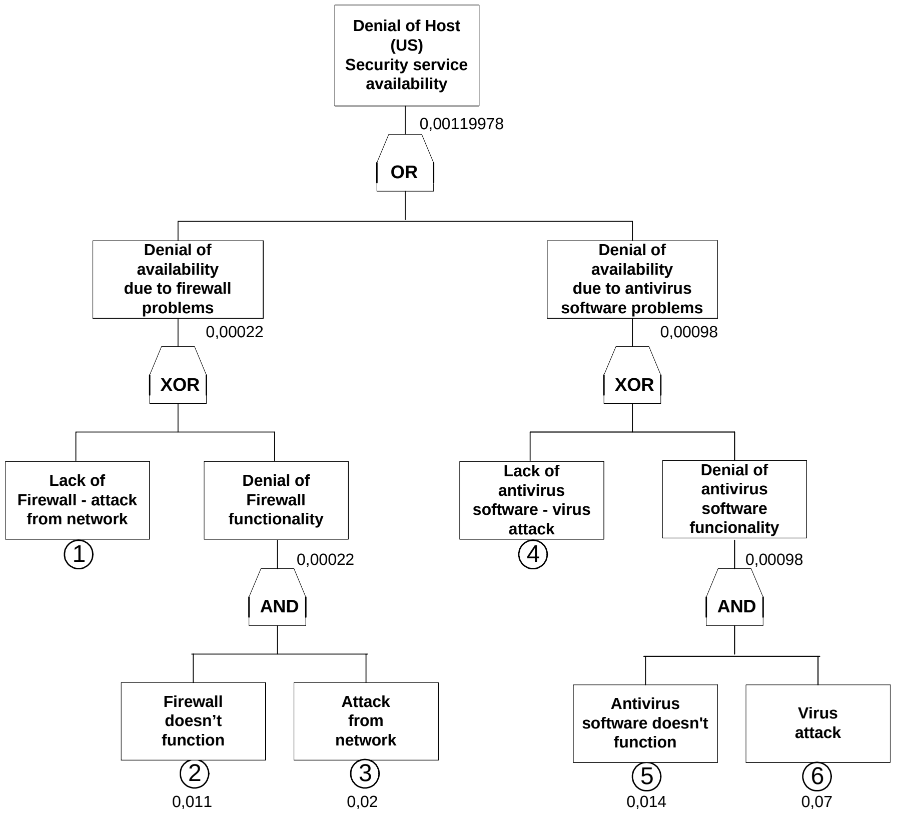

Denial of Host (US) Security service availability
0,00119978
OR
Denial of availability due to firewall problems
0,00022
Denial of availability due to antivirus software problems
0,00098
XOR
XOR
Lack of Firewall - attack from network
1
Denial of Firewall functionality
0,00022
Lack of antivirus software - virus attack
4
Denial of antivirus software funcionality
0,00098
AND
AND
Firewall doesn't function
2
0,011
Attack from network
3
0,02
Antivirus software doesn't function
5
0,014
Virus attack
6
0,07

Figure D.3.5: Determination of frequency for Denial of Host (US) security service availability

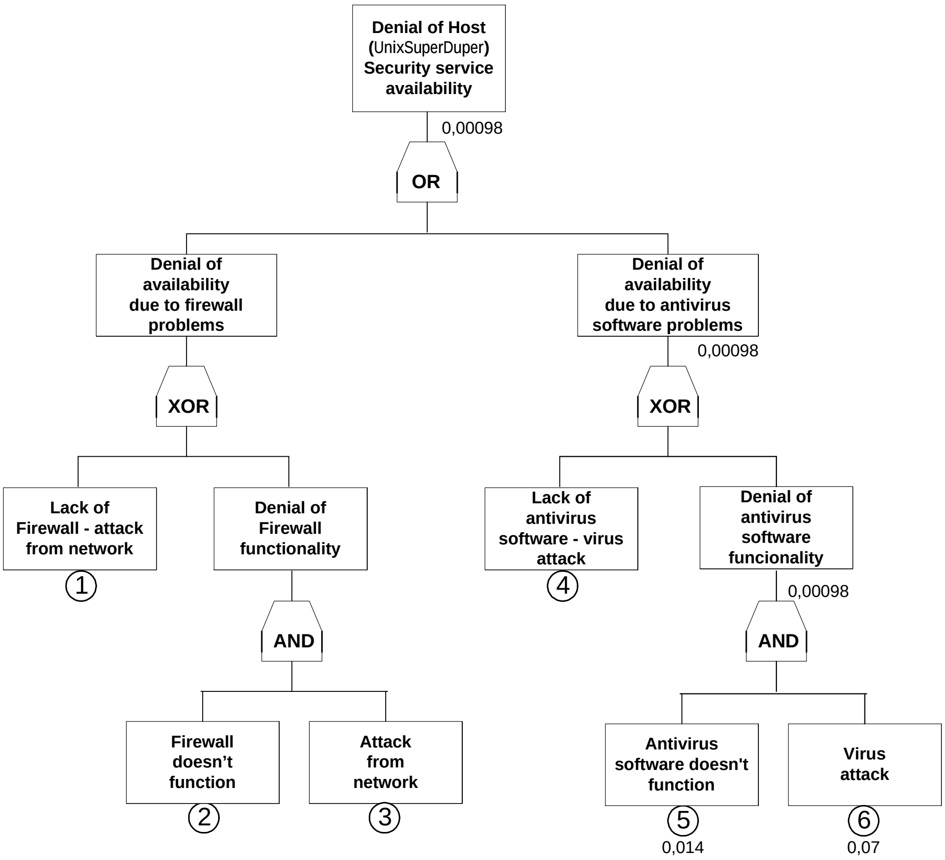

Denial of Host (UnixSuperDuper) Security service availability
0,00098
OR
Denial of availability due to firewall problems
Denial of availability due to antivirus software problems
0,00098
XOR
XOR
Lack of Firewall - attack from network
1
Denial of Firewall functionality
Lack of antivirus software - virus attack
4
Denial of antivirus software funcionality
0,00098
AND
AND
Firewall doesn’t function
2
Attack from network
3
Antivirus software doesn't function
5
0,014
Virus attack
6
0,07

Figure D.3.6: Determination of frequency for Denial of Host (USD) security service availability

Figures D.3.7, D.3.8, D.3.9 and D.3.10 show the fault trees with frequencies of risks that may lead to the *Denial of Host (US) software availability*, *Denial of Host (USD) software availability*, *Denial of Host (US) hardware availability* and *Denial of Host (USD) hardware availability*. The probabilities of basis events were defined with the help of available statistical information and the information provided by the software and hardware support companies used by the chat service administration.

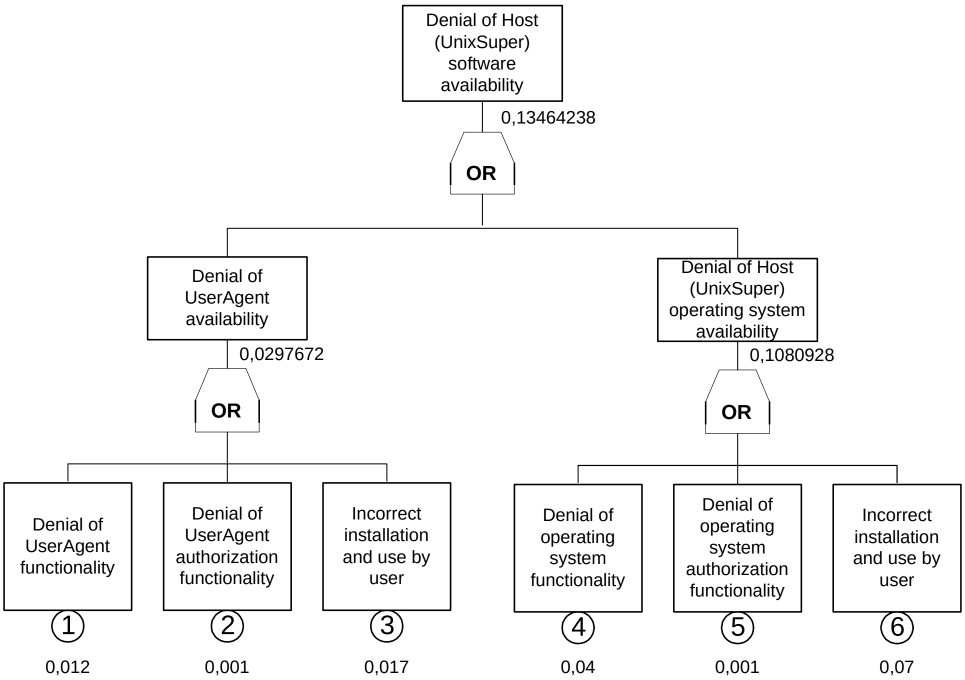

Denial of Host (UnixSuper) software availability
0,13464238
OR
Denial of UserAgent availability
0,0297672
OR
Denial of Host (UnixSuper) operating system availability
0,1080928
OR
Denial of UserAgent functionality
1
0,012
Denial of UserAgent authorization functionality
2
0,001
Incorrect installation and use by user
3
0,017
Denial of operating system functionality
4
0,04
Denial of operating system authorization functionality
5
0,001
Incorrect installation and use by user
6
0,07

Figure D.3.7: Determination of frequency for Denial of Host (US) software availability

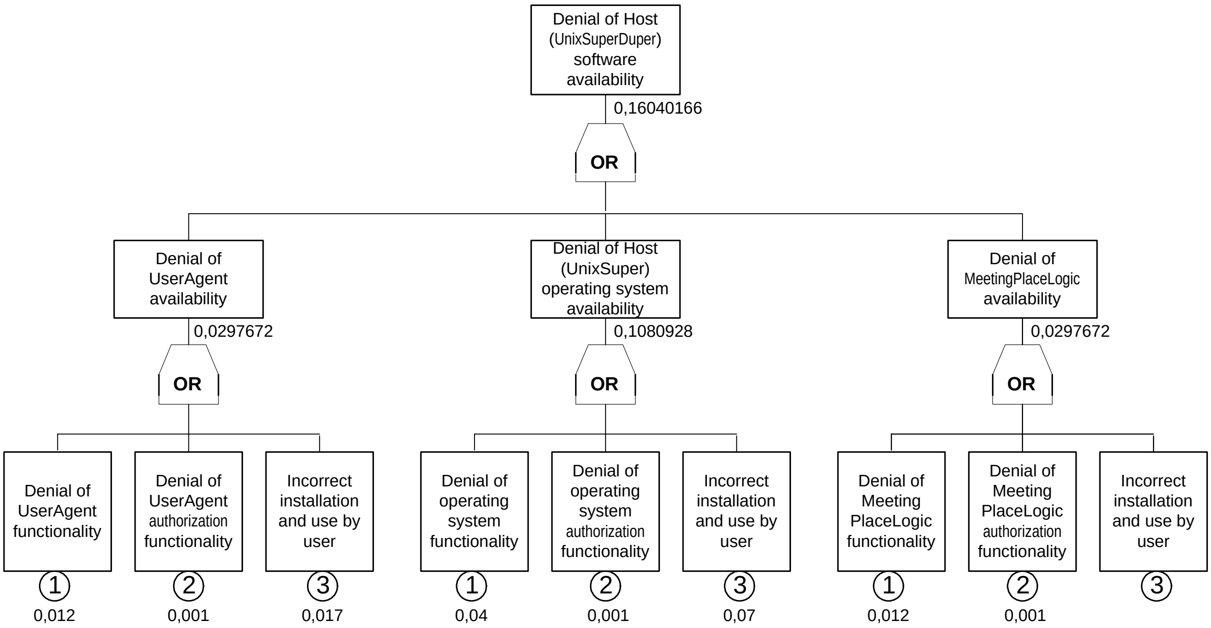

Denial of Host (UnixSuperDuper) software availability
0,16040166
OR
Denial of UserAgent availability
0,0297672
OR
Denial of Host (UnixSuper) operating system availability
0,1080928
OR
Denial of MeetingPlaceLogic availability
0,0297672
OR
Denial of UserAgent functionality
1
0,012
Denial of UserAgent authorization functionality
2
0,001
Incorrect installation and use by user
3
0,017
Denial of operating system functionality
1
0,04
Denial of operating system authorization functionality
2
0,001
Incorrect installation and use by user
3
0,07
Denial of Meeting PlaceLogic functionality
1
0,012
Denial of Meeting PlaceLogic authorization functionality
2
0,001
Incorrect installation and use by user
3

Figure D.3.8: Determination of frequency for Denial of Host (USD) software availability

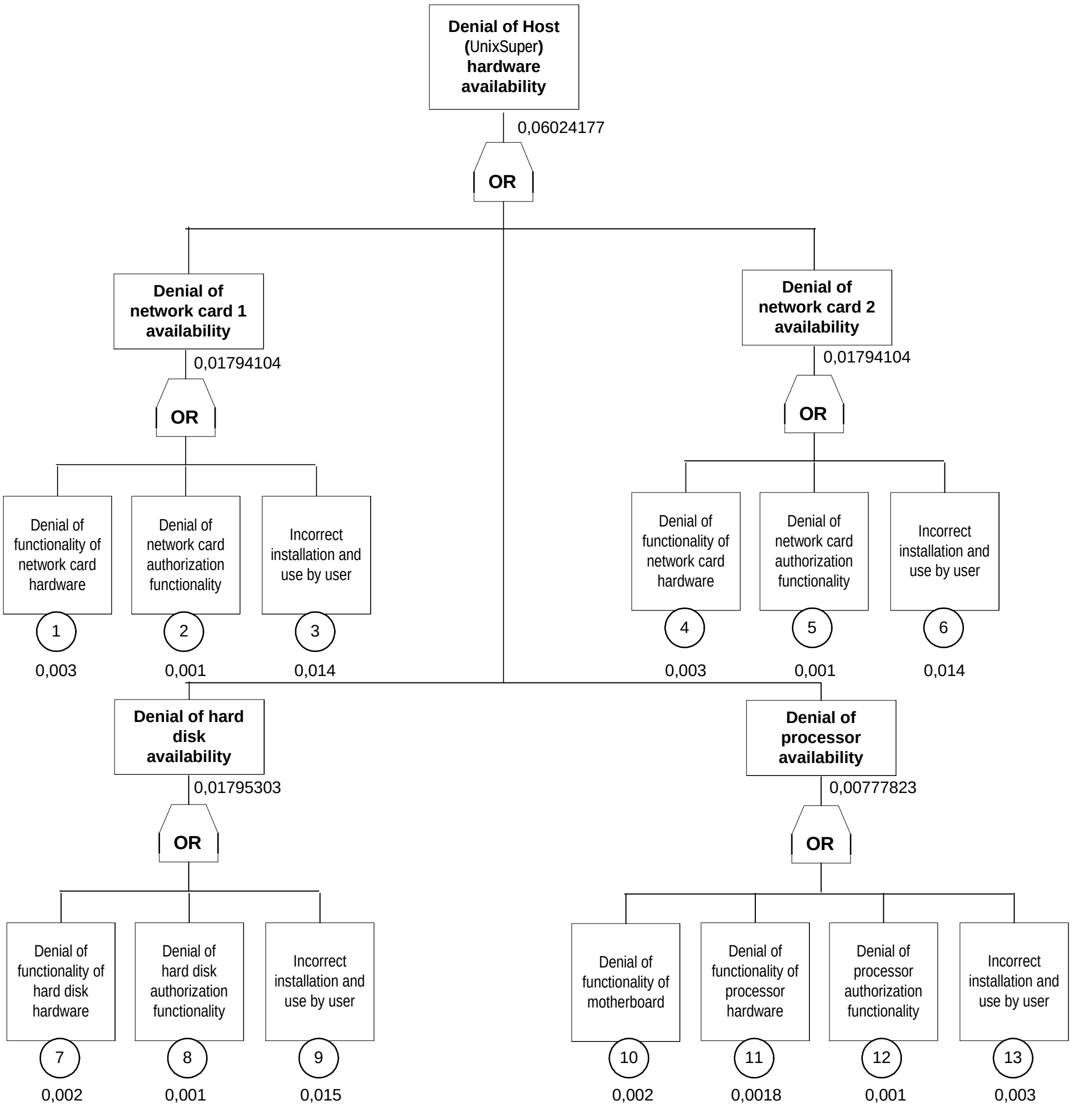

Denial of Host (UnixSuper) hardware availability
0,06024177
OR
Denial of network card 1 availability
0,01794104
OR
Denial of network card 2 availability
0,01794104
OR
Denial of functionality of network card hardware
1
0,003
Denial of network card authorization functionality
2
0,001
Incorrect installation and use by user
3
0,014
Denial of functionality of network card hardware
4
0,003
Denial of network card authorization functionality
5
0,001
Incorrect installation and use by user
6
0,014
Denial of hard disk availability
0,01795303
OR
Denial of processor availability
0,00777823
OR
Denial of functionality of hard disk hardware
7
0,002
Denial of hard disk authorization functionality
8
0,001
Incorrect installation and use by user
9
0,015
Denial of functionality of motherboard
10
0,002
Denial of functionality of processor hardware
11
0,0018
Denial of processor authorization functionality
12
0,001
Incorrect installation and use by user
13
0,003

Figure D.3.9: Determination of frequency for Denial of Host (US) hardware availability

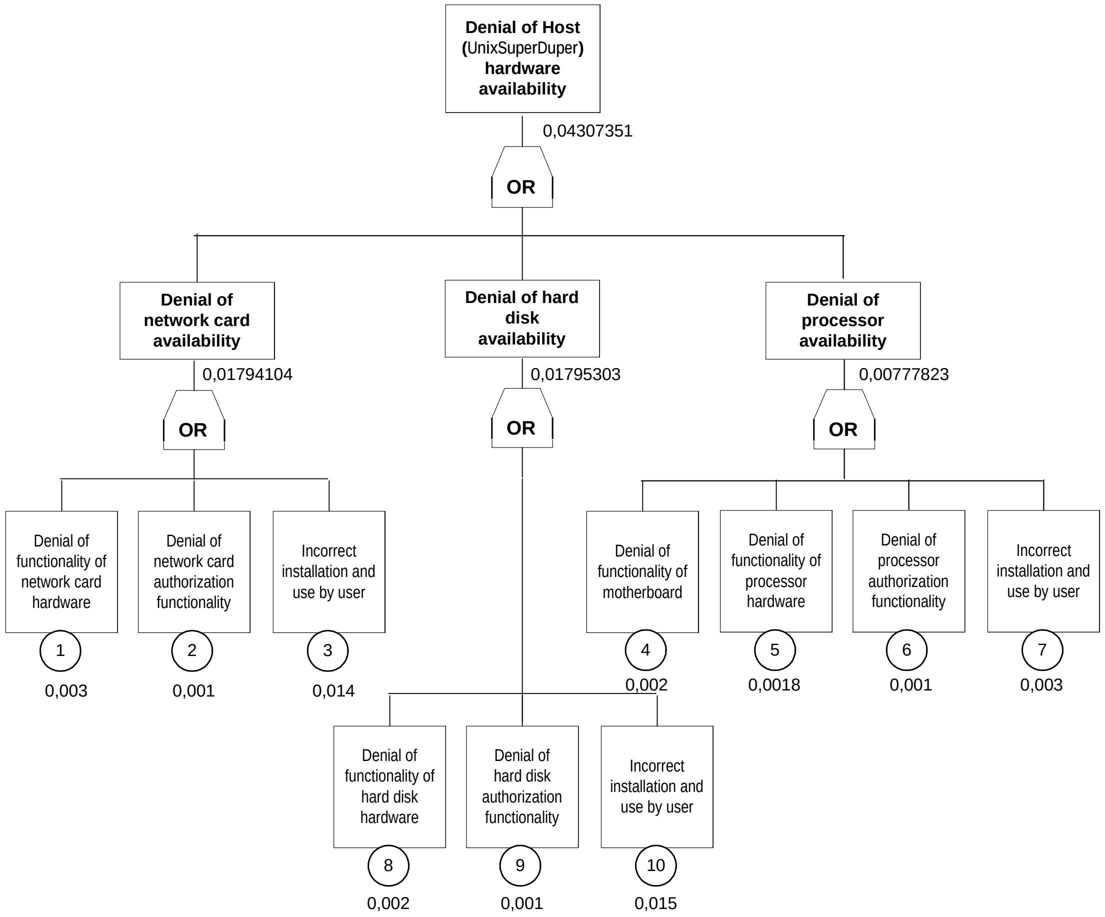

Denial of Host (UnixSuperDuper) hardware availability
0,04307351
OR
Denial of network card availability
0,01794104
OR
Denial of hard disk availability
0,01795303
OR
Denial of processor availability
0,00777823
OR
Denial of functionality of network card hardware
1
0,003
Denial of network card authorization functionality
2
0,001
Incorrect installation and use by user
3
0,014
Denial of functionality of motherboard
4
0,002
Denial of functionality of processor hardware
5
0,0018
Denial of processor authorization functionality
6
0,001
Incorrect installation and use by user
7
0,003
Denial of functionality of hard disk hardware
8
0,002
Denial of hard disk authorization functionality
9
0,001
Incorrect installation and use by user
10
0,015

Figure D.3.10: Determination of frequency for Denial of Host (USD) hardware availability

Figures D.3.11 and D.3.12 show the fault trees with frequencies of risks that may lead to the *Denial of Host (US) availability* and *Denial of Host (USD) availability*. The frequency of risk *Denial of power supply service availability* was defined with the help of information provided by the local power supply company. The probability of risk *Denial of host authorization availability* was defined with the help of available statistical information and the information provided by the local police office.

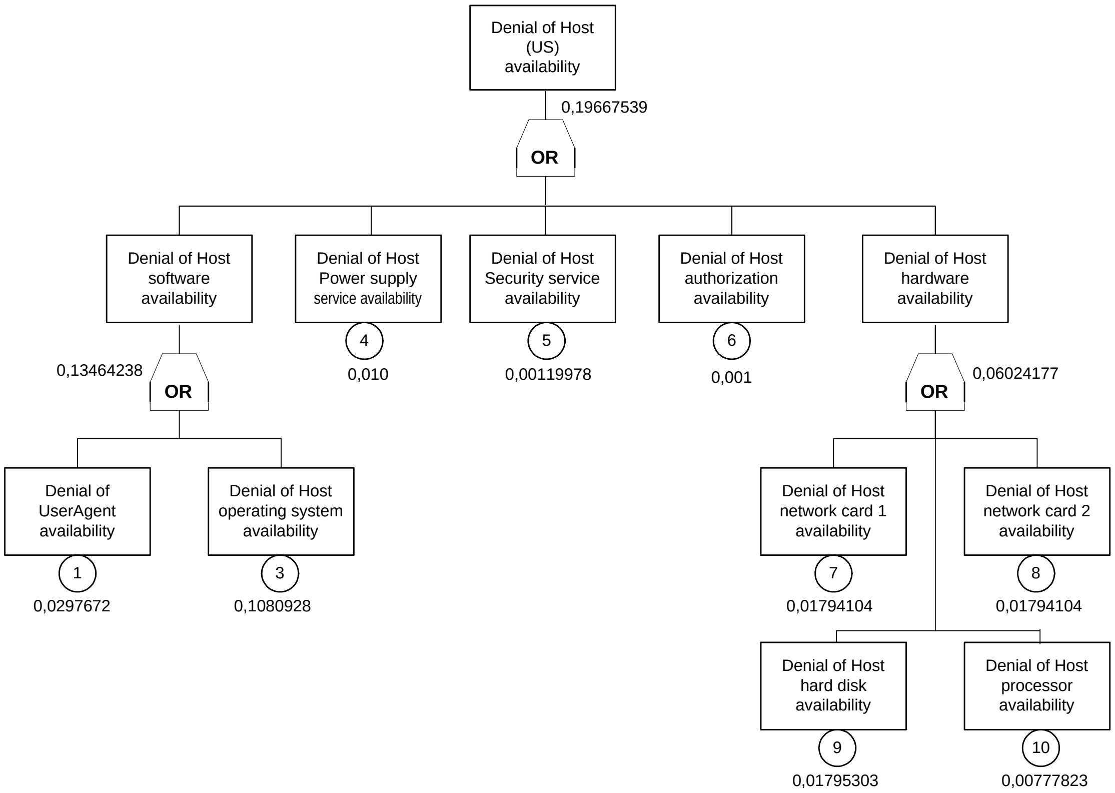

Denial of Host (US) availability
0,19667539
OR
Denial of Host software availability
Denial of Host Power supply service availability
Denial of Host Security service availability
Denial of Host authorization availability
Denial of Host hardware availability
0,13464238
OR
4
0,010
5
0,00119978
6
0,001
OR
0,06024177
Denial of UserAgent availability
Denial of Host operating system availability
Denial of Host network card 1 availability
Denial of Host network card 2 availability
1
0,0297672
3
0,1080928
7
0,01794104
8
0,01794104
Denial of Host hard disk availability
Denial of Host processor availability
9
0,01795303
10
0,00777823

Figure D.3.11: Determination of frequency for Denial of Host (US) availability

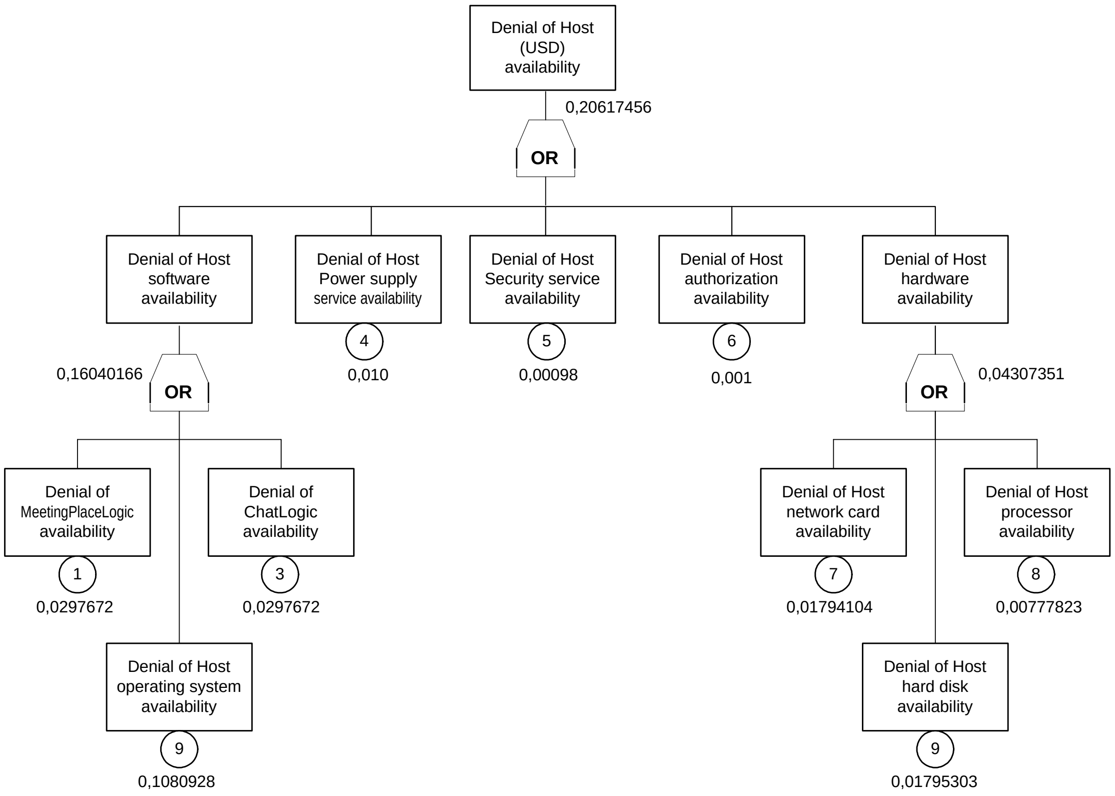

Denial of Host (USD) availability
0,20617456
OR
Denial of Host software availability
Denial of Host Power supply service availability
Denial of Host Security service availability
Denial of Host authorization availability
Denial of Host hardware availability
0,16040166
OR
4
0,010
5
0,00098
6
0,001
OR
0,04307351
Denial of MeetingPlaceLogic availability
Denial of ChatLogic availability
Denial of Host network card availability
Denial of Host processor availability
1
0,0297672
3
0,0297672
7
0,01794104
8
0,00777823
Denial of Host operating system availability
Denial of Host hard disk availability
9
0,1080928
9
0,01795303

Figure D.3.12: Determination of frequency for Denial of Host (USD) availability

Figures D.3.13, D.3.14 and D.3.15 show the fault trees with frequencies of risks that may lead to the *Denial of Network availability*, *Denial of wireless access to service availability* and *Denial of chat service availability*. Frequencies of risks *Denial of Internet connection availability* and *Denial of wireless network availability* were defined with the help of information provided by the network provider used by PDA users and chat service.

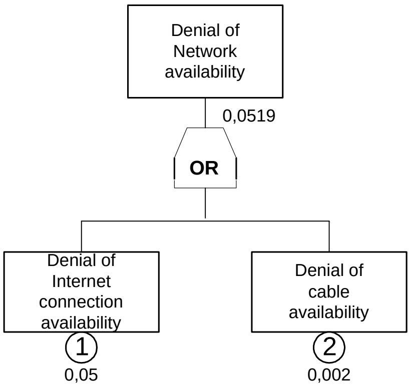

Denial of Network availability
0,0519
OR
Denial of Internet connection availability
Denial of cable availability
1
0,05
2
0,002

Figure D.3.13: Determination of frequency for Denial of Wireless access to service availability

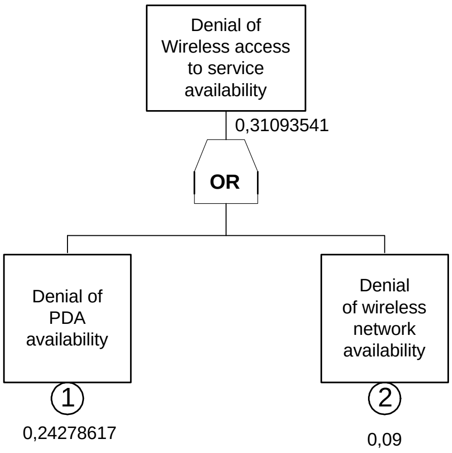

Denial of Wireless access to service availability
0,31093541
OR
Denial of PDA availability
Denial of wireless network availability
1
0,24278617
2
0,09

Figure D.3.14: Determination of frequency for Denial of Wireless access to service availability

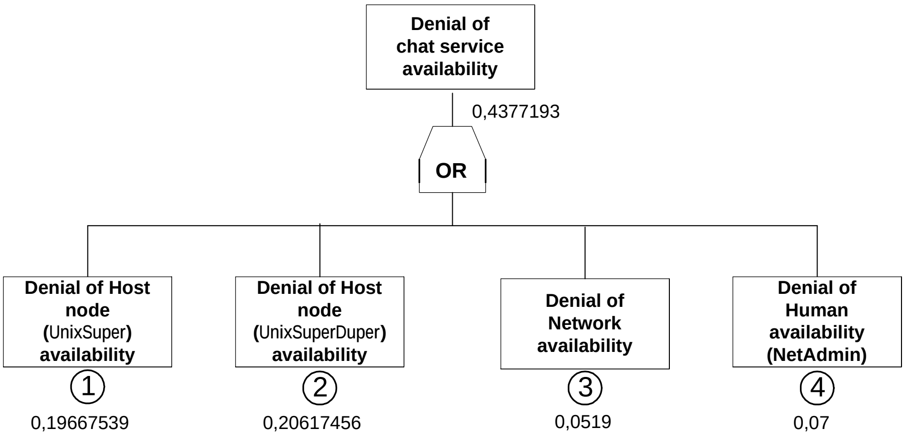

Denial of chat service availability
0,4377193
OR
Denial of Host node (UnixSuper) availability
Denial of Host node (UnixSuperDuper) availability
Denial of Network availability
Denial of Human availability (NetAdmin)
1
0,19667539
2
0,20617456
3
0,0519
4
0,07

Figure D.3.15: Determination of frequency for Denial of Chat service availability

The identified risks frequencies were documented in frequency tables shown below.

Table D.3.6: Frequency table for software availability risks

Stakeholder	Asset	Risk			Risk scenario	Frequency value	Frequency description
PDA user	Availability of service	Denial of host (PDA) software availability	Denial of host (PDA) operating system availability		The Host (PDA) operating system doesn’t function or malfunction	0,05412778 Possible	Probabilities of basis events were defined with help of information provided by PDA user support company
			Denial of Host (PDA) application software availability	Denial of PDA chat software functionality	PDA chat software doesn’t function or malfunction	0,0651544 Possible	Probabilities of basis events were defined with help of information provided by PDA user support company
System owner	Availability of service	Denial of host (US) software availability	Denial of host (US) operating system availability		The Host (US) operating system doesn’t function or malfunction	0,1080928 Possible	Probabilities of basis events were defined with help of available statistical information and information provided by a software support company used by chat service administration
			Denial of Host (US) application software availability	Denial of UserAgent software component functionality	UserAgent software component doesn’t function or malfunction	0,0297672 Unlikely	Probabilities of basis events were defined with help of information provided by a software support company used by chat service administration
		Denial of host (USD) software availability	Denial of host (USD) operating system availability		The Host (USD) operating system doesn’t function or malfunction	0,1080928 Possible	Probabilities of basis events were defined with help of available statistical information and information provided by a software support company used by chat service administration
			Denial of Host (USD) application software availability	Denial of MeetingPlace Logic software component functionality	MeetingPlaceLogic software component doesn’t function or malfunction	0,0297672 Unlikely	Probabilities of basis events were defined with help of information provided by a software support company used by chat service administration
				Denial of ChatLogic software component functionality	ChatLogic software component doesn’t function or malfunction	0,0297672 Unlikely	Probabilities of basis events were defined with help of information provided by a software support company used by chat service administration

Table D.3.7: Frequency table for hardware availability risks

Stakeholder	Asset	Risk		Risk scenario	Frequency value	Frequency description
PDA user	Availability of service	Denial of host (PDA) hardware availability	Denial of host (PDA) memory flash card availability	The Host (PDA) memory flash card doesn’t function or malfunction	0,01137002 Unlikely	Probabilities of basis events were defined with help of information provided by PDA user support company

			Denial of Host (PDA) internal hardware availability	Denial of network card availability	Network card doesn’t function or malfunction	0,0244051 Unlikely	Probabilities of basis events were defined with help of information provided by PDA user support company
System owner	Availability of service	Denial of host (US) and host (USD) hardware availability	Denial of host (US & USD) storage device availability		The host hard disc doesn’t function or malfunction	0,01795303 Unlikely	Probabilities of basis events were defined with help of available statistical information and information provided by hardware support company used by chat service administration
			Denial of host (US & USD) internal hardware availability	Denial of network card availability	Network card doesn’t function or malfunction	0,01794104 Unlikely	Probabilities of basis events were defined with help of available statistical information and information provided by hardware support company used by chat service administration
				Denial of processor availability	Processor doesn’t function or malfunction	0,00777823 Rare	Probabilities of basis events were defined with help of available statistical information and information provided by hardware support company used by chat service administration

Table D.3.8: Frequency table for host security service availability risks

Stakeholder	Asset	Risk		Risk scenario	Frequency value	Frequency description
PDA user	Availability of service	Denial of host (PDA) security service availability	Lack of firewall – host is attacked from the Internet	The host node is attacked from the Internet	0,02 Unlikely	Probabilities of basis events were defined with help of information provided by PDA user support company
			Lack of antivirus software – host is attacked by computer virus	The host node is attacked by computer virus	0,07 Possible	Probabilities of basis events were defined with help of information provided by PDA user support company
System owner	Availability of service	Denial of host (US & USD) security service availability	Host (US) is attacked from the Internet	The host node (US) is attacked from the Internet	0,00022 Rare	Probabilities of basis events were defined with help of available statistical information and information provided by software and hardware support company used by chat service administration
			Host (US & USD) is attacked by computer virus	The host node (US & USD) is attacked by computer virus	0,00098 Rare	Probabilities of basis events were defined with help of available statistical information and information provided by software and hardware support company used by chat service administration

Table D.3.9: Frequency table for host availability risks

Stakeholder	Asset	Risk		Risk scenario	Frequency value	Frequency description
PDA user	Availability of service	Denial of host (PDA) availability	Denial of host software availability	The host software doesn't function or malfunction	0,11575552 Possible	The frequency is based on frequencies of denial of availabilities of host operating system and chat software
			Denial of host hardware availability	The host hardware doesn't function or malfunction	0,03549764 Unlikely	The frequency is based on frequencies of denial of availabilities of memory flash card and network card
			Denial of power supply service availability	Lithium battery doesn't function or malfunction	0,014 Unlikely	Probabilities of basis events were defined with help of information provided by PDA user support company
			Denial of host security service availability	The host is attacked from the internet and/or by computer virus	0,0886 Possible	The probability is determined by analysing statistical information that shows percentage of PDA terminals attacked from the Internet or by computer virus
			Denial of host authorization availability	PDA is stolen	0,012 Unlikely	Probabilities of basis events were defined with help of information provided by PDA user support company
System owner	Availability of service	Denial of host (US & USD) availability	Denial of host (US) software availability	The host software doesn't function or malfunction	0,13464238 Possible	The frequency is based on frequencies of denial of availabilities of host (US) operating system and chat software
			Denial of host (USD) software availability	The host software doesn't function or malfunction	0,16040166 Possible	The frequency is based on frequencies of denial of availabilities of host (USD) operating system and chat software
			Denial of host (US) hardware availability	The host hardware doesn't function or malfunction	0,06024177 Possible	The frequency is based on frequencies of denial of availabilities of host (US) hard disc, two network cards and processor
			Denial of host (USD) hardware availability	The host hardware doesn't function or malfunction	0,04307351 Unlikely	The frequency is based on frequencies of denial of availabilities of host (USD) hard disc, network card and processor
			Denial of power supply service availability (US & USD)	The local provider of electricity has technical problems and can't provide electricity	0,010 Unlikely	The probability is determined with help of statistical information provided by the local electricity provider
			Denial of host (US) security service availability	The host is attacked from the internet and/or by computer virus	0,00119978 Rare	Probabilities of basis events were defined with help of available statistical information and information provided by support company used by chat service administration

			Denial of host (USD) security service availability		The host is attacked from the internet and/or by computer virus	0,00098 Rare	Probabilities of basis events were defined with help of available statistical information and information provided by support company used by chat service administration
			Denial of host (US & USD) authorization availability		The chat service nodes are stolen or damaged	0,001 Rare	Probability was defined with help of available statistical information

Table D.3.10: Frequency table for service availability risks

Stakeholder	Asset	Risk			Risk scenario	Frequency value	Frequency description
System owner	Availability of service	Denial of Service availability	Denial of host (US) availability		The host (US) is not available	0,19667539 Possible	The frequency is based on frequencies of denial of availabilities of host (US) software, hardware, power supply service, host authorization and security service
			Denial of host (USD) availability		The host (USD) is not available	0,20617456 Likely	The frequency is based on frequencies of denial of availabilities of host (USD) software, hardware, power supply service, host authorization and security service
			Denial of Network availability	Denial of Internet connection availability	The local Internet provider has technical problems and can't provide access to the Internet	0,05 Possible	The frequency is defined with help of available statistical information and information provided by Internet provider
				Denial of cable availability	The cable connecting two chat service nodes is damaged or doesn't function	0,002 Rare	The frequency is defined with help of available statistical information and information provided by support company
			Denial of Human availability		The network administrator makes fail during maintenance of chat service	0,07 Possible	Usually it takes 1 hour for network administrator to recover the chat service from fail ((41*1)/30000)*100 = 0,13%
PDA user	Availability of service	Denial of wireless access to service availability	Denial of PDA availability		PDA is not available	0,24278617 Likely	The frequency is based on frequencies of denial of availabilities of memory flash card, network card , lithium battery, host authorization and security service
			Denial of wireless network availability		Wireless network is not available	0,09 Possible	The frequency is based on information provided by wireless network provider

D.4 Risk evaluation

This section presents the results from the Risk evaluation of the chat service. The section is structured into four sub-sections. Sub-section D4.1 describes the Activity 4.1 Identification of risks values. Activity 4.2 Update of risks values is presented in sub-section D4.2. Sub-section D4.3 documents the Activity 4.3 Categorisation of risks into risk treatment categories. Sub-section D4.4 describes the Activity 4.4 Specification of priorities of risk treatment categories.

D.4.1 Activity 4.1: Identification of risks values

Objective	Determine the risk value for each risk

Table D.4.1 documents all risks along with their identified risk values. For the identification of risk values we applied the Risk Matrix (Table D.1.4)

Table D.4.1: Risk levels table

Stakeholder	Asset	Risk			Consequence value	Frequency value	Risk value
PDA user	Availability of service	Denial of host (PDA) software availability	Denial of host (PDA) operating system availability		Major	Possible	Moderate
			Denial of Host (PDA) application software availability	Denial of PDA chat software availability	Minor	Possible	Low
		Denial of host (PDA) hardware availability	Denial of host (PDA) memory flash card availability		Moderate	Unlikely	Low
			Denial of Host (PDA) internal hardware availability	Denial of network card availability	Major	Unlikely	Moderate
		Denial of host (PDA) security service availability	Lack of firewall – host is attacked from the Internet		Catastrophic	Unlikely	Moderate
			Lack of antivirus software – host is attacked by computer virus		Major	Possible	Moderate
		Denial of Host (PDA) power supply service availability			Moderate	Unlikely	Low
		Denial of Host (PDA) authorization Availability			Catastrophic	Unlikely	Moderate
		Denial of wireless network Availability			Minor	Possible	Low
System owner	Availability of service	Denial of host (US) software availability	Denial of host (US) operating system availability		Moderate	Possible	Moderate
			Denial of Host (US) application software availability	Denial of UserAgent software component availability	Minor	Unlikely	Low

		Denial of host (USD) software availability	Denial of host (USD) operating system availability		Moderate	Possible	Moderate
			Denial of Host (USD) application software availability	Denial of MeetingPlace Logic software component availability	Minor	Unlikely	Low
				Denial of ChatLogic software component availability	Minor	Unlikely	Low
		Denial of host (US) and host (USD) hardware availability	Denial of host (US & USD) storage device availability		Moderate	Unlikely	Low
			Denial of host (US & USD) internal hardware availability	Denial of network card availability	Major	Unlikely	Moderate
				Denial of processor availability	Major	Rare	Low
		Denial of host (US & USD) security service availability	Host (US) is attacked from the Internet		Moderate	Rare	Low
			Host (US & USD) is attacked by computer virus		Major	Rare	Low
		Denial of Host (US & USD) power supply service availability			Moderate	Unlikely	Low
		Denial of Host (US & USD) authorization availability			Catastrophic	Rare	Moderate
		Denial of Network availability	Denial of Internet connection availability		Minor	Possible	Low
			Denial of cable availability		Minor	Rare	No risk
		Denial of Human availability			Minor	Possible	Low

D.4.2 Activity 4.2: Update of risks values

Objective	Update risks values in order to eliminate risks that have acceptable risk values

We compared the risk values documented in the Risk levels table (Table D.4.1) with the risk evaluation criteria and concluded that we can accept all risks that have the risk value equal or less than “Low”. We documented updated risk values in the Updated risk levels table shown in Table D.4.2

Table D.4.2: Updated risk levels table

Stakeholder	Asset	Risk			Consequence value	Frequency value	Updated Risk value
PDA user	Availability of service	Denial of host (PDA) software availability	Denial of host (PDA) operating system availability		Major	Possible	Moderate
			Denial of Host (PDA) application software availability	Denial of PDA chat software availability	Minor	Possible	Accepted
		Denial of host (PDA) hardware availability	Denial of host (PDA) memory flash card availability		Moderate	Unlikely	Accepted
			Denial of Host (PDA) internal hardware availability	Denial of network card availability	Major	Unlikely	Moderate
		Denial of host (PDA) security service availability	Lack of firewall – host is attacked from the Internet		Catastrophic	Unlikely	Moderate
			Lack of antivirus software – host is attacked by computer virus		Major	Possible	Moderate
		Denial of Host (PDA) power supply service availability			Moderate	Unlikely	Accepted
		Denial of Host (PDA) authorization Availability			Catastrophic	Unlikely	Moderate
		Denial of wireless network availability			Minor	Possible	Accepted
System owner	Availability of service	Denial of host (US) software availability	Denial of host (US) operating system availability		Moderate	Possible	Moderate
			Denial of Host (US) application software availability	Denial of UserAgent software component availability	Minor	Unlikely	Accepted
		Denial of host (USD) software availability	Denial of host (USD) operating system availability		Moderate	Possible	Moderate
			Denial of Host (USD) application software availability	Denial of MeetingPlace Logic software component availability	Minor	Unlikely	Accepted
				Denial of ChatLogic software component availability	Minor	Unlikely	Accepted
		Denial of host (US) and host (USD) hardware availability	Denial of host (US & USD) storage device availability		Moderate	Unlikely	Accepted
			Denial of host (US & USD) internal hardware availability	Denial of network card availability	Major	Unlikely	Moderate
				Denial of processor availability	Major	Rare	Accepted
		Denial of host (US &	Host (US) is attacked from the Internet		Moderate	Rare	Accepted

		USD) security service availability	Host (US & USD) is attacked by computer virus	Major	Rare	Accepted
		Denial of Host (US & USD) power supply service availability		Moderate	Unlikely	Accepted
		Denial of Host (US & USD) authorization availability		Catastrophic	Rare	Moderate
		Denial of Network availability	Denial of Internet connection availability	Minor	Possible	Accepted
			Denial of cable availability	Minor	Rare	Accepted
		Denial of Human availability		Minor	Possible	Accepted

D.4.3 Activity 4.3: Categorisation of risks into risk treatment categories

Objective	Organise risks into risk treatment categories to make the risk treatment more effective

We categorised risks into risk treatment categories with the help of the Possible risk treatment categories table (Table 5.48). Table D.4.3 shows the categorization of risks into risk treatment categories.

Table D.4.3: Risk treatment category table

Risk Treatment Category	Risks
Host operating system availability risks	1. Denial of host (PDA) operating system availability 2. Denial of host (US) operating system availability 3. Denial of host (USD) operating system availability
Host hardware availability risks	1. Denial of network card availability (PDA) 2. Denial of network card availability (US) 3. Denial of network card availability (USD)
Host security service availability risks (firewall)	1. Lack/Denial of firewall – host (PDA) is attacked from the Internet
Host security service availability risks (antivirus software)	1. Lack/Denial of antivirus software – host (PDA) is attacked by computer virus
Host authorization availability risks	1. Denial of Host (PDA) authorization availability 2. Denial of Host (US) authorization availability 3. Denial of Host (USD) authorization availability

D.4.4 Activity 4.4: Specification of priorities of risk treatment categories

Objective	Organise risks into risk treatment categories to make the risk treatment more effective

The risk treatment category value was calculated with the help of *the highest risk value* approach (see the MODA Activity 4.4):
The risk treatment category value consists of two elements:

- The highest risk value represented in this risk treatment category.
- The number of risks with the highest risk level.

For example, M3 means that the highest risk value represented in this category is “Moderate” (M) and 3 is the number of risks with this risk value. The identified values and priorities of risk treatment categories are shown in Table D.4.4.

Table D.4.4: Risk treatment category priority table

Risk Treatment Category	Risks	Risk Treatment Category Value	Risk Treatment Category Priority
Host operating system availability risks	1. Denial of host (PDA) operating system availability 2. Denial of host (US) operating system availability 3. Denial of host (USD) operating system availability	M3	1
Host hardware availability risks	1. Denial of network card (PDA) availability 2. Denial of network card (US) availability 3. Denial of network card (USD) availability	M3	1
Host authorization availability risks	1. Denial of Host (PDA) authorization availability 2. Denial of Host (US) authorization availability 3. Denial of Host (USD) authorization availability	M3	1
Host security service availability risks (antivirus software)	1. Lack/Denial of antivirus software – host (PDA) is attacked by computer virus	M1	2
Host security service availability risks (firewall)	1. Lack/Denial of firewall – host (PDA) is attacked from the Internet	M1	2

D.5 Risk treatment

This section presents the results from the Risk treatment of the chat service. The section is structured into two sub-sections. Sub-section D.5.1 describes the Activity 5.1 Identification of treatment options. Sub-section D.5.2 presents the Activity 5.2 Specification of risks treatment priorities.

D.5.1 Activity 5.1: Identification of treatment options

Objective	Identify risk treatment options and risk treatment actions for each risk treatment category

The risk treatment options and risk treatment actions were identified with the help of templates for risk treatment. The identified treatment options and treatment actions are documented in the risk treatment tables that were constructed for each risk treatment category. Figure D.5 shows how templates from appendix B were used to identify treatment options and treatment actions for each risk treatment category. This figure also shows treatment tables that we constructed to document chosen risk treatment options and risk treatment actions.

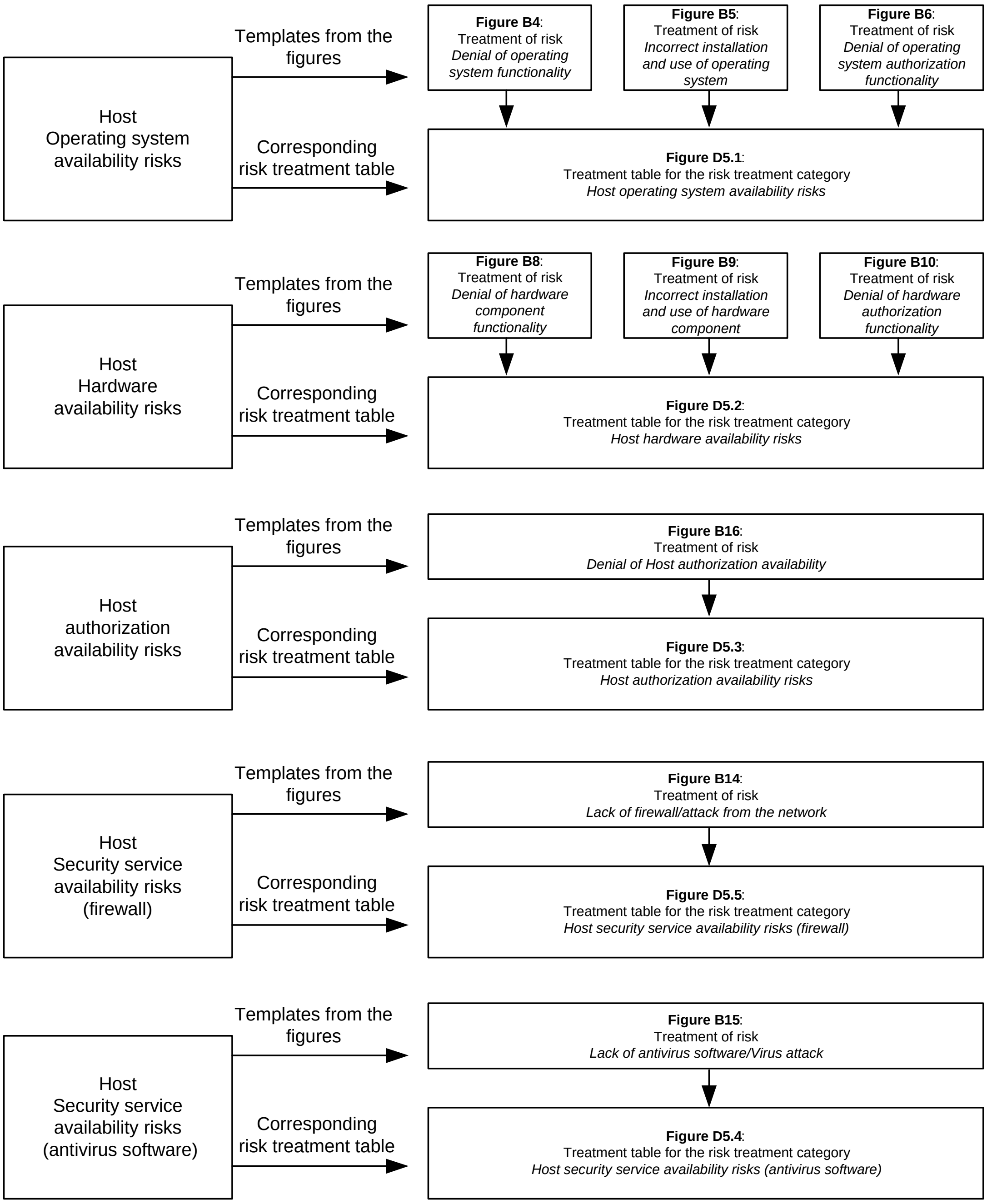

Host
Operating system
availability risks
Templates from the figures
Corresponding risk treatment table
Figure B4: Treatment of risk *Denial of operating system functionality*
Figure B5: Treatment of risk *Incorrect installation and use of operating system*
Figure B6: Treatment of risk *Denial of operating system authorization functionality*
Figure D5.1: Treatment table for the risk treatment category *Host operating system availability risks*
Host
Hardware
availability risks
Templates from the figures
Corresponding risk treatment table
Figure B8: Treatment of risk *Denial of hardware component functionality*
Figure B9: Treatment of risk *Incorrect installation and use of hardware component*
Figure B10: Treatment of risk *Denial of hardware authorization functionality*
Figure D5.2: Treatment table for the risk treatment category *Host hardware availability risks*
Host
authorization
availability risks
Templates from the figures
Corresponding risk treatment table
Figure B16: Treatment of risk *Denial of Host authorization availability*
Figure D5.3: Treatment table for the risk treatment category *Host authorization availability risks*
Host
Security service
availability risks
(firewall)
Templates from the figures
Corresponding risk treatment table
Figure B14: Treatment of risk *Lack of firewall/attack from the network*
Figure D5.5: Treatment table for the risk treatment category *Host security service availability risks (firewall)*
Host
Security service
availability risks
(antivirus software)
Templates from the figures
Corresponding risk treatment table
Figure B15: Treatment of risk *Lack of antivirus software/Virus attack*
Figure D5.4: Treatment table for the risk treatment category *Host security service availability risks (antivirus software)*

Figure D.5: Templates and the corresponding risk treatment tables

Table D.5.1: Chat Service Treatment table for host operating system availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Denial of operating system functionality	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Operating system must be kept updated	More stable and effective operating system	Cost of work time of user (update) and cost of update
			2)	Upgrade to the more reliable version of OS	More reliable and stable functionality of OS	Cost of work time of user (update) and cost of update
			3)	Regular tests of operating system	Early discovering and preventing of operating system problems	Cost of work time of user (tests) and cost of tests
			4)	Install software for monitoring of operating system functionality	Early discovering and preventing of operating system problems	Cost of work time of user (installation) and cost of software
		c)	**1)**	Daily full data and system backup	Insure possibility for recovery from operating system problems	Cost of work time of user (backup) and cost of backup software and hardware
				Have compact discs with operating system, diagnostic and recovery tools available	Insure possibility for recovery from operating system problems	Cost of OS, diagnostic and recovery tools
			2)	Install OS and application programs on additional work station	Insure possibility for recovery from operating system problems – use of additional work station in case of denial of OS functionality on the main workstation	Cost of additional work station and cost of work time of user (installation)
			3)	Regular tests of OS installed on additional work station	Insure correct functionality of OS on additional work station - use of additional work station in case of denial of OS functionality on the main workstation	Cost of work station, installation (user work hours) and cost of tests
			4)	Install software on additional work station for monitoring of operating system functionality	Insure correct functionality of OS on additional work station - use of additional work station in case of denial of OS functionality on the main workstation	Cost of installation (user work hours) and cost of software
		d)	**1)**	Have an insurance that covers the financial consequences of denial of operating system functionality	Reduce financial consequences of denial of operating system functionality	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

	Denial of operating system authorization functionality	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Introduce the strict rules for choosing and changing of password	Insure strong protection against unauthorized access to OS	Cost of work time of user/specialist to formulate the rules
				Use the screensaver with password protection	Better protection of OS against unauthorized access	Cost of time to change screensaver options
				Users should always logout whenever they leave computer for any period of time	Better protection of OS against unauthorized access	Cost of time to logout
			2)			
			3)	Regular update and tests of employees/users security awareness	Better protection of OS against unauthorized access	Cost of update and tests
			4)			
		c)	**1)**	Recovery from operating system problems should be done only by a specialized company (technical support)	Quick recovery from OS problems	Cost of technical support
			2)			
			3)			
			4)			
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to operating system	Reduce financial consequences of unauthorized access to operating system	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

	Incorrect installation and use of operating system	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	The competence of personnel responsible for use/installation of OS should be updated regularly (regular training courses)	More correct use of operating system	Cost of training course
			2)	Help in installation and use of OS from a software support service	More correct and efficient use of operating system	Cost of software support service
			3)	Self study of user manual/text book and self testing of knowledge	More correct and efficient use of operating system	Cost of book/teaching program
			4)			
		c)	**1)**	Use software support service for recovery from OS problems	Quick recovery from OS problems	Cost of software support service
			2)	Have a backup competent user available	Possible more efficient use of operating system. OS user can always get quick help from competent user	Cost of work time of backup user
			3)			
			4)			
		d)	**1)**	Have an insurance that covers the financial consequences of incorrect use of OS	Reduce financial consequences of incorrect use of operating system.	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

Table D.5.2: Chat Service Treatment table for host hardware availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Denial of hardware component functionality	a)	1)			
			2)			
			3)			
			4)			
		b)	1)			
			2)	Install another more reliable hardware component	Possible more reliable and effective functionality of hardware component	Cost of work time of user (installation) and cost of hardware component
			3)	Regular tests of hardware component	Early discovering and preventing of hardware component problems	Cost of work time of user (tests) and cost of tests
			4)	Install software for monitoring of hardware component functionality	Early discovering and preventing of hardware component problems	Cost of work time of user (installation) and cost of software
		c)	1)	Have an additional hardware component available	Use additional hardware component in case of denial of main hardware component	Cost of additional hardware component
			2)	Install an additional hardware component with the same functionality	Use additional hardware component in case of denial of main hardware component	Cost of installation (work hours) and cost of additional hardware
			3)	Regular tests of additional hardware component functionality	Insure correct functionality of additional hardware component -insure possibility for its use in case of denial of main hardware component	Cost of additional hardware component and cost of tests
			4)	Install software for monitoring of additional hardware component functionality	Early discovering and preventing of additional hardware component problems - insure possibility for its use in case of denial of main software	Cost of installation (work hours) and cost of software
		d)	1)	Have an insurance that covers the financial consequences of denial of basic hardware component functionality	Reduce financial consequences of denial of basic hardware component functionality	Cost of insurance
			2)			
			3)			
			4)			
		e)	1)			
			2)			
			3)			
			4)			

	Denial of hardware component (HC) authorization functionality	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Provide regular security awareness training of employees who use/install hardware components	Better protection of hardware component against unauthorized access	Cost of training
			2)			
			3)	Regular update and tests of security personal competence	Better protection of hardware component against unauthorized access	Cost of update and tests
			4)	Install software for monitoring and detection of access to the room/area where HC is installed	Insure access to hardware of only authorized users	Cost of work time of user (installation) and cost of software
		c)	**1)**	Recovery from hardware problems should be done only by a specialized company (technical support)	Quick recovery from hardware problems	Cost of technical support
			2)			
			3)			
			4)			
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to hardware component	Reduce financial consequences of unauthorized access to hardware component	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

	Incorrect installation and use of hardware	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	The competence of personnel responsible for use/installation of hardware components should be updated regularly	More correct use of hardware component	Cost of regular update of user competence (e.g. cost of computer magazine subscription)
			2)	Help in installation and use of hardware component from a hardware support service	More correct and efficient use of hardware component	Cost of hardware support service
			3)	Self study of user manual/text book and self testing of knowledge	More correct and efficient use of hardware component	Cost of book/user manual
				Use of interactive teaching program with tests of knowledge	More correct and efficient use of hardware component	Cost of interactive teaching program
			4)			
		c)	**1)**	Use hardware support service	Quick recovery from hardware problems	Cost of hardware support service
			2)	Have a backup competent user available	User can always get quick help from competent user	Cost of work time of backup user
			3)			
			4)			
		d)	**1)**	Have an insurance that covers the financial consequences of incorrect use of hardware component	Reduce financial consequences of incorrect use of hardware component	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

Table D.5.3: Chat Service Treatment table for host authorization availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Denial of Host authorization availability	**a)**	**1)**			
			2)			
			3)			
			4)			
		b)	**1)**	Host node should be fastened with screws to a wall, floor or table and physical access to the host node should be secured with a lock	Improve protection against unauthorized access to host node	Cost of work time of user (installation) and cost of equipment (screws, lock)
				Access to the room where host node is installed should be protected by door with a lock	Improve protection against unauthorized access to host node	Cost of work time of user/specialist to formulate the rules
			2)	Install host node in an other room/area with more strong access control	Improve protection against unauthorized access to host node	Cost of work time of user (installation)
			3)	Self study of user manual/text book about host security and self testing of knowledge	Better protection of host node against unauthorized access	Cost of book/manual
			4)	Install software for monitoring and detection of access to the room/area where host node is installed	Insure access to the host node of only authorized users	Cost of work time of user (installation) and cost of software
		c)	**1)**	Have an additional host node with installed operating system and application programs available	Better availability of service in case of damage (denial) of original host node	Cost of additional host node
			2)	Install and fasten with screws an additional host node with installed OS and application programs in another room with more strong access control	Improve protection against unauthorized access to additional host node – insure possibility of its use in case of denial of the main host node	Cost of work time of user (installation) and cost of additional host node
			3)	Test regularly (monthly) the functionality of OS and application programs installed on additional host node	Insure correct and effective functionality of additional host node – denial of functionality of original host node will not affect service availability	Cost of work time of user (tests)
			4)	Install software for monitoring and detection of access to the room/area where additional host node is installed	Insure access to additional host node of only authorized users – insure possibility of its use in case of denial of the main host node	Cost of work time of user (installation) and cost of software
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to host node	Reduce financial consequences of unauthorized access to host node	Cost of insurance
			2)			
			3)			
			4)			
		e)	**1)**			
			2)			
			3)			
			4)			

Table D.5.4: Chat Service Treatment table for host security service availability risks (antivirus software)

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Lack of antivirus software/virus attack	a)	1)			
			2)			
			3)			
			4)			
		b)	1)	Attachments from unknown sources should not be opened	Reduce the possibility for virus attack	No cost
				Compact disks and diskettes should be virus checked before they can be used	Reduce the possibility for virus attack	No cost
				Antivirus software should be regularly updated	Reduce the possibility for virus attack	Cost of update
			2)	Install antivirus software	Reduce the possibility for virus attack	Cost of software
			3)	Self study of user manual/text book about host security and self testing of knowledge	Better protection of host node against virus attack	Cost of book/manual
			4)			
		c)	1)	Recovery from a virus attack should be done by specialized company (technical support)	Quick recovery from virus attack	Cost of technical support
			2)	Install OS, application programs and antivirus software on additional work station	Use of additional work station in case of denial of functionality of the main work station	Cost of additional work station and cost of work time of user (installation)
			3)	Regular tests of OS and application programs installed on additional work station	Insure possibility for use of additional work station in case of denial of functionality of the main work station	Cost of work station, installation of OS and application programs (work hours) and cost of tests
			4)			
		d)	1)	Have an insurance that covers the financial consequences of virus attack	Reduce financial consequences of virus attack	Cost of insurance
			2)			
			3)			
			4)			
		e)	1)			
			2)			
			3)			
			4)			

Table D.5.5: Chat Service Treatment table for host security service availability risks (firewall)

ID	Risk	Approach	Treatment option	Treatment action	Benefit	Cost
	Lack of firewall/attack from the network	a)	1)	Remove connection from the Internet	Eliminate the possibility of attack from the Internet	Possible reduction of service availability and revenue
			2)			
			3)			
			4)			
		b)	1)	Firewall should be regularly updated	Reduce the possibility for virus attack	Cost of update
			2)	Install firewall	Better protection of host node against network attacks	Cost of work time of user (installation) and cost of software
			3)	Self study of user manual/text book about host security and self testing of knowledge	Better protection of host node against network attacks	Cost of book/manual
			4)	Install software for monitoring of network traffic	Early discovering and preventing of network problems – better protection against possible network attack	Cost of work time of user (installation) and cost of software
		c)	1)	Daily full data and system backup	Higher availability of operating system, application programs and data –reduction of network attack consequence	Cost of work time of user (backup) and cost of backup software and hardware
			2)	Install OS, application programs and antivirus software on additional work station	Use of additional work station in case of denial of functionality of the main work station	Cost of additional work station and cost of work time of user (installation)
			3)	Regular tests of OS and application programs installed on additional work station	Insure possibility for use of additional work station in case of denial of functionality of the main work station	Cost of work station, installation of OS and application programs (work hours) and cost of tests
			4)			
		d)	1)	Have an insurance that covers the financial consequences of network attack	Reduction of financial consequences of network attack	Cost of insurance
			2)			
			3)			
			4)			
		e)	1)			
			2)			
			3)			
			4)			

D.5.2 Activity 5.2: Specification of risk treatment priorities

Objective	Define priority among risk treatment actions

The PDA user and the system owner assigned costs and benefits for treatment actions according to the following scale: “very low” (VL), “low” (L), “moderate” (M), “high” (H), “very high” (VH). Treatment actions priorities were identified with the help of the Risk treatment action priority matrix (Table D.1.5). Both the PDA user and the chat system owner assigned costs to the treatment actions according to the scale shown in Table D.5.6. To define the cost value, the total monthly income of the system owner/PDA user was compared to the cost of treatment action.

Table D.5.6: Cost values scale

	Cost of treatment action				
	Very low	Low	Moderate	High	Very high
Cost of treatment action compared to the total income of the system owner/PDA user	0 – 1%	1 – 3%	3 – 6%	6 – 10%	> 10% more than 10%

The identified priorities of treatment actions are documented in the treatment priorities tables shown below.

Table D.5.7: Chat Service Treatment priority table for host operating system availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit (PDA)	Benefit (chat)	Cost (PDA)	Cost (chat)	Treatment action priority (PDA)	Treatment action priority (chat)
	Denial of operating system functionality	a)	1)							
			2)							
			3)							
			4)							
		b)	1)	Operating system must be kept updated	High	High	Low	Very low	High	Very high
			2)	Upgrade to the more reliable version of OS	Mode rate	High	High	Low	Low	High
			3)	Regular tests of operating system	Low	Mode rate	Mode rate	Low	Low	Moderate
			4)	Install software for monitoring of operating system functionality	Low	Mode rate	Mode rate	Mode rate	Low	Moderate
		c)	1)	Daily full data and system backup	Mode rate	High	Low	Low	Moderate	High
				Have compact discs with operating system, diagnostic and recovery tools available	Mode rate	High	Very low	Very low	High	Very high
			2)	Install OS and application programs on additional work station	N/A	High	N/A	High	N/A	Moderate
			3)	Regular tests of OS installed on additional work station	N/A	Mode rate	N/A	High	N/A	Low
			4)	Install software on additional work station for monitoring of operating system functionality	N/A	Mode rate	N/A	High	N/A	Low
		d)	1)	Have an insurance that covers the financial consequences of denial of operating system functionality	Low	Mode rate	Very high	Very high	Low	Low
			2)							
			3)							
			4)							
		e)	1)							
			2)							
			3)							
			4)							

	Denial of operating system authorization functionality	**a)**	**1)**						
			2)						
			3)						
			4)						
		b)	**1)**	Introduce the strict rules for choosing and changing of password	High	High	Very low	Very low	Very high	Very high
				Use the screensaver with password protection	High	High	Very low	Very low	Very high	Very high
				Users should always logout whenever they leave computer for any period of time	High	High	Very low	Very low	Very high	Very high
			2)							
			3)	Regular update and tests of employees/users security awareness	Mode rate	High	Low	Low	Moderate	High
			4)							
		c)	**1)**	Recovery from operating system problems should be done only by a specialized company (technical support)	Mode rate	High	Mode rate	Low	Moderate	High
			2)							
			3)							
			4)							
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to operating system	Low	Mode rate	Very high	Very high	Very low	Low
			2)							
			3)							
			4)							
		e)	**1)**							
			2)							
			3)							
			4)							

	Incorrect installation and use of operating system	**a)**	**1)**							
			2)							
			3)							
			4)							
		b)	**1)**	The competence of personnel responsible for use/installation of OS should be updated regularly (regular training courses)	High	Very high	Mode rate	Low	High	Very high
			2)	Help in installation and use of OS from a software support service	Mode rate	High	Mode rate	High	Moderate	Moderate
			3)	Self study of user manual/text book and self testing of knowledge	Low	Mode rate	Low	Mode rate	Low	Moderate
			4)							
		c)	**1)**	Use software support service for recovery from OS problems	Mode rate	High	Mode rate	High	Moderate	Moderate
			2)	Have a backup competent user available	Mode rate	Low	High	High	Low	Very low
			3)							
			4)							
		d)	**1)**	Have an insurance that covers the financial consequences of incorrect use of OS	Low	Mode rate	Very high	Very high	Low	Low
			2)							
			3)							
			4)							
		e)	**1)**							
			2)							
			3)							
			4)							

Table D.5.8: Chat Service Treatment priority table for host hardware availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit (PDA)	Benefit (chat)	Cost (PDA)	Cost (chat)	Treatment action priority (PDA)	Treatment action priority (chat)
	Denial of hardware component functionality	**a)**	**1)**							
			2)							
			3)							
			4)							
		b)	**1)**							
			2)	Install another more reliable hardware component	Mode rate	High	Mode rate	Mode rate	Moderate	High
			3)	Regular tests of hardware component	Low	Mode rate	Low	Low	Moderate	Moderate
			4)	Install software for monitoring of hardware component functionality	N/A	Mode rate	N/A	Mode rate	N/A	Moderate
		c)	**1)**	Have an additional hardware component available	High	Very high	Mode rate	Low	High	Very high
			2)	Install an additional hardware component with the same functionality	N/A	Very high	N/A	Mode rate	N/A	High
			3)	Regular tests of additional hardware component functionality	N/A	Low	N/A	Low	N/A	Low
			4)	Install software for monitoring of additional hardware component functionality	N/A	Low	N/A	Mode rate	N/A	Low
		d)	**1)**	Have an insurance that covers the financial consequences of denial of basic hardware component functionality	Low	Mode rate	Very high	Very high	Very low	Low
			2)							
			3)							
			4)							
		e)	**1)**							
			2)							
			3)							
			4)							

	Denial of hardware component authorization functionality	**a)**	**1)**							
			2)							
			3)							
			4)							
		b)	**1)**	Provide regular security awareness training of employees who use/install hardware components	High	High	Very low	Very low	Very high	Very high
			2)							
			3)	Regular update and tests of security personal competence	N/A	High	N/A	Low	N/A	High
			4)	Install software for monitoring and detection of access to the room/area where HC is installed	N/A	Mode rate	N/A	Mode rate	N/A	Moderate
		c)	**1)**	Recovery from hardware problems should be done only by a specialized company (technical support)	Mode rate	High	Mode rate	Mode rate	Moderate	High
			2)							
			3)							
			4)							
		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to hardware component	Low	Mode rate	Very high	Very high	Very low	Low
			2)							
			3)							
			4)							
		e)	**1)**							
			2)							
			3)							
			4)							

	Incorrect installation and use of hardware	**a)**	**1)**							
			2)							
			3)							
			4)							
		b)	**1)**	The competence of personnel responsible for use/installation of hardware components should be updated regularly	High	Very high	Mode rate	Low	High	Very high
			2)	Help in installation and use of hardware component from a hardware support service	Mode rate	High	Mode rate	High	Moderate	Moderate
			3)	Self study of user manual/text book and self testing of knowledge	Low	Mode rate	Low	Mode rate	Low	Moderate
				Use of interactive teaching program with tests of knowledge	Low	Mode rate	Low	Mode rate	Low	Moderate
			4)							
		c)	**1)**	Use hardware support service	Mode rate	High	Mode rate	High	Moderate	Moderate
			2)	Have a backup competent user available	Mode rate	Low	High	High	Low	Very low
			3)							
			4)							
		d)	**1)**	Have an insurance that covers the financial consequences of incorrect use of hardware component	Low	Mode rate	Very high	Very high	Low	Low
			2)							
			3)							
			4)							
		e)	**1)**							
			2)							
			3)							
			4)							

Table D.5.9: Chat Service Treatment priority table for host authorization availability risks

ID	Risk	Approach	Treatment option	Treatment action	Benefit (PDA)	Benefit (chat)	Cost (PDA)	Cost (chat)	Treatment action priority (PDA)	Treatment action priority (chat)
	Denial of Host authorization availability	**a)**	**1)**							
			2)							
			3)							
			4)							
		b)	**1)**	Host node should be fastened with screws to a wall, floor or table and physical access to the host node should be secured with a lock	N/A	High	N/A	Very low	N/A	Very high
				Access to the room where host node is installed should be protected by door with a lock	N/A	High	N/A	Very low	N/A	Very high
			2)	Install host node in an other room/area with more strong access control	N/A	Mode rate	N/A	Mode rate	N/A	Moderate
			3)	Self study of user manual/text book about host security and self testing of knowledge	High	High	Very low	Very low	Very high	Very high
			4)	Install software for monitoring and detection of access to the room/area where host node is installed	N/A	Mode rate	N/A	Mode rate	N/A	Moderate
		c)	**1)**	Have an additional host node with installed operating system and application programs available	High	High	Very high	High	Moderate	Moderate
			2)	Install and fasten with screws an additional host node with installed OS and application programs in another room with more strong access control	N/A	High	N/A	High	N/A	Moderate
			3)	Test regularly (monthly) the functionality of OS and application programs installed on additional host node	N/A	Mode rate	N/A	Mode rate	N/A	Moderate
			4)	Install software for monitoring and detection of access to the room/area where additional host node is installed	N/A	Mode rate	N/A	Mode rate	N/A	Moderate

		d)	**1)**	Have an insurance that covers the financial consequences of unauthorized access to host node	High	High	Very high	Very high	Moderate	Moderate
			2)							
			3)							
			4)							
		e)	**1)**							
			2)							
			3)							
			4)							

Table D.5.10: Chat Service Treatment priority table for host security service availability risks (antivirus software)

ID	Risk	Approach	Treatment option	Treatment action	Benefit (PDA)	Benefit (chat)	Cost (PDA)	Cost (chat)	Treatment action priority (PDA)	Treatment action priority (chat)
	Lack of antivirus software/ virus attack	**a)**	**1)**							
			2)							
			3)							
			4)							
		b)	**1)**	Attachments from unknown sources should not be opened	High	High	Very low	Very low	Very high	Very high
				Compact disks and diskettes should be virus checked before they can be used	High	High	Very low	Very low	Very high	Very high
				Antivirus software should be regularly updated	High	High	Very low	Very low	Very high	Very high
			2)	Install antivirus software	Very high	N/A	Low	N/A	Very high	N/A
			3)	Self study of user manual/text book about host security and self testing of knowledge	High	High	Low	Low	High	High
			4)							
		c)	**1)**	Recovery from a virus attack should be done by specialized company (technical support)	High	High	Low	Low	High	High
			2)	Install OS, application programs and antivirus software on additional work station	N/A	High	N/A	High	N/A	Moderate
			3)	Regular tests of OS and application programs installed on additional work station	N/A	Mode rate	N/A	High	N/A	Low
			4)							
		d)	**1)**	Have an insurance that covers the financial consequences of virus attack	Low	Mode rate	Very high	Very high	Very low	Low
			2)							
			3)							
			4)							
		e)	**1)**							
			2)							
			3)							
			4)							

Table D.5.11: Chat Service Treatment priority table for host security service availability risks (firewall)

ID	Risk	Approach	Treatment option	Treatment action	Benefit (PDA)	Benefit (chat)	Cost (PDA)	Cost (chat)	Treatment action priority (PDA)	Treatment action priority (chat)
	Lack of firewall/ attack from the network	**a)**	**1)**	Remove connection from the Internet	N/A	N/A	N/A	N/A	N/A	N/A
			2)							
			3)							
			4)							
		b)	**1)**	Firewall should be regularly updated	N/A	High	N/A	Very low	N/A	Very high
			2)	Install firewall	Very high	N/A	Low	N/A	Very high	N/A
			3)	Self study of user manual/text book about host security and self testing of knowledge	Mode rate	Mode rate	Low	Low	Moderate	Moderate
			4)	Install software for monitoring of network traffic	N/A	Mode rate	N/A	Mode rate	N/A	Moderate
		c)	**1)**	Daily full data and system backup	High	High	Low	Very low	High	Very high
			2)	Install OS, application programs and antivirus software on additional work station	N/A	High	N/A	High	N/A	Moderate
			3)	Regular tests of OS and application programs installed on additional work station	N/A	Mode rate	N/A	High	N/A	Low
			4)							
		d)	**1)**	Have an insurance that covers the financial consequences of network attack	Low	Mode rate	Very high	Very high	Very low	Low
			2)							
			3)							
			4)							
		e)	**1)**							
			2)							
			3)							
			4)							

D.6 Summary of main conclusions

The availability risk assessment has covered the following functionality of the chat service:

- The authentication control of users
- The chat service functionality
- The wireless access to the chat service

The goal of this availability risk assessment has been to identify and analyse risks that represent a risk towards availability for the above-mentioned functionality of the chat service.

In order to focus on the most important risks, the stakeholders along with the assets that are of value for them were identified. Table D.6.1 shows the stakeholders and the assets that were identified in the availability risk assessment of the chat service.

Table D.6.1: The stakeholders along with the assets

Stakeholder	Asset Category	Asset	Description	Value
System owner	Organizational	Availability of service	The highly available service is one of the main sources of income for the system owner	30000$ per month
PDA user	Organizational	Availability of service	The PDA user pays 1$ for each hour of service usage	1$ for 1 hour of service usage

Twenty-four risks were identified. Further analysis of these risks resulted in the identification of nine risks with risk level “Moderate”, fourteen risks with risk level “Low” and one risk with risk level “No risk”. All risks with risk level “Moderate” were organised into the following five risk treatment categories:

- Host operating system availability risks
- Host hardware availability risks
- Host authorization availability risks
- Host security service availability risks (firewall)
- Host security service availability risks (antivirus software)

The management of the chat service should consider carefully whether the chat service might be continued/used if sufficient treatment of risks with risk level “Moderate” is not implemented. In order to achieve an acceptable risk level for the chat service, we recommend implementing a treatment that reduces the risk level of the risks with risk level “Moderate” to risk level “Low”. Figure D.6.2 summarizes the treatment proposals of priority “Very high” that will reduce the risk level of the relevant risks in an adequate manner.

Table D.6.2: The summary of the treatment proposals of priority "Very high"

Risk	Treatment action
Denial of host operating system availability	• Operating system must be kept updated • Have compact discs with operating system, diagnostic and recovery tools available • Introduce the strict rules for choosing and changing of password • Use the screensaver with password protection • Users should always logout whenever they leave computer for any period of time • The competence of personnel responsible for use/installation of operating system should be updated regularly (regular training courses)
Denial of host hardware availability	• Have an additional hardware component available • Provide regular security awareness training of employees who use/install hardware components • The competence of personnel responsible for use/installation of hardware components should be updated regularly
Denial of host authorization availability	• Host node should be fastened with screws to a wall, floor or table and physical access to the host node should be secured with a lock • Access to the room where the host node is installed should be protected by door with a lock • Self study of user manual/text book about host security and self testing of knowledge
Lack of antivirus software/virus attack	• Install antivirus software • Attachments from unknown sources should not be opened • Compact disks and diskettes should be virus checked before they can be used • Antivirus software should be updated regularly
Lack of firewall/attack from the network	• Install firewall • Firewall should be updated regularly • Daily full data and system backup