CHALMERS

Business Impact Analysis (BIA) process for Siemens Industrial Turbomachinery AB

Development of an asset-based, cost-efficient and time-efficient Business Impact Analysis process which also encompasses a risk assessment methodology, for Siemens SIT

Master of Science Thesis in Secure and Dependable Computer Systems

ALIREZA TAMADONI

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
Göteborg, Sweden, February 2015

The Author grants to Chalmers University of Technology and University of Gothenburg the non-exclusive right to publish the Work electronically and in a non-commercial purpose make it accessible on the Internet.
The Author warrants that he/she is the author to the Work, and warrants that the Work does not contain text, pictures or other material that violates copyright law.

The Author shall, when transferring the rights of the Work to a third party (for example a publisher or a company), acknowledge the third party about this agreement. If the Author has signed a copyright agreement with a third party regarding the Work, the Author warrants hereby that he/she has obtained any necessary permission from this third party to let Chalmers University of Technology and University of Gothenburg store the Work electronically and make it accessible on the Internet.

Business Impact Analysis (BIA) process for Siemens Industrial Turbomachinery AB

Development of an asset-based, cost-efficient and time-efficient Business Impact Analysis process which also encompasses a risk assessment methodology, for Siemens SIT

Alireza Tamadoni

© Alireza Tamadoni, February 2015.

Examiner: Professor Erland Jonsson

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
Göteborg, Sweden February 2015

Abstract

The threats encountered by companies and organizations must be dealt with in order to secure their survivability. This is especially important as the survivability of society and its economic infrastructure depends on companies and organizations continuing their business operations. As a result, Business Continuity Planning (BCP) has proliferated by the years in order to reduce the risks of potentially damaging and disruptive events. The rapid proliferation of BCP has contributed to different standards used by different companies and different organizations worldwide. The wide variety of standards and the lack of an international standard leads to difficulties when determining which methodologies to use for performing BCP.

This project presents a process for performing a Business Impact Analysis (BIA) which is an essential part of BCP. The process is tailored for Siemens Industrial Turbomachinery (SIT) AB. From SIT's point of view, a BIA should provide a decision basis. This would enable management to justify and perform pre-cautionary measures to hinder potential damages on business. In order to meet the demands from the management of SIT, the process was built from scratch based on a comprehensive literature study and reviewing existing material from SIT and the Siemens Corporation. Bits and pieces from different methodologies were reviewed and used when appropriate. One demand was to develop a process that is both cost-efficient and time-efficient. As a result, the process was built based on the company's resource assets instead of on its complex business processes. In order to gather the information needed about these assets and to determine which assets are critical for the company, a customized method on how to gather data was developed. The method suggested an integrated solution in which the data gathering process would integrate with an existing web-based information security survey system. The method, and consequently the questions involved in the developed questionnaire were to the largest possible extent validated by performing a number of interviews with managers within the different business divisions. Furthermore, the methods driving the BIA process were developed based on the concepts of confidentiality, integrity and availability so that threat-scenarios and potential financial impact losses could be derived in a structured and systematic manner. Consequently, it is possible to estimate the risks involved in order to derive decision basis for pre-cautionary measures. A decision could be to reduce a risk, plan or manage the risk or simply to accept the risk. In most of the parts of the process, tools were created in Microsoft Excel Sheets. This simplifies the description of the process within this report. It also to simplifies the actual execution of a BIA, for the management of SIT.

Preface

This report constitutes the final activity for the degree of Master of Science in the Secure and dependable computer systems program at Chalmers University of Technology in Göteborg. The Master's thesis covers 30 higher education points and has been performed at, Siemens Industrial Turbomachinery AB in Finspång, Sweden.

The work in the project was carried out in 2009 within the Master's program Secure and Dependable Systems (MPDCS), but for various reasons the report was not finalized until 2015. The MPDCS program has since been replaced by the Master's program in Computer Systems and Networks (MPCSN).

I would like to thank some people that have reached out with a helping hand during the project:

My supervisor Göran Hellström, at SIT and supervisor Erland Jonsson, at Chalmers for their invaluable support, patience and dedication throughout the project has contributed with valuable input and discussions.

The managers at SIT that have offered their valuable time for interviews and meetings have contributed with valuable data and information for the project.

And finally, to my family and friends for their constant support and patience with the project, has been equally valuable.

Göteborg, February, 2015

Alireza Tamadoni

Abbreviations

AB	Aktiebolag
BCP	Business Continuity Planning
BIA	Business Impact Analysis
CA	Critical Asset
CIA	Central Intelligence Agency
CIO	Corporate Information Office
DA	Deficiency Analysis
DRJ	Disaster Recovery Journal
EBIT	Earnings Before Interest and Taxes
FDT	Forecast Data Table
IEC	International Electrotechnical Commission
IRAM	Information Risk Analysis Methodologies
ISF	Information Security Forum
ISO	International Organization for Standardization
IT	Information Technology
LC	Lower Confidence
LT	Line-item Threshold
MSEK	Million Swedish Crowns
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
PCM	Preventive Crisis Management
PM	Planning Materiality
RTO	Recovery-Time Objective
SIT	Siemens Industrial Turbomachinery
SOA/SOX	Sarbanes-Oxley Act
WEP	Words of Estimative Probability

Table of contents

1 Introduction

1.1 Background

Siemens Industrial Turbomachinery AB delivers gas turbines, steam turbines, turn-key power plants, service and components for heat and power production. Everything is performed under one roof, from research and development, manufacturing, marketing, sales and installation of turbines and complete power plants to service and refurbishing. The company employs about 2300 people in Finspång and another 100 in Trollhättan. On top of that, the company has temporarily employed personnel and consultants. In total, the company consists of nearly 2800 people. SIT belongs to the Siemens Group which has 460 000 employees in 190 countries [*1*].

In today's world, society is faced with different kind of threats. Among others, information security threats, extreme weather, espionage and sabotage are just some of the many possible threats that can bring a company to its knees. If a company fails to function, other companies may become affected as a consequence which in turn affects other companies. It is therefore extremely crucial for companies and organizations to secure their survival capabilities, not only for commercial reasons, but also for the sake of society and its economic infrastructure [*2*]. To complicate matters even more, the worst kind of threats today, exist within the organization, namely employees or externally hired personnel [*3*]. As a result of the threats facing today's companies and organizations, the following statement was made by Krisberedskapsmyndigheten,

> *"It is important that companies' plan to strengthen their abilities to continue operations in case of all types of interferences and events. Also, critical processes should be restarted for the companies, within a tolerable space of time."* [*2*]

To address these threats and to secure companies' survival, **Business Continuity Planning** (BCP) has proliferated by the years [*4*]. The main purpose of a BCP is to develop plans and creating the framework to secure the continuity of a business in case of an emergency. In other words, preparing, testing and updating actions required to protect critical business processes from the effects of disruptions and failure events. When creating a BCP, the company has to initially perform a **Business Impact Analysis** (also referred to as Business Impact Assessment). The purpose of the BIA is to understand the potential impacts of disruptive events by performing a **vulnerability assessment** and by doing so, providing decision basis which is then used as a foundation to create a **Disaster Recovery Plan** [*5,6*].

1.1.1 Current situation at SIT

As of now, SIT has an unclear process for a BIA which is meant to analyze different areas such as human resources, facility, information technology, supplies, paper documentation and workshop (machinery). At the same time, in parallel there exists a special IT BIA which should be reported to the IT Crisis Manager [*1*]. The IT BIA only analyzes applications and information systems, in contrast to the BIA which is meant to analyze all other resources.

Tasks related to BCP, are included in one of SIT's support processes called Preventive IT Crisis Management (PCM) which is meant to perform all BCP related activities, such as performing a BIA yearly.

The following figure (*Figure 1*), presents the PCM process flow (the figure is a simplified version of the original process flow) according to SIT's process views.

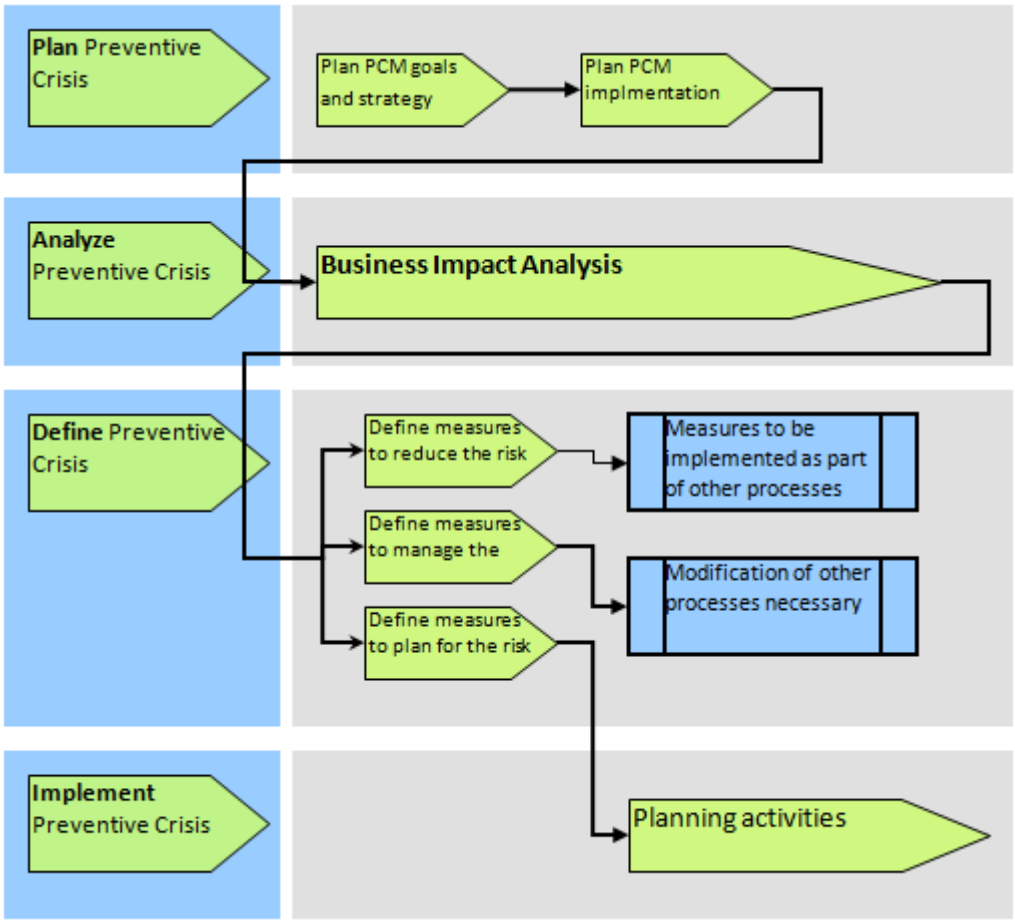


Figure 1. The figure describes the process flow for the support process Preventive IT Crisis Management (corresponds to SIT's BCP process). As one can observe, the BIA is performed in the analysis stage. The steps within the BIA are not visible in the figure. The BIA outputs potential pre-cautionary measures that need to be taken in the definition stage (it is part of alternative planning which corresponds to the general term Disaster Recovery Planning **[6]***).*

The current BIA process is done as a best-effort approach. Managers from different divisions are invited to meetings that sometimes go on for hours without these meetings being productive. Discussions include what kind of assets that exist, that needs to be protected and historical incidents in the company. Some of the problems in these meetings are the lack of a common terminology and also the level of detail in the discussions. Some managers want to discuss details on a high level and some on a low level. The results from those meetings are then summarized in a simple excel worksheet and is used as the result of the BIA.

One requirement that is clear with the current BIA process, is the desired strategy of the resulting risk analysis (see *Figure 31*).

1.1.2 Lack of an international standard

There exists no international standard for performing Business Continuity Planning. Consequently, no uniform terminology exists. What is common between the different models is the comprehensive view on BCP as a process with focus on critical business units. A technical committee (ISO/TC223) within ISO is currently developing what is meant to become a comprehensive standard practice for performing BCP [*2*].
The following table contains different BCP standards and practices:

Table 1. The presents some BCP related standards and methodologies that are available. On the left are the countries or organization utilizing, supporting and encouraging each respective standard or methodology (included on the right column). Information included in the table is partly taken from **[2]**.

United Kingdom	BS 25999-1 Code of practice for business continuity management (replacing PAS56 which is used within the Siemens enterprise).
United States of America	NFPA 1600 Standard Disaster/Emergency Management and Business Continuity Programs.
Australia	AS/NZS HB221:2004 Business Continuity Management.
Singapore	TR19:2995 Business Continuity Management.
ISO/IEC 17799:2005	Information Technology – security techniques – code of practice for information security management.
Jointly developed by the Disaster Recovery Journal (DRJ) and the Disaster Recovery Institute International (DRI)	Generally Accepted Business Continuity Practices
Information Security Forum	Information Risk Analysis Methodologies (IRAM) project: Business Impact Assessment.

1.2 Aim and purpose

The primary purpose and goal of this thesis project is to develop a uniform and thorough process for the Business Impact Analysis. The process should be fully or partly usable as a foundation for performing a Business Impact Analysis at SIT. The following requirements apply:

- The process must provide an appropriate level of granularity, such that it is usable with respect to SIT's business culture and complexity.
- The process should be able to provide methods for identifying assets that are critical for SIT and financial loss impacts of potential disruptive events and

potential damaging events with respect to confidentiality, integrity and availability.
- The process should hinder doubt and ambiguity regarding relevant BCP terms and definitions for the personnel involved in performing the BIA.
- The process should encompass a threat assessment method, usable to bind assets to threats with similar themes and provide a systematic approach for analyzing threat scenarios based on confidentiality, integrity and availability.
- The process should encompass methods on how to determine necessary risk mitigation strategies with respect to SIT's Preventive Crisis Management process.
- The process should be optimized with respect to cost and time.

1.3 Limitations

The Business Impact analysis is performed as a process-based methodology. The goal is to identify the most important processes that are critical for survival. The problem with such a methodology is the time and resources needed for larger corporations because of their immense business complexity. Obviously, a thorough analysis of each process and all assets would provide a robust foundation for when performing pre-cautionary measures in order to protect the processes and the assets. Still, it would require a large amount of time and resources, and ultimately it is money companies want to save. Why spend money on pre-cautionary measures if they cost more to implement than the actual potential damage or disruptive event threatening the business?

One requirement for the thesis project is to derive a time-efficient and cost-optimized process that can be performed with an appropriate level of granularity with respect to SIT's business culture. Developing a BIA process based on the business processes has been determined as infeasible because of the business complexity. Also, previous attempts within SIT has been unsuccessful in doing so. Furthermore, analyzing the processes would require a type of "process-application-landscape" analysis [*7*], which would force the granularity of the analysis work to an inappropriate (low) level. As a result, the BIA process will not be developed based on SIT's critical business processes (at least not as the starting point).

Additionally, a BIA involves calculating or estimating financial impact losses. An additional limitation is the development of precise financial methods related to calculating (or estimating) financial impact losses, which will not be included. These types of calculations or estimations with respect to the BIA demands business expert knowledge and are consequently outside the scope of this project. However, the process will provide some type of indicators on how to start the process to estimate these losses.

1.4 Method

The project was divided into three phases, phase I, phase II and phase III. Phase I consisted of pre-studies which encompassed theoretical knowledge gathered from books, electronic journals, publications and information from search engines. Development of a project plan, administrative work and looking at some of the SIT material related to this project was also done.

Phase II included reviewing all current and existing work related to Siemens BCP material, such as existing methodologies used in different Siemens corporate areas, the last performed BIA within SIT. A BIA process framework was derived, although a lot was changed and evolved with time. Questionnaires were developed and

information on potential interview candidates was analyzed. Phase III included performing interviews, compiling the gathered data and writing the final report. A questionnaire was created and used in the interviews. The aim with the interviews was to gather the data needed but also to validate the questionnaire and to get feedback on the questions. The questionnaire could then be used to gather data quantitively in the future. The compiling of data was done by creating excel sheets with simpler macro scripts to automate the summarizing process.

1.5 Report setup

Chapter 1 provides background information, describing BCP and consequently the use of BIA. A brief overview of the current situation at SIT with respect to the BCP process was described. The purpose, limitations and method are also included.

Chapter 2 provides with an overview and definitions of the BIA process developed in this thesis project. Definitions and terms related to the execution of the BIA process in chapter 3 have been described in order to support and simplify the different parts of the process. The chapter exists as a support chapter, which the audience is recommended to consult whenever necessary.

Chapter 3 describes the BIA process. The interviews conducted, the threat assessment and the risk analysis are clarified and discussed. The different methods used are clarified with the help of simpler developed excel macro scripts.

Chapter 4 describes the overall results, proposals and discussions for future work related to the subject of the thesis.

Appendix A contains the created questionnaire to identify critical assets, operations and impacts. The chapter also contains help documentation to assist respondents fill in the questionnaire.

Appendix B describes threat profile trees derived using OCTAVE, as described in chapter 3.7.1 Identifying threat-scenarios using OCTAVE.

Appendix C contains a summary of all threat scenarios derived.

2 Overview of the BIA process and definitions

The BIA process consists of several parts. This chapter will supplement the main execution of the BIA with definitions and overviews. The purpose is to define a common ground for terminology and prior knowledge.

2.1 Presentation of the BIA process

The core parts of the BIA process are presented in *Figure 2* below.

Figure 2. The figure presents the core parts of the developed BIA process. These parts consists of assessing which assets that are critical for the company and estimating how much damage that could occur in lost earnings for the company (impacts), and assessing the probabilities of threats occurring and the extent of damage that could occur (vulnerabilities) based on these threats. These parts are crucial in order to perform a risk analysis which decides the appropriate pre-cautionary measure needed to be taken.

The result of the BIA is aimed at providing decision basis for performing pre-cautionary measures in order to mitigate the risks of different types of threat scenarios, which could potentially cause damage to SIT. The pre-cautionary measures to be performed are based on the level of risk (decision basis) involved and should be performed accordingly. In order to determine the level of risk involved, risk levels must be estimated by looking at the companies' most critical assets and determining the amount of damage to business they could cause if they were to be destroyed, lost, stolen, interrupted etc. Furthermore, the probability of different types of threats must be scrutinized, meaning to analyze the probability of potential threats occurring and analyzing how vulnerable critical assets are with respect to the threats. The BIA is in other words a kind of vulnerability assessment in order to derive decision basis for costly threat events. However, *Figure 2* does not present every aspect of the BIA process. In order to determine and analyze SIT's critical assets, one must be able to gather information in order to determine which asset's that are critical and which that are not critical. There is also the need to determine which threats that should be analyzed and which that simply do not need to be accounted for, in order to create a reasonable scope for performing a BIA. These parts have been developed and included in the process. However, they could be seen as belonging to the outer shell of the process, existing to support the core parts.

2.1 BIA process preparation

In order to avoid unnecessary discussions about terms, abbreviations and definitions, this section will define the scope and context of the BIA process. It is recommended to consult chapter 2 for when performing the vulnerability assessment in chapter 3.

2.1.1 Deliverables of the BIA

The main purpose of the BIA is to create a document to be used to help understand potential future business impact of potential disruptive events [*6*] and potential damaging events on the business. These impacts are assessed with respect to certain assets, defined within this process as critical assets (CA). These impacts together with probabilities of threats provide the level of risk involved. The management of SIT can use this information, such that being able to take the necessary pre-cautionary steps in order to avoid costly damages. The category of an impact type can be of one of the following:

- Financial impacts (for example loss of sales and orders).
- Operational impact (for example loss of competitiveness).
- Customer-related impacts (for example delayed deliveries to customers).
- Employee related impacts (for example reduction in staff morale).

Each category contains a number of impact-types, which are available in Appendix A. These impacts could be measured differently based on the type. For example, within the financial category there is "Loss of sales, orders or contracts" which could be measured in "% of sales opportunities missed". However, within SIT impacts are solely to be measured financially. The following is a definition for the term impact within this process.

Definition of ***impact***: An impact is the financial loss occurred as the consequence of some damaging event or disruptive event.

2.1.2 Concepts of confidentiality, integrity and availability

This BIA process is driven by the concepts of confidentiality, integrity and availability (C.I.A.). The reason is that basically everything within information security; information security controls, safeguards, threats and security processes are subject to the C.I.A triad (see *Figure 3*) [*6*]. The use of these concepts provides a structured process such that critical assets can be analyzed and sorted based on their security requirements, financial losses can be estimated in an objective and considered manner [*8*] and threats can more easily be identified and connected to critical assets based on each critical asset's security requirements.

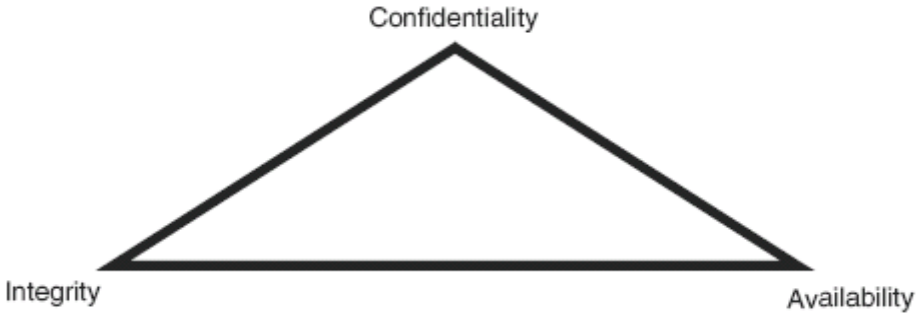


Figure 3. The C.I.A triad, taken from **[6]**. *These concepts are three very important principles with respect to information security* **[6]**.

Confidentiality ensures the prevention of intentional or unintentional disclosure of information or data to unauthorized parties. Loss of confidentiality (damaging event) can occur through the intentional (malicious) disclosure or theft of data and information. It can also occur accidently by well intentioned and authorized personnel. Analysis of loss of confidentiality is limited to assets definable as *Critical Assets*.

Integrity ensures the prevention of unauthorized modification of data or information. Loss of integrity (damaging event) can occur through intentional and malicious modification. It can also occur accidently by well intentioned and authorized personnel. Analysis of loss of integrity is limited to assets definable as *Critical Assets*.

Availability ensures reliable and timely operational status of an *Operation (O)* dependent on some critical assets. Loss of availability (disruptive event) can occur by some intentional (malicious) event, unintentional (accidental) event or random (natural) event. Within this threat assessment, the destruction of an *Operation (O)'s* services, resources or information is regarded as loss of availability if its operational status is halted to some extent or fully with respect to time and/or reliability of delivery. Analysis of loss of availability is limited to assets definable as *Critical Assets*.

Destruction (implies loss of availability) can occur by some intentional event (malicious), unintentional (accidental) event or random event (natural). Destruction loss is included to supplement the above loss concepts.

Note: At the time of writing this report, the current requirement for the BIA at Siemens SIT only encompasses the concept of availability, meaning disruptive events.

2.1.3 Definition of Critical Assets and Operations (O)

The aim for this process is to encompass all kinds of resources as possible critical assets. It is not limited to just information systems, data and applications. Additional possible resources are for example heavy machinery and personnel. The following definition is used throughout the BIA process.

Definition of ***Critical Assets (CA)*** – An asset can be regarded as a Critical Asset if having at least one of the following properties:

1. For **confidentiality**: Contains information or data classified as confidential, strictly confidential according to Siemens SIT security classification system and/or could in some way damage Siemens SIT if disclosed.
2. For **integrity**: Contains information or data with the requirement of it being internally and externally consistent. The information is consistent among all sub-entities and consistent with the real world. [CISSP]
3. For **availability**: Provides services, resources or information **belonging to *Operations (O)***. A CA is necessary for one or several *Operations (O)* continuance and normal functioning.

The overall criticality of the asset must at least be determined as significant as described in chapter 3.4.

The following list contains examples of possible properties belonging to CA's.

- The CA has been classified with a higher level of security classification (the asset is confidential).
- The CA will damage Siemens SIT if published without authorization.
- Competitors or other third-parties could benefit financially if acquiring the CA (confidentiality is lost).
- Customers would be affected negatively if the CA became inaccessible, destroyed, lost etc (availability is lost).

CA's will be explained more thoroughly in chapter 3.3.

As mentioned earlier the Business Impact Analysis is usually based on gathered knowledge about business critical processes [*7*,*9*,*10*], but the complexity of these processes at SIT are such that basing the analysis on them is not feasible with respect to time and cost. Instead, the BIA and consequently the threat assessment will focus on Critical Assets with respect to certain business operation activities, processes or sub-processes within each department and business division. The business divisions are the following.

- The service division.
- The steam turbine division.
- The gas turbine division.
- The oil and gas division.

Deciding what constitutes a business operation activity will not be done. The reason is that almost every type of activity within the organization can be regarded as a business operation activity, at least to some extent. What are interesting are those activities within each division, which directly enables each respective division to function in order to support SIT's business goals. In some cases several processes regarded as core processes in a department or division altogether can be regarded as one Operation. In

other cases one or two processes might be considered as separate Operations. The following is the definition of such activities.

Definition of ***Operations (O)***: A process, sub-process or business operation activity within one of the four business divisions. The activity is crucial to such an extent that if it failed to function (**this definition only encompasses loss of availability**), could potentially cause noticeable or severe negative impact to the business goals of the division and consequently, Siemens SIT's business goals. Example of properties belonging to Operations *(O):*

- Key process, sub-process or business operation activity directly supporting continuance of production.
- Key process, sub-process or business operation activity directly supporting continuance when making deliveries.
- Key process, sub-process or business operation activity directly supporting continuance of processing orders.
- Key process, sub-process or business operation activity directly supporting continuance of research and development.
- Key process, sub-process or business operation activity directly supporting continuance of customer support.

The following figure (*Figure 4*), presents the relation between critical assets and operations.

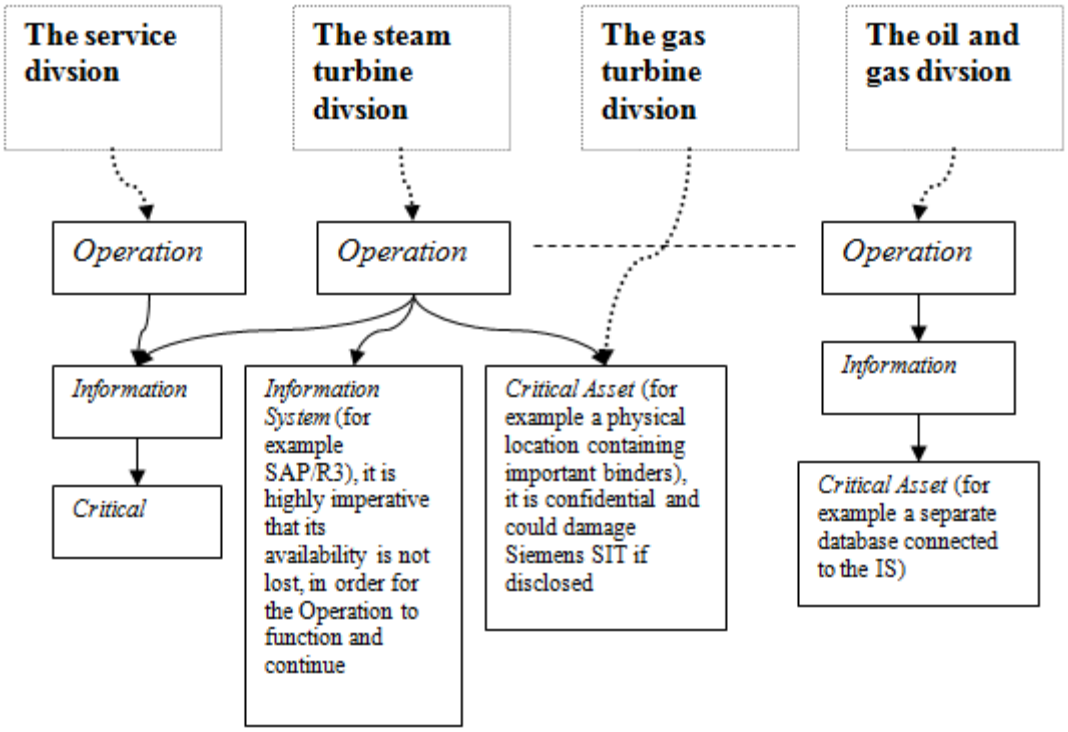


Figure 4. The figure visually describes the definitions of Operations (O) and Critical Assets (CA). If a branch contains an Operation then the Critical Asset following that branch is imperative with respect to at least availability for the corresponding Operation. If a branch lacks an Operation then that Critical Asset is imperative with respect to confidentiality and/or integrity. In other words, a Critical Asset should only be given the availability security requirement if dependent by some or several Operations (O).

2.2 Defining criticality criteria

In order for the BIA to achieve its functionality with respect to identifying impacts and being able to somehow grade these impacts in order to understand the criticality of them, it is necessary to proceed as follows [*9*]:

1. Establishing a **definition for criticality**, using a single level or multiple levels for criticality, i.e. should a common level be set for the entire SIT or should individual levels be set for each business division?
2. Depending on if we use a **single level** or **multiple levels**, establishing or identifying a method on how to derive a maximum threshold value for impacts. In other words, the maximum tolerable loss in earnings before interest and taxes (EBIT) for the entire SIT or for each individual business division.
3. Based on the maximum threshold value. The scales low, medium and high (with high constituting as the maximum threshold level) are used.

2.2.1 Definition for criticality of business impacts

It has been found appropriate to use a single level for defining the criticality of impacts for the entire SIT. The use of a single level will lead to a less complex BIA process because it removes the necessity to determine impact criticality uniquely for each business division. Consequently, it removes the necessity for calculating impacts differently for each business division. What this means is that the criticality of estimated financial losses, can only be measured on the company level as a whole. Observe that the following definition is unrelated to the term critical asset.

Definition of ***Criticality for impacts***: Criticality for impacts can only be measured on a single level. The single level corresponds to the only available level, in which *it is possible to measure criticality of impact*. The single level is the point in which estimated financial loss of all four business divisions are summed together and analyzed. In other words, within this process, estimated financial loss measured on a sublevel (for example within one business division) is not measurable with respect to criticality.

2.2.2 Deriving a maximum tolerable financial loss threshold value

Siemens adopted the Sarbanes-Oxley act [*11*,*12*] of 2002 (SOA) in July 2002. Within SOA (also referred to as SOX), section 404 includes **assessment of internal control**. SOA 404 requires SIT to assert that its internal controls are able to prevent or detect misstatements in annual financial statements. The SIT SOA 404 methodology includes a definition of a local set of significant accounts. A significant account is the same as an account or a group of accounts, subject to similar risks estimations, based on the result of different classes of transactions [*11*]. The starting process for deriving these accounts is to look at the balance sheet and income statement. These accounts are then subject to something that is called Planning Materiality (PM), referring to key financial statement benchmarks. If an account exceeds the PM Line-Item threshold (5 % x 75 % x EBIT) then that account is significant, meaning for example that the account possibly

could contain misstatements. The PM and LT thresholds can be used to define a "High" impact threshold level with respect to the BIA.[1]

Definition of ***High impact*** (for Siemens SIT): High impact gives the maximum level of tolerable financial loss with respect to one incident during one year for the entire Siemens SIT. This level can be calculated as 5 % x 75 % x EBIT which equals the Line-Item threshold. 5 % x EBIT equals the Planning Materiality threshold which constitutes as the maximum level of tolerable financial loss with respect to all incidents during one year.

For example, the EBIT for year 2008 equalled 109 571 109 Euros. To derive what constitutes "High impact", is done by calculating 5 % x 75 % x EBIT which equals 4 108 917 Euros. Consequently, estimating a financial loss (impact) equaling or exceeding this value, based on the possibility of some damaging event being realized would define the impact of that loss as "High impact". Furthermore, this impact is defined on the company level as a whole, meaning that individual sums from sublevels (each business division) are individually irrelevant. It is the final sum of all sublevels that defines the impact for the company as whole.

2.2.3 Scale for criticality impact

Within this process, criticality of impact is based on a three-level scale, low, significant and high. This criticality impact scale has been found in Siemens Corporate Information Office (CIO) documents related to BCP and consequently BIA. The following intervals will be used in order to derive significant and low impacts. These intervals used are the same as in [*7*]. The high-impact threshold is based on the definition of high-impact (see chapter 2.2.2).

Table 1. The tables contain the impact levels, low, significant and high. These impact levels are essential for the BIA process and will be used throughout the BIA process in order to identify criticality of impacts.

	High impact	Significant impact	Low impact
Minimum	5 % x 75 % x EBIT	Maximum (Low impact)	0
Maximum	∞	Minimum(High impact)	4% x Minimum(High impact)

2.3 Identifying relevant threats

This part of the process (the first part of the threat assessment) has been included to set the scope for the threat assessment. Determining a static list of relevant threats limits the scope of the threat assessment and avoids unnecessary work for when analyzing different threat scenarios in chapter 3.7. In addition to the threats taken from different databases, as included in chapter 3.3, the following list originating from [*7*] will be considered for when determining relevant threats to include. The list contains threats identified by an international association of leading companies, Information Security Forum (ISF).

[1] The use of the LT threshold for "High impact" was based on discussions with Siemens SIT financial management experts.

ISF have identified and classified threats that organizations typically face on a day-to-day basis. Some of these threats are summarized below:

Table 2. This table presents some of the threats identified by ISF, which companies typically face.

Threat category	Threat type
External attack	Distributing computer viruses (and worms).
	Hacking into systems.
Internal misuse	Modifying or inserting software without authorization (e.g. creating backdoors).
	Misusing systems to commit fraud (e.g. salami slicing).
Theft	Theft of proprietary business information.
Human error	Errors by IT/Network staff (e.g. misconfiguration).
Malfunctions	Malfunction of application software and services developed in-house.
Service interruption	Loss of power or system overload.

2.5 Gathering assessment data

This part of the process describes the method to gather most of the data required to perform a BIA. It was identified as possible to use an existing corporate information security web-based survey system called Deficiency Analysis [*13*], in order to gather data.

Interviews were conducted in order to verify the validity of the additional questions needed to gather data. The aim of the process is to enable gathering of data using the survey system. But it requires that additional questions be included. The questions that were asked are available in appendix A.

2.6 Identifying critical assets

The BIA process is an asset-based vulnerability process. This means that one first asks business representatives which resources they are dependent on and to what extent. With such information it is possible to decide which asset's that are critical and which that are not critical.

The process to identify critical assets has been simplified by creating a tool called the Critical Asset tool, which allows the BIA practitioners to compile the gathered data and automatically estimate criticality of assets. Criticality of the assets is based on a criticality scale from 1 to 5 (Low = 1, Significant = 3 and High = 5). By using the data gathered it is possible to estimate an average score for each asset and thus determining it as critical if it exceeds a specific criticality value.

2.7 Deriving impacts and determining recovery-time objective

Chapter 3.6 describes how to derive impacts and recovery-time objectives (RTO). The impacts estimated are needed in order to understand to what extent a critical asset could cause damage to the company with respect to loss of confidentiality, integrity and/or availability. For confidentiality and integrity it is merely a matter of calculating impacts

with respect to loss of confidentiality or loss of integrity. For example, what is the estimated damage if an employee steals information and starts a competing company or what kind of damage would occur if data held in by some information resource were to be corrupt and thus would provide false information as a basis for important decisions? For availability, impact is estimated differently. Damage because of interruption usually increases with time and at some point, the damage have increased so much that the significant impact level is reached. The closest point in time before reaching this impact is referred to as the RTO.

Definition of ***Recovery-time objective (RTO)***: The recovery-time objective is the estimated time (in the chosen time scale 1 hour, 1 day, 2-3 days, 1 week and 1 month) until significant impact is reached. The RTO indicates the time in which a critical asset must be restored to normal operation in order to avoid further increase in impact causing at least significant impact (and consequently high impact).

For example, given loss of availability (interruption) for the critical asset X, the damage because of interruption is estimated to reach significant impact after 1 week. In order to avoid reaching significant impact, the critical asset must be restored within 2-3 days (which is the nearest time point in the scale). The RTO is thereby determined as 2-3 days.

It is however not enough to determine just the RTO. It is also necessary to estimate the actual recovery time.

Definition of ***Recovery-time***: The recovery time is the estimated actual time to restore a critical asset. It is the time, in which one considers already existing incident plans or emergency plans in order to estimate how fast the critical asset could be restarted/restored in reality, given worst case full interruption.

For example, in the case one would like to determine the recovery time for an information technology resource, call it X, a subscription service might be used. In such case, assume that there exists a hot site or perhaps a cold site. A hot site is the best disaster recovery alternate backup solution as it is immediately available after some disruptive event such that the resource X could be restored, or the data held by X could be restored immediately. The recovery time in such a case, could be estimated as very low. However, a cold site is not considered as an adequate solution because it usually takes more time to get it going in comparison with a hot site. In such a case, the recovery time might be estimated as higher. [*6*]

After determining the RTO and the recovery time for the critical asset, one of the following actions needs to be taken based on the recovery time and the RTO.

If *Recovery time* $\geq$ *RTO:* Further analysis and threat profiling is needed.

If *Recovery time* < *RTO:* No further analysis is needed.

The first condition states that if the actual recovery time is equal to or more than the RTO then the estimated impact could be realized, which is unacceptable. In such case, the critical asset must undergo further analysis in the process to mitigate risks. The second condition states that if the actual recovery time is less than the RTO then significant impact should not be reachable in reality. The unacceptable estimated impact is not realizable and the critical asset needs no further analysis with respect to loss of availability because significant impact will never be reached.

2.8 Threat profiling and assigning risk-levels

The estimated impact is a good indication to assess if it is worth spending time and money in order to prevent the damage. After all why spend time and money on something that costs more to fix than to accept? So there is a need to act such that significant or even worse, high impacts, never happen. In order to act, it is necessary to estimate if the risk involved is worth spending time and money on. This process describes a method on how to derive threat profiles (second part of the threat assessment) which is a list of a number of threat scenarios derived based on the relevant threats identified in chapter 3.3 (the first part of the threat assessment). With each threat scenario, the BIA practitioners can estimate the probability of the scenario actually occurring and also the vulnerability level with respect to the critical asset being profiled. The estimated impact, the probability of the threat occurring and the vulnerability level altogether (Risk level = Impact x Threat x Vulnerability) [*14*] gives an indication of the level of risk involved. Based on the estimated risk, one decides to reduce the risk immediately, manage or plan for the risk or simply accept the risk.

3 Performing the BIA

This chapter contains all steps needed to perform the BIA including gathering of data. An introduction to threat assessment is also described with definitions, examples and ways to analyze threats based on historical data. The purpose is to provide possible methods to use for when assessing probability of threats.

3.1 Threat Assessment

As previously mentioned, the main purpose of the BIA is to create a document in which the impact of potential disruptive events and damaging events would become clear for the management of SIT and with such information, being able to take the necessary pre-cautionary steps [*6*]. In order to accomplish this task, one needs to somehow understand and estimate the likelihoods of threats. But what kind of threats should even be considered for scrutiny? In order to limit the scope of the threats that need to be analyzed, relevant threats must be identified.

Potential threats (later evaluated with ***threat profiles***) [*15*] affecting *Critical Assets* must be analyzed.

3.2 Scope and Context of the threat assessment

There exist several definitions for related terms, such as "threat" [*16*]. Within this section, related terms and the scope for the threat assessment will be outlined.

A ***threat*** is any circumstance or event with the potential to intentionally (maliciously), unintentionally (accidentally) or randomly (natural event) exploit one specific or several ***vulnerabilities*** through a ***threat agent*** in some *Critical Asset* resulting in the loss of one or several of the following [*16*,*6*,*14*]:

- Loss of confidentiality (C)
- Loss of integrity (I)
- Loss of availability (A)
- Destruction (D)

3.2.1 Threat agent

A *threat agent* is a method used to exploit a vulnerability in a *Critical Asset* [*16*].

3.2.2 Attack

Within the scope of the threat assessment, a deliberate attack is defined as:

- Attempt to gain unauthorized access to an *Operation's (O)* services, resources or information with the possibility of compromising confidentiality, integrity or availability [*16*].
- Attempt to cause direct destruction to an *Operation's (O)* services, resources or information by some physical means.
- Attempt to compromise a *Critical Asset's (CA)* confidentiality, integrity or availability [*16*].

3.2.3 Vulnerability

Vulnerability is a weakness with respect to security procedures, internal security and pre-cautionary measures, that could be exploited in order to compromise or gain ***access*** to a *Critical Asset (CA)*. It is possible to measure risk that remains against critical assets by comparing vulnerability before implementing new pre-cautionary measures with vulnerability after implementing the new pre-cautionary measures (see chapter 3.7 or [*17*]).

3.2.4 Threat source

The source of a threat (also known as ***actor*** [*15*,*18*]) can just about be anything. This definition narrows down all the possibilities into six main source classes. Actors share the property of being internal or external, meaning for example an employee or someone outside an organization.

- A threat source can be a person deliberately implementing a threat [*16*].
- A threat source can be a person unintentionally implementing a threat.
- A threat source can be an organization sponsoring and/or implementing a threat [*16*].
- A threat source can be a group of people deliberately implementing a threat.
- A threat source can be some circumstance implementing a threat (for example natural events) [*16*].
- A threat source can be some technical or system problems implementing a threat.

When deriving threat scenarios in chapter 3.7, only internal or external actors are used.

3.2.5 Words of estimative probability (WEP) for assessments

The use of *Words of estimative probability* (WEP) deals with some specific chosen terms, usually used by intelligence personnel in order to express probability of future events. The instigator of WEP was a former CIA analyst Sherman Kent whom also was one of the first contributors to a formal discipline of intelligence analysis. Kent's efforts with WEP, were aimed at trying to solve misleading expressions of odds in National Intelligence Estimates [*19*]. Kent's efforts to quantify what was, qualitative judgments did not entirely prevail, but his essay [*20*], still remains valid and is today used in threat assessments by security services and organizations [*21*,*22*].

Estimates based on ambiguous or vague terms, could potentially hide an increasing likelihood of poor decision making. Within the BIA, decisions are made based on estimated probabilities and impacts which set the level of risk involved. Communicating poor estimated probabilities using weasel terms [*23*] would cause the BIA decision matrix (see chapter 3.7) into a state of uncertain outcome. The decision would simply become untrustworthy and thus useless.

In order for the BIA practitioners to efficiently communicate estimates of probability within the BIA and consequently the threat assessment, a well-chosen and

unambiguous WEP-table should be implemented in the process to avoid poor decision making. Furthermore, one of the proposed reforms in [*24*] should be implemented as for example done in [*22*] to also include *Confidence in Assessments (CiA)*. When using CiA the sources of assessments can be graded with a level of confidence.

The WEP-table used in this threat assessment, is based on Kent's original WEP [*20*], from the Centre of the Study of Intelligence, CIA, 1964 and [*21*]. The following table presents states of probabilities, corresponding phrases of probabilities, quantification of probabilities and per year basis expressions.

Table 3. The table shows how probability phrases can be quantified. This table is used in the entire threat assessment and the risk analysis. Every phrase of probability in one state of probability should be regarded as equals. E.g. the phrases "Virtually certain" and "Highly likely" are the same.

State of probability	Quantification	Phrases of probability	Per year basis
Certainty	100%		Once every year
Almost certain	93% (give or take 6%)	Virtually certain Highly likely All but certain Odds overwhelming	
Probable	75% (give or take 12%)	Likely Probable	
Chances about even	50% (give or take 10%)	Chances about even	Once every two years
Probably not	30% (give or take 10%)	Unlikely Low probability	Once every 3 to 5 years
Almost certainly not	7% (give or take 5%)	Extremely unlikely Virtually impossible Slight chance Little prospect Highly unlikely Highly doubtful	Once every 9 to 50 years
Impossibility	0%		

The purpose of using phrases including terms like "we estimate a *probable* chance of…" or "it has been estimated as *extremely unlikely* that..." is to simply communicate analytical assessments and estimations. Any decisions made to use such phrases are not meant to present facts or proofs. Additionally, as mentioned above, CiA will be utilized to set a level of confidence attributed to the judgments made by the BIA practitioners. The following CiA scale will be used [*22*] in the threat assessment.

Table 4. Confidence in Assessments is used to support qualitative judgments by assigning them with a level of confidence. The confidence levels are also used within the risk analysis.

Confidence in Assessments	
High confidence	Indicates that judgments are based on that the circumstance of the issue makes it possible to give a solid assessment. BIA practitioners making the judgment has past knowledge and/or experiences which he or she feels very solid about and which sounds plausible. Several

	motivations exist as basis for the judgment. High confidence is not a fact or a certainty and carries a risk of being wrong.
Medium confidence	Same as high confidence with the exception of information behind the judgment lacks sufficient quality or is not corroborated sufficiently. There are few motivations behind the judgment.
Low confidence	Information and/or experiences behind the judgment are questionable with respect to plausibility. The BIA practitioner is doubtful of his or hers judgment with respect to the issue. Very few or none motivations exist as basis for the judgment.

3.3 Identifying threats

All critical assets are threatened in some manner with a certain level of risk. The threat assessment should be able to include a large range of threats, covering as much as possible or most of the modern threats today. It should also stand as a foundation, for future updates and improvements. Initially it seems reasonable to limit the scope of the threat assessment because each threat identified as relevant could potentially contribute with several threat scenarios (see chapter 3.6) and this could create a too large scope. Each threat identified will not alone provide enough information and foundation to be able to make decisions. There are simply too many properties for the threats, meaning that the threat "X" could occur differently based on its properties. For example, the threat "Theft of confidential information" could occur by someone from within the organization, but it could also occur by someone outside the organization. Both of these threat scenarios have different probabilities because they are very different. Since they are different, reducing the risk (if decided necessary) for them involves implementing different controls.

This section will describe various methods on how to identify potentially relevant threats without looking at their properties. However, the properties will be analyzed in chapter 3.6 when deriving threat scenarios.

There are three upper-level threat classes:

- Natural events
- Intentional acts to cause harm (criminal threats)
- Accidents

The threat assessment should analyze the probability of each type of threat [*25*] within each class, chosen to be analyzed for relevance.[2] When writing probability, the audience should interpret this as the likelihood of occurrence [*26*]. Furthermore,

[2] Determining which threats to analyze for relevancy is an arbitrary choice, which could be extended with time. Several databases and sources are provided within this report.

probability can be derived differently for each type of threat-class. The aim is to derive *related* threats for each class of threats.

3.3.1 Threats consisting of natural events

By analyzing historical data, one can analyze the *probability* of natural threats [*25*]. Not all natural threats should be taken into consideration and the reasons for that is based on available data and past experiences within SIT. The delimitation of this assessment is simply that at least one of the following two criteria must hold in order to include the threat in the assessment:

1. There exists historical data, claiming at least one occurrence during the last 20 years within Swedish borders, arbitrarily adjacent located geographically and which caused noticeable impact on society and infrastructure.[3]
2. There exists no historical data but its probability of occurring is estimated, as at least "extremely unlikely" (phrase of probability converts to 7 % probability with give or take 5 % probability according to the WEP-table). There should be at least medium confidence behind the judgment from the person or persons making the judgment.

As an example we can look at the following expression

> "What is the probability of a tsunami reaching Finspång in Sweden?"

One can for example with common sense, claim that this is indeed an impossibility just by looking at a map.

3.3.2 Natural threats to consider

The number of natural events threatening companies today can possibly be counted in hundreds of different scenarios, although the term "natural event" is an ambiguous term if comparing the simple definition in [*27*] with [*14*]. When saying natural event within the context of this threat assessment, it is aimed at natural disasters. Within this threat assessment, the following natural threats as included in [*28*] will be analyzed for their relevance in the context of this assessment.

Natural threats consisting of:

- Extreme rainfall
- Earthquakes
- Avalanches
- Landslides
- Forest fires
- Storms
- Beach erosions
- Floods

[3] The choice of limiting to the past 20 years is an arbitrary choice.

The first step in the process of analyzing relevance is to examine each threat against the first criteria of the threat-class assessment. The historical data required can be gathered from the statistical database in [*28*] for natural events.

3.3.3 Natural threats example: extreme rainfall

According to [*28*], seven larger natural events could be noted, which caused noticeable damage to society and infrastructure. Two of these events are summarized below.

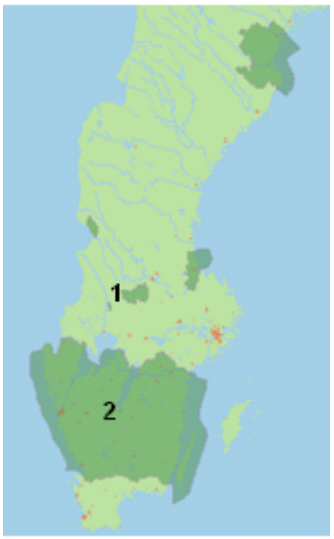


Figure 5. The map shows which areas (transparent layer) of Sweden that were affected by disasters. The numbers 1 and 2 refers to the examples given on the right and below.

1. Extreme rainfalls stroke Värmland in year 2004 with devastating downfall. The water masses caused road inaccessibility together with electronic and telecommunication disruptions. The following were consequences of the event:

    - Damage to human Health: 2 counts
    - Environmental health damage: Yes
    - Damage to habitation: Yes
    - Damage to business operations: Yes
    - Cost of damages: 47 MSEK

2. Extreme rainfalls stroke the western and southern parts of Orust in year 2005 caused by heavy thunderstorms. Many roads became inaccessible. Residential buildings, civic buildings and industrial buildings became flooded. Society became isolated and 20000 subscribers lost telecommunication capabilities and furthermore, 6000 subscribers lost electric power. The following were consequences of the event:

    - Environmental damage: Yes
    - Damage to habitation: Yes
    - Damage to business operations: Yes
    - Cost of damages: 153 MSEK

The delimitation to include extreme rainfall as a relevant threat under the natural threats-class holds on the first criteria. Consequently, extreme rainfall should be included in the threat assessment.

3.3.4 Threats consisting of intentional acts to cause harm

The criminal threats-class is a bit more complex. Not so different from natural threats, the surrounding crime rate will stand as a potential starting point to determine relevance of crime threats to include using the method in [*29*].

Crime threats occur much more frequently and are differently distributed in time than natural threats. As such, another criteria for including criminal threats has been developed. The delimitation of this assessment is that at least one of the following two criterias should hold in order to include the threat in the threat assessment. :

1. There exists historical data for the years, **n-3**, **n-2** and **n-1** such that a forecast can be calculated for the current or upcoming year **n**. The forecast reveals that the probability of the threat, in Östergötland county or Finspång county (if data is available), holds according to *Equation 4*. The method of calculation is first to derive median values (forecasts) for each month [*29*], followed by calculating a 90 % normal confidence interval for each month. The lower limit for each month is then summed. Next step is to derive a future probability estimation which later converts to a phrase of probability according to WEP. First one needs to calculate the monthly forecasts for the number of events, according to *Equation 1*:

Equation 1

$$\tilde{F}(x_{n,m}) = \mu_{\frac{1}{2}}(x_{n-3,m}, x_{n-2,m}, x_{n-1,m})$$

Where, $\mu_{\frac{1}{2}}(x_{n-s,m}, x_{n-2,m}, x_{n-1,m})$ is used as a denotation for the median for a set of data $\{x_{n-3,m}, x_{n-2,m}, x_{n-1,m}\}$ containing number of events in the past three months. $\tilde{F}(x_{n,m})$ is the forecast for each month in the current year. Months are indexed with the letter ***m*** and years with ***n***.

The reason for only using the past three years is to avoid using data that is too old. The inaccuracy of the forecast can increase by doing so. Society changes over time and so does the pre-conditions for crime [*29*]. By only using the past two years, the last year might contain extraordinary number of events, which will never occur again. It might also be inappropriate to include more than three years, as the uncertainty of the forecast could increase due to past changes in time, to society and its internal relations with respect to criminal postulation which is claimed in [*29*] One could however argue that it would be more beneficial to use more than the past three years to calculate forecasts, based on the assumption that crime does not change in the time stated in [*29*]. It is however assumed within this report that the author and the organization behind [*29*] have the sufficient expert knowledge within this field and subject.

Calculating the lower limit for each month with a 90 % normal confidence interval is done with the following formula:

Equation 2

$$LC_{n,m} = \tilde{F}(x_{n,m}) - 1.64\sqrt{\tilde{F}(x_{n,m})} \qquad [29]$$

LC is here the lower limit in a 90 % normal confidence interval, for the forecast in month **m** in year **n.** The constant 1.64 can be derived by looking into a statistical table. The lower-limit forecasts for each month are then added together as in *Equation 3*:

Equation 3

$$\tilde{x}_n = LC_{n,1} + LC_{n,2} + LC_{n,3} + \ldots + LC_{n,11} + LC_{n,12} \qquad [29]$$

It is now possible to derive a probability of the threat for the year in question using *Equation 3*. Anything below 2 % probability (2% probability converts to "extremely unlikely" according to WEP) is assumed in this assessment, as negligible. Further look at *Equation 4* reveals that forecasts with less than 7.2 events can be disregarded, and consequently do not hold in this criteria.

Equation 4

$$\mathrm{P}(Threat) = \frac{\tilde{x}_n}{365} \geq 0.02$$

What this means is that there has to exist, at least a minimum (with a 90 % confidence) estimated 2 % probability of the threat within the Östergötland county any given day in the year in question for including it in the assessment. This limit can of course be increased or decreased. The reason for including "extremely unlikely" threats is based on the potential of such threats causing severe impacts. If that is the case, then necessary pre-cautionary actions are needed regardless of low probability (which is explained in more depth in chapter 3.7). This is simply based on the fact that risk equals the product of probability and consequence, where consequence in the context of this BIA process, would be impact.

2. There exists no historical data, related to events that have occurred within SIT in Finspång. In such case, the BIA practitioners should make an estimation based on WEP. The threat is excluded if estimated as less than "extremely unlikely".

Note: The use of median values in the calculation of forecasts in criteria one, is appropriate when dealing with extremes. Extremes can make the forecasts unstable.

3.3.5 Criminal threats to consider

In this assessment intentional acts to cause harm are considered as the criminal threats-class. The number of different crime types exists in manifold. It is therefore appropriate and also necessary to delimit this assessment to some specific type of crimes which fits the purpose of this threat assessment more applicably, meaning that the crimes must have the potential to cause significant or high impact to SIT. The following crime types have been arbitrarily chosen, as included in the statistical database [*30*] and criminal types from *Table 2* should be examined for relevancy.

Criminal threats consisting of:

- Theft of proprietary business information (included in *Table 2*).
- Distributing computer viruses and worms (included in *Table 2*).
- Modifying software or inserting software without authorization (included in *Table 2*).
- Physical sabotage, with the intention to hinder normal business operations (included in the database [*30*]).

This list of possible threats to identify as relevant should be updated continuously in the future and should as of now, could be seen as a starting point for the threat assessment. When later deriving a standard threat profile (which is a list of threat scenarios), it is recommended to update this list before creating threat profiles for each critical asset. The reason is that the threat scenarios derived in chapter 3.6 are initially based on identifying relevant threats.

3.3.6 Criminal threats example: Sabotage

This example will show how to analyze relevance of the threat "sabotage with the intention to hinder normal business operations". Using the available data gathered from [*30*], a threat-class assessment controlling against criteria one, could reveal the relevance of the threat. Criteria one is only applicable when gathering data from [*30*] or if the data is available from other sources.

To estimate forecasts for the current year 2009, one needs monthly data for the crime in the years 2008, 2007 and 2006 according to criteria one. The data is available for Östergötland County.

Table 5. The table contains crime data, of Sabotage within Östergötlands county. This data can be used to predict forecasts. These forecasts can be used to estimate if a certain crime threat is relevant for the threat assessment according to criteria one.

Forecast Data Table (FDT)	Months											
Years	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Okt	Nov	Dec
2008	3	1	1	1	3	0	2	1	2	3	1	2
2007	2	0	1	1	0	1	1	0	1	0	0	0
2006	0	1	0	0	1	0	0	0	0	2	0	0

It is worth mentioning that the population data in *Table 3* is somewhat limited (some months only have one event, which is quite random). This type of population contributes to higher variances and higher uncertainty. Other crime types with higher populations (for example more than 20 events per month) decreases variances and the outcome carries a higher relative certainty. This issue is handled by using the lower limits, in a 90 % normal confidence interval.

The next step is to calculate a forecast for each month for the current year $n = 2009$ according to *Equation 1*, the forecast per month is estimated as

$$\tilde{F}(x_{n,m}) = \mu_{\frac{1}{2}}(x_{n-3,m}, x_{n-2,m}, x_{n-1,m})$$

The following result can be derived.

Table 6. The following table contains forecasts for each month based on the data from Table 5 . The forecast is calculated as medians according to Equation 1.

Forecast year 2009	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
	2	1	1	1	1	0	1	0	1	2	0	0

The following figure (*Figure 6*) visualizes the forecast.

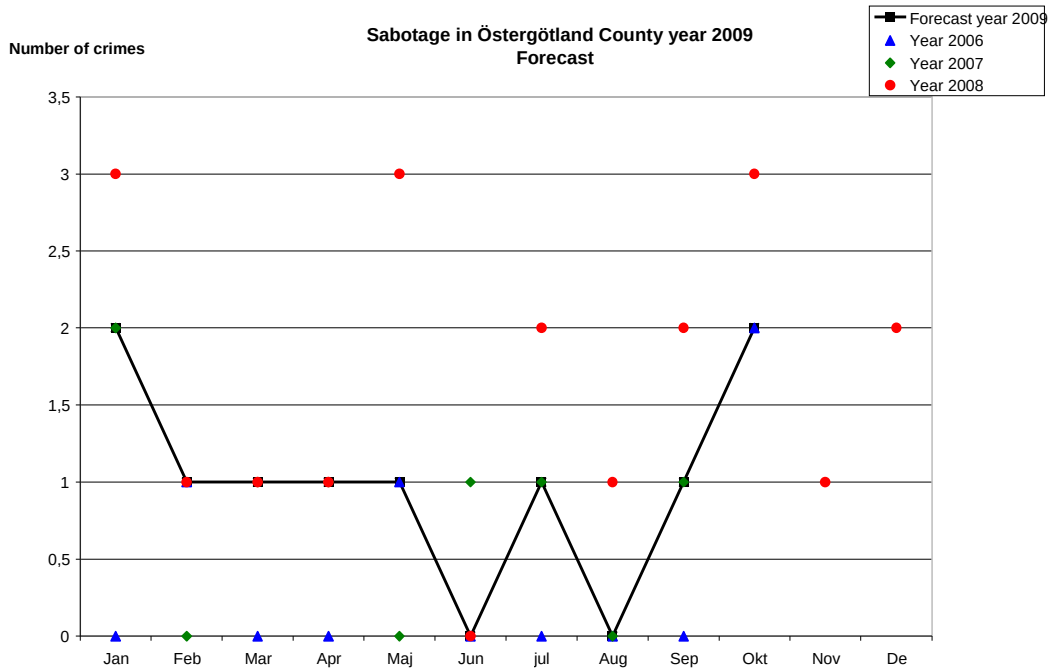


Figure 6. The figure demonstrates the results of the method for calculating forecasts and as one can observe, year 2008 consists of a noticeable increase of events, although by using the past three years, and given that only 2008 deviates do not cause the outcome into taking consideration to these extremes which may only happen this one year.

The next step is to, for each month; calculate the minimum value in a 90 % normal confidence interval which gives the following results.

Table 7. The table contains calculated, lower limits in a 90 % normal confidence interval.

Lower forecast limits (90 % normal confidence interval)	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Okt	Nov	Dec
	0	-1	-1	-1	-1	0	-1	0	-1	0	0	0

At this point, all values in table minimum are added together as

$$\tilde{x}_n = \sum_{m=1}^{12}\left(\tilde{F}\left(x_{n-3,m}, x_{n-2,m}, x_{n-1,m}\right) - 1.64\sqrt{\tilde{F}\left(x_{n-3,m}, x_{n-2,m}, x_{n-1,m}\right)}\right)$$

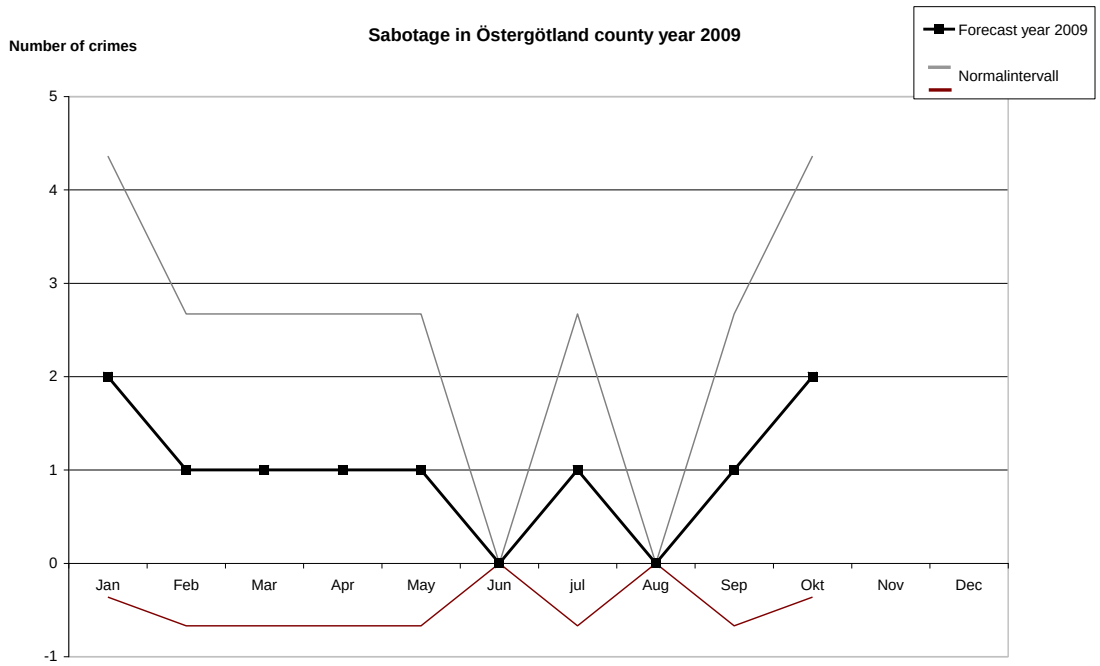


Figure 7. The figure visualizes the forecast (black line), the upper limits in a 90 % normal confidence interval (grey line) and the lower limits (red line) for each month.

Total number of future occurrences is estimated as $\tilde{x}_n = 0$ and by checking against *Equation 4* we derive the following:

$$\mathrm{P}(Sabotage) = \frac{\tilde{x}_n}{365} = 0 \text{ (0 \% probability).}$$

Which does not hold according to the first criteria requirement and, as such including the threat in the assessment is not appropriate. The threat is simply not significant enough to include it in the threat assessment based on the found data. We also note according to WEP that the minimum probability (within a 90 % normal confidence interval) of this threat being realized within Östergötland County at any given day, in the year 2009, is estimated as less than "extremely unlikely".

3.3.7 Accidental threats to consider

The type of activities located within each business unit in SIT, relates directly to the probability of different types of accidents. Generally, activities using heavy machinery in the workshops for example are at higher risk for serious or life-threatening accidents than typical office locations [*25*].

Assessing whether a specific accident is relevant for SIT and consequently the threat assessment, based on surrounding accident rates is assumed as infeasible because of poor decision basis. Accident rates in an adjacent located company as for example SAPA (which is located nearby) could possibly produce a lot more accidents than SIT based on differing types of business operation activities. Basing relevant accidental threats on surrounding rates, and consequently on companies located close by is simply illogical, especially if no physical interdependencies exist amongst the companies.

Given this reasoning, determining relevant accidental threats will solely be based on past experiences within the company.

The following threats could potentially be relevant:

- Fire in buildings.
- Technical failure of important and costly machinery.
- Errors made by IT/network staff or regular staff (included in *Table 2*)
- Malfunctions of software and services developed in-house (included in *Table 2*).
- Loss of power and/or system overload (included in *Table 2*).

This list could contain countless more potential accident types. As previously mentioned for criminal threats, it is appropriate to always think immensely regarding potential threats. The BIA is aimed at deriving decision basis for costly impacts (significant or even worse, high impacts).

3.3.8 Threats consisting of accidents

As previously mentioned, evaluating relevant accidental threats could be based on past experiences within SIT. Companies have diverse security cultures and making decisions based on surrounding statistical data have been judged as unwise.

The following criteria for including accidental threats is proposed.

1. Each proposed threat must be estimated as at least "extremely unlikely" by the BIA practitioners, according to WEP. The confidence level should be at least medium confidence according to CiA.

These estimations could possibly be made based on the BIA practitioners past experiences within SIT.

3.4 Gathering assessment data

When performing a BIA there is a need to gather information and data. Gathering of data and information can usually be made quantitatively and/or qualitatively [*9*]. Qualitative methods include performing workshops and/or interviews which usually take some time if many interview candidates are involved. A quantitative method could be sending out surveys which is time-efficient but may lack the same quality compared to performing interviews or workshops.

As previously mentioned, one of the requirements for the BIA process is that it should be optimal with respect to time and cost. It has been discovered possible to use an already existing corporate information security survey process to gather data. It is called Deficiency Analysis (DA). The DA uses a quantitative approach for gathering data using a web-based intranet survey system in which managers are invited to participate yearly. The target group for this analysis is for those who are directly responsible for and have the necessary knowledge of the respective processes in the work area which includes office, laboratory, workshop etc. A DA invitation is usually sent out to around 150 managers at different management levels within SIT and around

50 to 100 of them execute the survey. What is useful in the data gathered from the DA is included within the first part, called Appraisal. The Appraisal is a part of DA for which the managers are asked to evaluate and note assets, under their responsibility by checking thru control questions with respect to confidentiality, integrity and availability (see paragraph A5 in appendix A).

The BIA process is driven based on the concepts of confidentiality, integrity and availability, because of this using the DA to gather information about potential critical assets seems reasonable. The BIA practitioners can gather information from the existing DA process and thus providing SIT with an integrated solution for which repetitive activities are avoided.

3.4.1 Lack of data and lack of quality in data gathered from DA

The data gathered from Appraisal in the DA is presented in a list with the following format.

Table 8. The gathered data from Appraisal in the DA is presented in the following format (the brackets and the contents are replaced with real data), usually containing one to ten entries. The type of the information held in by the information resource is entered first, followed by which system, software and/or services holding the data. The last three columns address the security requirements with respect to confidentiality, integrity and availability. Each box is marked if the requirement exists for the asset (see paragraph A5 in appendix A).

[Type of information]	[System (Archive/IT platform)]	[Confidentiality]	[Availability]	[Integrity]

When reviewing the last executed Appraisals from last year (2008) it was noted that the results of the Appraisals varied significantly. Some of the managers marked every security requirement for every asset and some did not mark any of them (the purpose is to at least mark one if noting an asset). Furthermore, the DA in its current form does not gather additional information for the purpose to decide relative importance of the assets, meaning that it is impossible to decide which assets that are critical and which that are less critical. The following was realized after initially reviewing the information:

- Several of the managers are not familiar with the concepts of confidentiality, integrity and availability within the field of information security.
- To be able to use DA in order to gather information on which assets that are Critical Assets requires including additional questions in the DA, or specifically updating the Appraisal part. By doing so (if possible) would provide the BIA process with a quantitative data gathering approach.

A questionnaire was developed, called the Critical Asset Identification Template (available in appendix A). This template is meant to be used in order to evaluate if an asset can be regarded as a critical asset and also to provide indications of the type of losses (impacts) that could strike the company given that confidentiality, integrity and/or availability were lost for the assets. Furthermore, the Critical Asset Identification Template supports unlike the Appraisal in DA, various types of assets. The following types have been included within this process, partly originating from [*31*].

- **Systems assets** which include information systems that store, transmit and/or processes information and data. The components of systems are software, information and hardware. Examples are networks, embedded systems (special purpose computer systems like for example routers and switches) and other devices which support SIT's IT-infrastructure.

- **Hardware assets** consisting of physical workstations and servers. A potential asset can also consist of several workstations within some finite physical area.

- **Information assets** which consist of electronic or paper documentation. Intellectual assets belong in this group. These are closely related to "Systems" and "Software and services" which store, process and transmits critical information that drives the organization.

- **Software and services assets** consisting of applications which could be operating systems, database applications, custom applications or office applications. When for example identifying a software application, it is appropriate to explain if the software as whole is the asset or the connected database.

- **Other resources** consisting of for example certain heavy machinery in the workshop.

- **Personnel** who carries important knowledge, training and experience.

An asset could also be regarded as a combination of the above categories, e.g. an application which contains sensitive information could be regarded as a "Software/Information" asset.
The DA in its current format only treats information systems and this is something that needs to be updated or altered in the future.
In order to verify the validity of the questions included within the Critical Asset Identification Template (See: Appendix A Identifying Critical Assets) and that its granularity level is appropriate, a number of interviews were conducted with some of the local managers at SIT in Finspång.

3.4.2 Interviews conducted

Approximately 40 managers answered all the questions in the last DA. Out of these 40, 10 managers were selected for interviews. The selection was partly based on the answers given with respect to gathering information based on a wide distribution of the different business divisions (gas turbines, oil and gas, service and steam turbines) and work areas (research and development, logistics, marketing and sales, service etc).

3.4.2.1 Assessing types of assets

The first initial interviews could sometimes go on for two hours which was based on the number of assets reported (because each asset was reviewed once independently) and discussions that arise regarding the questions, which were modified successively as more and more interviews were conducted. During each interview, every asset was reviewed once using the Critical Asset Identification Template. The first question was quite straightforward and asked what the type of the asset was. The majority of the

assets were classified as a *system and information asset* or *software and information asset*. The assets that were discussed were regarding some type of information stored, processed or transmitted in some system or some software.

3.4.2.2 The asset from the managers point of view

The next question was aimed at trying to describe the asset from the managers' departments' point of view with an appropriate level of granularity in which the managers were asked to describe the asset they had noted with not too much and not too little detail. Virtually all managers could describe the asset with respect to why it exists and how it is used by their respective department. Some assets were noted by the majority of the managers and the descriptions were in many cases similar. The descriptions given also included if information and/or data was mostly inserted or extracted from the system or software by their departments. Dependencies to other divisions and departments were also brought up.

3.4.2.3 Identifying loss concepts

When arriving at the question regarding the loss properties (confidentiality, integrity and availability, see paragraph A5 in appendix A), answers sometimes varied significantly. The question is the same as Appraisal within DA. A number of control questions (available in appendix A) guides the interviewee thru identifying if the asset in question requires confidentiality, integrity or availability with respect to the interviewees department. The variation within the answers and results of this question depended on the interviewees understanding of the loss concepts and also their ability to discuss each asset on a high level. Some of them understood the concepts and had within the last performed Appraisal within DA, reasoned enough to provide a sufficient answer. Some of the interviewees had not understood the concepts and were at the same time unable to reason on a higher level, meaning that some had problems looking at the overall picture and instead engaged their focus on details. This issue contributed to changing the loss properties during some of the interviews. It was also realized how the managers looked at yearly performing the DA, which was interpreted as somewhat of a burden for the managers because of constantly working with an already high workload. This issue was even confirmed after speaking with some of them, although everyone agreed on the importance of information security and showed interest in answering and discussing the questions.

3.4.2.4 Criticality assessment

The question that followed was a criticality assessment of the asset and asked the interviewees to very approximately, in the scale low, significant and high, provide the maximum level of harm that the business could suffer if for example key information held in, processed or transmitted by the system or software were to lose confidentiality, integrity and/or availability. For the most of the interviewees, this question was straightforward. Some interviewees had problems with the granularity, meaning that details were brought up regarding different types of scenarios etc. There were also issues regarding how to interpret for example "Low" and "High" maximum damage. As a result, additional clarifications were added to the question.

3.4.2.5 Previous experiences

The next question asked the interviewees to elaborate potential loss concepts with respect to the control questions mentioned earlier. This question have a lot of freedom when answering and was included in order to gather additional information more

specific to the asset with respect to the interviewees past experiences and specific areas of concern. The interviewees were given the opportunity to provide an example scenario (for example a scenario, the possibility of third-parties getting held of confidential information or past problems with previous employees etc). The responses to this question were also quite varying. Specific events that have occurred in the past were given and potential events which could occur in the future was discussed and noted. Some of the interviewees provided the same information or at least with similar themes.

3.4.2.6 Connecting assets and operations

The second last question was regarding which *Operations* the asset belongs to with respect to the definition of *Operations* provided earlier in this report. Additionally, the interviewees were provided with a potential way of answering this question by explaining to them, that the SIT process structure (see paragraph A8 in appendix A) could be used in order to answer the question in order to provide which processes, sub-processes or business operation activities that are critical for business and dependent on the asset in question in order to function and continue normally. The answers to this question were dependent on how widely the asset is used within SIT, meaning that it is hard to pin down specific business operation activities when the asset is used in practically all activities and from which the majority of them are highly dependent on the asset. In some cases the interviewees' entire departments were given as an *Operation*. Some interviewees could provide specific processes.

3.4.2.7 Potential impacts on business

The last question (see paragraph A10) was regarding potential business impacts that could occur (very approximately), given worst-case loss of confidentiality (the most sensitive information), integrity and/or availability (one month disruption) with respect to potential *Operations* (which is only relevant in the case of loss of availability). The interviewees were provided with a list of business impact categories and business impact types under each category [*8*]. Each type could be answered yes or not applicable and also if the potential impact type was related to confidentiality, integrity and/or availability. If answering yes then that was considered an indication of the type of impact that could potentially occur (the goal was to select only a few potential impact types). The purpose of the impact list is to use it as a general list applicable for different types of assets and business areas. This question was experienced by some, as a bit hard to answer depending on which asset that was under review. A lot of the managers had noted widely used assets in the Appraisal and in such cases some of the impact types were too specific (in relation to widely used assets). Widely used assets could potentially cause all kinds of impacts when thinking worst case in different scenarios based on the relevant security requirement concepts (C.I.A).
Initially, one could answer yes or no to each impact type (which was later changed). This contributed with issues regarding impact types which were inappropriate to even discuss depending on the asset. For example, given an asset used in engineering of gas turbines could not be determined to potentially cause "Loss of confidence by key institutions" if the assets confidentiality, integrity or availability became lost. One could naturally answer no in such a case but even when considering answering no, discussions aroused with some of the managers. The choices were therefore changed to "Yes" or "Not applicable".

Furthermore, the core problem with some of the interviewees (quite few) could be noted when they brought up detailed worst-case scenarios in which something that

is actually possible, but with an extremely low probability. Therefore, the problem with conducting a BIA for a large company like Siemens is the need to think on a high-level, and not to get stuck on details. In the end with the majority of the interviews, the interviewees were asked for their opinion regarding the questions. The majority of the interviewees said that they thought the questions were good, although it was easier with the interviewer guiding and supporting them with the questions. The majority of them were asked the following "Do you think it would be easier to fill out the questionnaire alone given an already filled out example on the side and additional clarifications with each question?", and the majority of them answered yes to this question. Especially when considering, looking at already filled out examples on the side which was an interesting note as such examples did not exist for the DA which was considered as hard to complete by the majority of the interviewees.
A compilation of the summary of the conducted interviews is available in appendix C (*excluded in this version of the report because of confidential content*). However, answers to some of the questions are not included in the summary and are available in a Microsoft Excel Sheet.

3.4.3 Using the Deficiency Analysis to gather data

It has been found possible to utilize the DA in order to gather assessment data for performing a BIA with respect to identifying *Critical Assets, Operations* and possible indications of business impact type losses. In order for this quantitative data gathering approach to work, the DA must contain *some* of the additional questions as included in the Critical Asset Identification Template (see appendix A). It is at the time of writing this report, unknown if future updates to the DA is possible and if possible, how flexible such a solution would end up to become? The following is a proposition for the process flow to gather data from DA given that DA is updated with some of the additional questions in appendix A.

Note: It is assumed possible, at the time of writing this report given the possibility to update the DA, to send out traditional DA invitations to all managers and at the same time in parallel send out to some managers an updated version containing the additional questions required to identify critical assets.

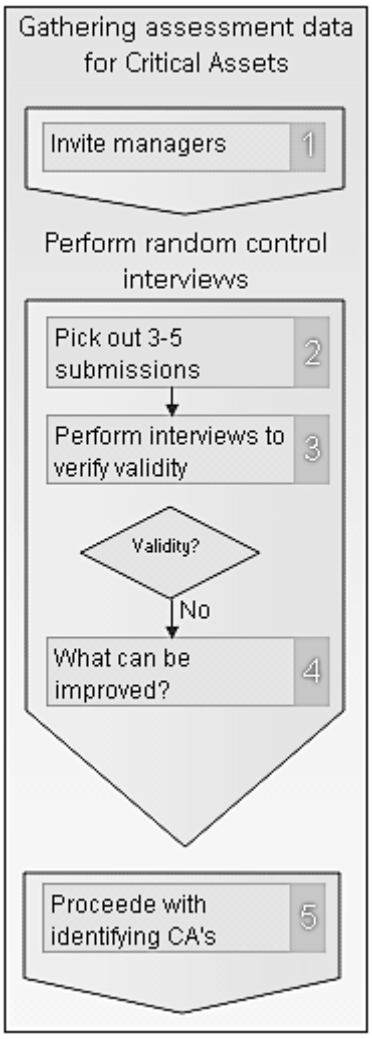


Figure 8. The proposed process to gather assessment data for critical assets.

The first step to gather assessment data is to send out DA invitations to around 20 to 30 managers at different manager levels within the four business divisions. When performing the interviews it felt equally beneficial to gather data from department managers as business division managers. Varying input was received and with different perspectives. As such, data should be gathered with respect to different departments (research and development, production, logistics, marketing and sales, service etc) in order to get a picture of the totality.

With the problems mentioned in chapter 3.4.2 Interviews conducted, one could imagine misunderstandings in the given answers, unanswered parts and illogical reasoning. It is therefore appropriate to verify the validity of those answers. Verifying validity in all submissions is not optimal with respect to time and resources needed. Additionally, continuously improving the data gathering process would result in the BIA process maturing with time. Therefore, random control interviews should be conducted by picking out three to five submissions, and performing interviews in order to verify validity. Based on these interviews, improvements can be made to the questions by clarifications and additional examples on how to fill out the questionnaire. These improvements could then be used to improve the questions for the next time invitations are sent out.

The next step is to identify *Critical Assets* based on the gathered data using the Critical Asset tool.

3.5 Identifying Critical Assets (CA)

In order to determine the criticality of an asset for SIT, the company as a whole must contribute with data as described in the process for gathering assessment data (see 3.4.3 Using the Deficiency Analysis to gather data). After gathering assessment data, there should be enough data to indicate the criticality of various assets and by having such information being able to proceed with the steps that follow (see *Figure 9*). Criticality can be determined using the Critical Asset tool which is a Microsoft Excel spreadsheet. All information gathered in the data gathering process for assets can be compiled in the Critical Asset tool.

3.5.1 Gathering assets in the critical asset tool

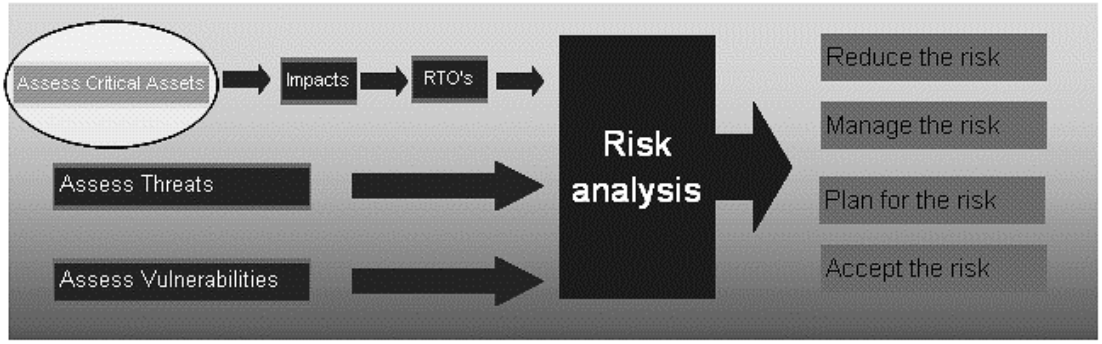


Figure 9. The figure visualizes which core part of the process that is treated. After gathering assessment data, one should be able to identify assets that are critical to business.

When the interviews were performed, the results for each interview (which includes a number of reviewed assets) were compiled in one spreadsheet per asset in which the data gathered for the assets were compiled in rows. For each respective compilation, the first four columns in the Critical Asset tool contain the basic properties for each asset, as can be observed in *Figure 10*.

3.5.1.1 Basic asset information

The type column corresponds to one or a combination of asset categories as previously mentioned and is/are available in the Critical Asset Identification Template, available in appendix A. The description column contains information about the asset from the departments' point of view with respect to each business division as interpreted by each manager. The information entered here should be basic enough to get the picture of the totality. Answers could be very varying depending on how widely the asset is used. The last column identifies the loss properties of the asset, or in other words the asset's security requirements with respect to confidentiality, integrity and availability.

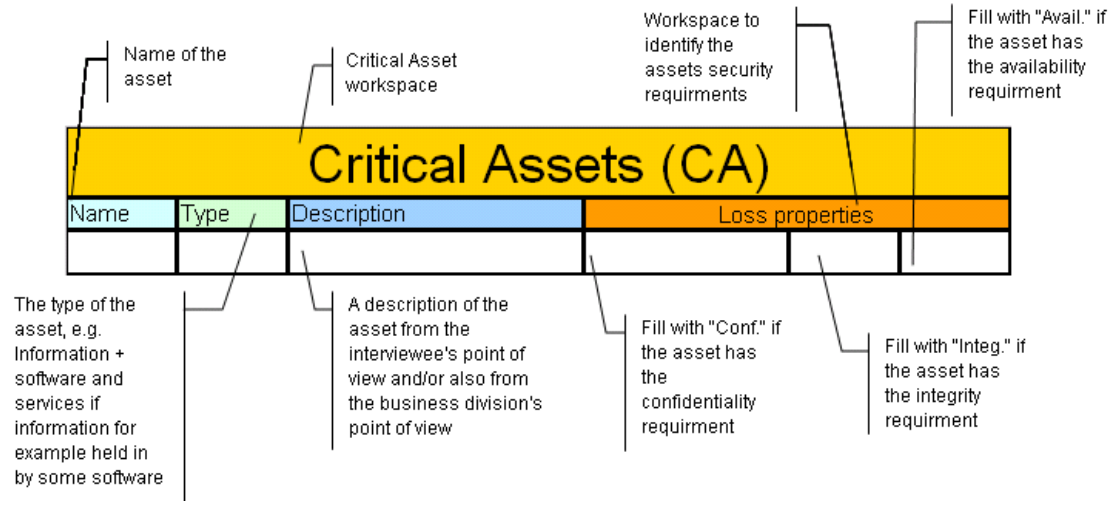


Figure 10. The first four columns in the Critical Asset Tool have room for basic properties. The name column holds the name of the asset. The description holds information about the asset from the departments' point of view. The type column holds which category the asset belongs to and the loss properties column holds the assets security requirements.

3.5.1.2 Criticality information

The next four columns (see *Figure 11*) are sub-columns of the criticality assessment (see paragraph A6 in appendix A or consult chapter 3.4.2). For each submission and for each asset, criticality is determined for each asset with respect to confidentiality, integrity and availability. Based on the identified security requirements from the previous column, managers are to select one of the potential maximum harm levels "Low", "Significant" or "High" for confidentiality, integrity and/or availability respectively. Selecting "Low" indicates from the manager's point of view given loss of confidentiality in worst-case that the maximum level of harm to the business would be "Low" meaning that harm could occur but it would not be noticeable neither for his or hers area of business and neither for the company as whole. If selecting "Significant" than that would indicate that the manager is uncertain of the maximum level of harm but cannot rule out "High" harm to the business. Selecting "High" indicates that the manager is quite certain that his or hers area of business would suffer severely and noticeably (consult paragraph A10 in appendix A).

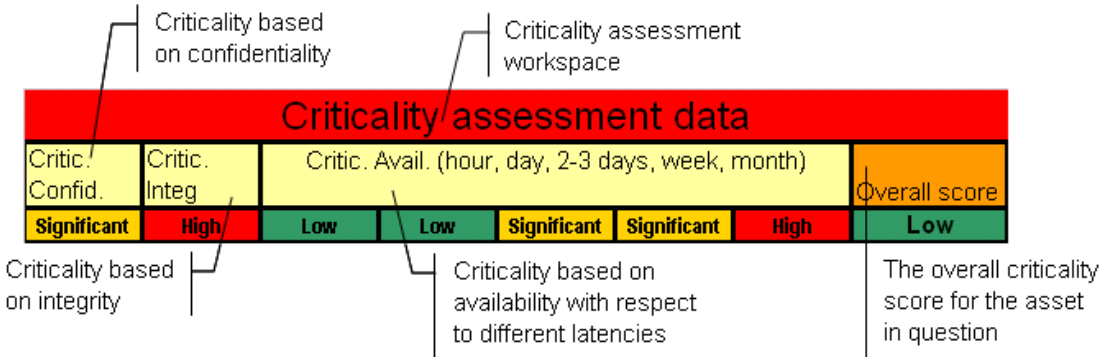


Figure 11. The next four columns in the Critical Asset Tools, holds criticality assessment data. The last column, Overall score, automatically calculates an overall criticality score for the asset in question.

For availability, maximum harm levels can be chosen based on the delayed duration of the loss of availability for the asset which varies significantly with time. One could also discuss how the loss of for example confidentiality could contribute with an evolving harm to the business with time. An example scenario could be that confidential drawings are somehow leaked out of the company into the hands of competitors and causing SIT to lose sales after a couple of months or a couple years. The damage evolves with time, but the loss of confidentiality is instant. But taking such reasoning into consideration is assumed as to complex and un-feasible. The final of the four columns automatically estimates an overall criticality score for each asset (and for each manager). This score is estimated differently based on the relevant security requirements. If for example only loss of availability is relevant, the overall score is estimated based on only availability, meaning that the average score is calculated on those four cells (see the note below).

Note: It is again worth mentioning that the requirement for performing a BIA within Siemens SIT only encompasses loss of availability. Criticality identification is therefore only required for assets with at least the availability requirement.

3.5.1.3 Operation and impact types

The last four columns (see *Figure 12*) hold additional information to be used in later steps in the BIA process. The first column "Elaborate" holds managers' past experiences related to previous security incidents and/or current areas of concern. The column "Part of "Operations (O)" holds information about processes, sub-processes or business operation activities which are highly dependent on the asset with respect to normal functioning and continuance. This column provides direction to which critical areas of business (consult the definition of Operations in chapter 2.1.3) that would suffer if availability for the asset were to be lost.

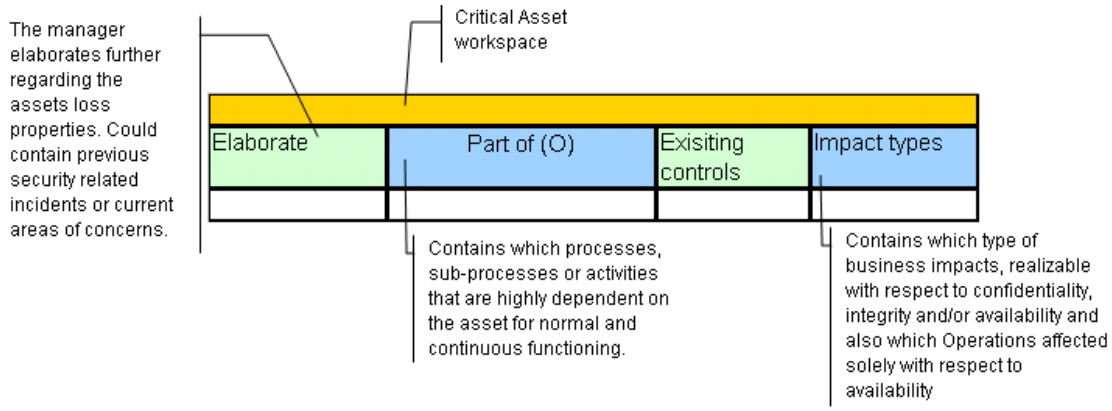


Figure 12. The last four columns in the Critical Asset Tool hold other information relevant for later steps within the BIA process.

The "Impact Types" column contains chosen business impact types potentially realizable with respect to confidentiality, integrity and/or availability. Operations identified in the previous "Part of Operations" column are connected to each identified business impact type with respect to availability, e.g. which Operation if disrupted would cause loss of sales, orders, contracts etc. These business impact types identified provide approximate indications of the type of losses to expect.

In order to identify Critical Assets (CA), all information and data gathered could be compiled in the Critical Asset tool. The following is a method on how to identify those assets that can be considered critical from the entire local SIT's view in a structured manner.

3.5.1.4 Using the tool in the BIA when identifying critical assets

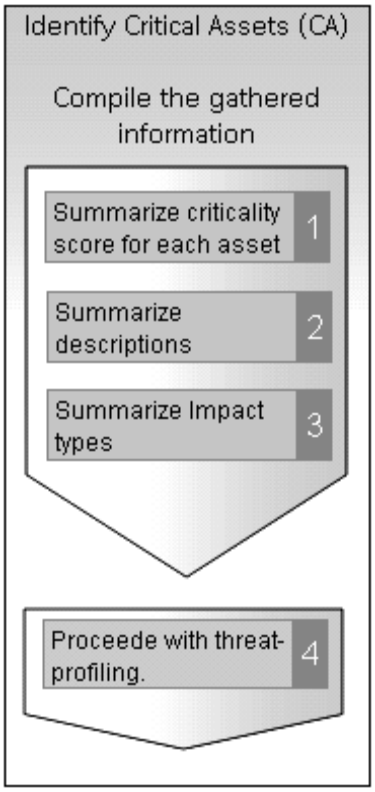


Figure 13. Process for identifying assets that are critical for SIT.

The first step when identifying/validating critical assets is to summarize the final criticality score for each asset. Using the Critical Asset Tool, it is enough to write the name of the asset under the "Name" column in the summary sheet. The implemented VBA code will automatically scan all the sheets and calculate the final score when executed. The next column to the right ("In Scope?") will automatically state if the asset is a critical asset simply by printing "Yes" or "No" based on if the average score reaches at least "Significant" criticality (consult chapter 2.6). Assets which are calculated with a final criticality of "Low" will get the output "No" under the column "In Scope". Note that several inputs from several managers for some asset, will likely decrease uncertainty when calculating the final criticality score. For example, if only one manager exclusively reports a specific asset with an overall criticality score of "High", risk of being incorrect is higher (less chance of that score being representative) with respect to the entire SIT.

The next step is to summarize the descriptions for all critical assets. General and widely used assets throughout the company should be described as general and widely used, simply because they are. Other assets might be engineering specific or might contain data and information. Additionally, some assets could be characterized as storages for data and information.

The final step is to summarize impact-types (consult chapter 3.6.2). Impact-types chosen by each manager for each asset should be chosen based on how many times they were chosen for the critical asset. For example several managers might have chosen "Loss of competitiveness" with respect to the asset X. In that case, that impact-type should be entered into the "Impact-type pick list" column for that specific asset (see *Figure 16* in chapter 3.6.2). It is simply an indication of the kind of potentially realizable negative impact, relevant with respect to loss of confidentiality, integrity and/or availability for the asset in question, e.g. if critical asset X loses availability then the effect on business will be such that competitiveness is lost. Summarizing impact-types is explained more thoroughly in chapter 3.6.2.

3.6 Deriving impacts and determining RTO

The following chapter will describe how to derive impacts and consequently RTO's based on the gathered data. The method used, is partly based on Information Risk Analysis Methodologies (IRAM) by the Information Security Forum (ISF) [*8*].

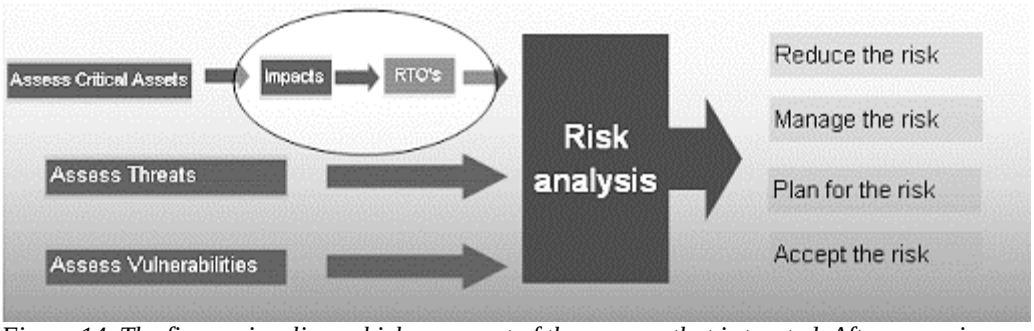


Figure 14. The figure visualizes which core part of the process that is treated. After assessing assets that are critical to business, potential impacts and consequently RTO's needs to be estimated.

A very central part of the BIA is to estimate the potential costs of losses (impacts), within this process with respect to confidentiality, integrity and availability. According to [*8*] it is important to develop a Business Impact Reference Table in order to simplify this part of the BIA. The estimated impacts are then to be used in order to estimate risk-levels as described in upcoming chapters.
Remember that data was gathered related to potential impact-types to expect for the various assets. These impact-types could be used in order to provide indications of the type of losses to expect and therefore simplify cost estimations. The business impact types treated in [*8*] have been evaluated in the interviews and the ones proven relevant are to be used within this process.

3.6.1 Impact types typically experienced

The impact-types evaluated in the interviews, were included based on a survey performed by ISF in year 2003 (and are also included in [*8*]) which was aimed towards average applications (widely used applications amongst the organization). Those organizations that participated experienced 160 incidents per annum. The following figure (*Figure 15*) presents the result of the survey.

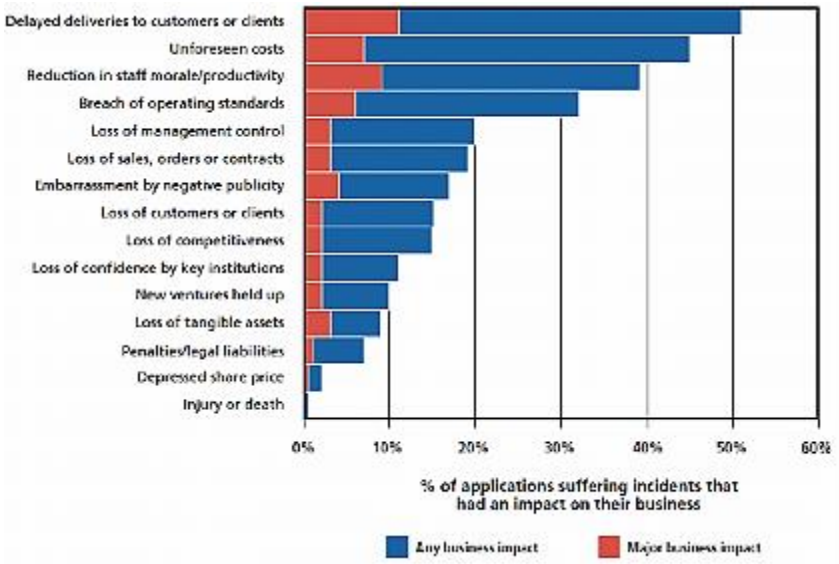
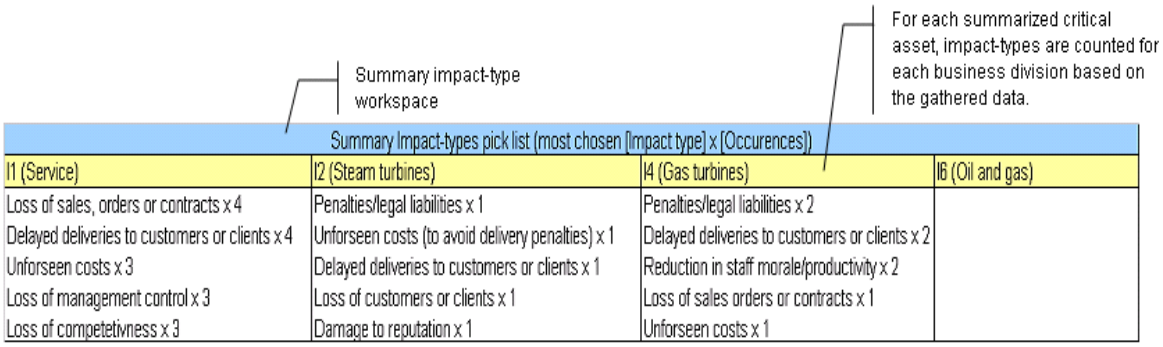


Figure 15. The figure presents the results of a survey conducted by ISF. The survey reveals which impact types, usually encountered by companies in case of incidents and emergencies.

The survey reveals how common some of these business impact types actually are with respect to commonly used applications. The most significant impact type was "Delayed deliveries to customers or clients".

3.6.2 The impact-type results from the interviews

After gathering all the necessary data as described in chapter 3.4, all data gathered should be compiled as described in chapter 3.5. The method described includes summarizing the impact-types. Summarizing the impact-types will be explained in more depth in this chapter.
In the Critical Asset Tool, a summary sheet has been created in which the results are to be summarized (see *Figure 16*).



Summary Impact-types pick list (most chosen [Impact type] x [Occurences])			
I1 (Service)	I2 (Steam turbines)	I4 (Gas turbines)	I6 (Oil and gas)
Loss of sales, orders or contracts x 4	Penalties/legal liabilities x 1	Penalties/legal liabilities x 2	
Delayed deliveries to customers or clients x 4	Unforseen costs (to avoid delivery penalties) x 1	Delayed deliveries to customers or clients x 2	
Unforseen costs x 3	Delayed deliveries to customers or clients x 1	Reduction in staff morale/productivity x 2	
Loss of management control x 3	Loss of customers or clients x 1	Loss of sales orders or contracts x 1	
Loss of competetivness x 3	Damage to reputation x 1	Unforseen costs x 1	

Figure 16. Within the Critical Asset Tool, a summary sheet contains a summary of all interviews. Each asset is summarized in rows, with one row for each asset in the summary sheet. The figure visualizes one column containing a summary of the most chosen impact types for each business division.

Each critical asset (each asset is summarized and determined as critical or not critical in the summary sheet), is summarized on its own row in the summary sheet. In each row, impact types are counted based on the managers' input. For example (see *Figure 16*), say that the critical asset X is under analysis. A number of managers (four managers in this case) in the business division service have chosen "Loss of sales, orders or contracts" if the availability for the critical asset X were lost in worst-case (which is one month). That particular impact type has been chosen the most in comparison with the other impact types. This provides with indication of how to estimate the financial loss for X given the loss of availability, for the service division (estimating loss based on the number of sales that would be missed). The impact-types summarized are usable as pick lists when trying to estimate losses. It is in other words, not necessary to try to estimate loss for all impact types noted but to choose the most relevant ones. The most relevant have higher counts and are located at the top and the ones relatively less relevant are placed at the bottom of each list. Those impact types which were never chosen have not been included in the BIA reference table which is used to input estimated losses with respect to loss of confidentiality, integrity or availability. **It is also worth mentioning that the results of the interviews conducted coincide with the results of the survey mentioned earlier. The top three impact types from the ISF survey were most frequently chosen in the interviews, conducted with the managers.**

Note: In the above figure (*Figure 16*) and the summary sheet, impact types were only summarized based on loss of availability as the BIA at Siemens SIT only demands estimating losses with respect to loss of availability as previously mentioned.

3.6.3 The BIA reference tables

Based on the results of the interviews and [*8*], three BIA reference tables have been derived, one with respect to loss of confidentiality, one with respect to integrity and one for availability. Having reference tables contributes with a powerful and simple approach for estimating financial losses [*8*]. The tables for confidentiality and integrity look the same and are presented in the figure below (*Figure 17*).

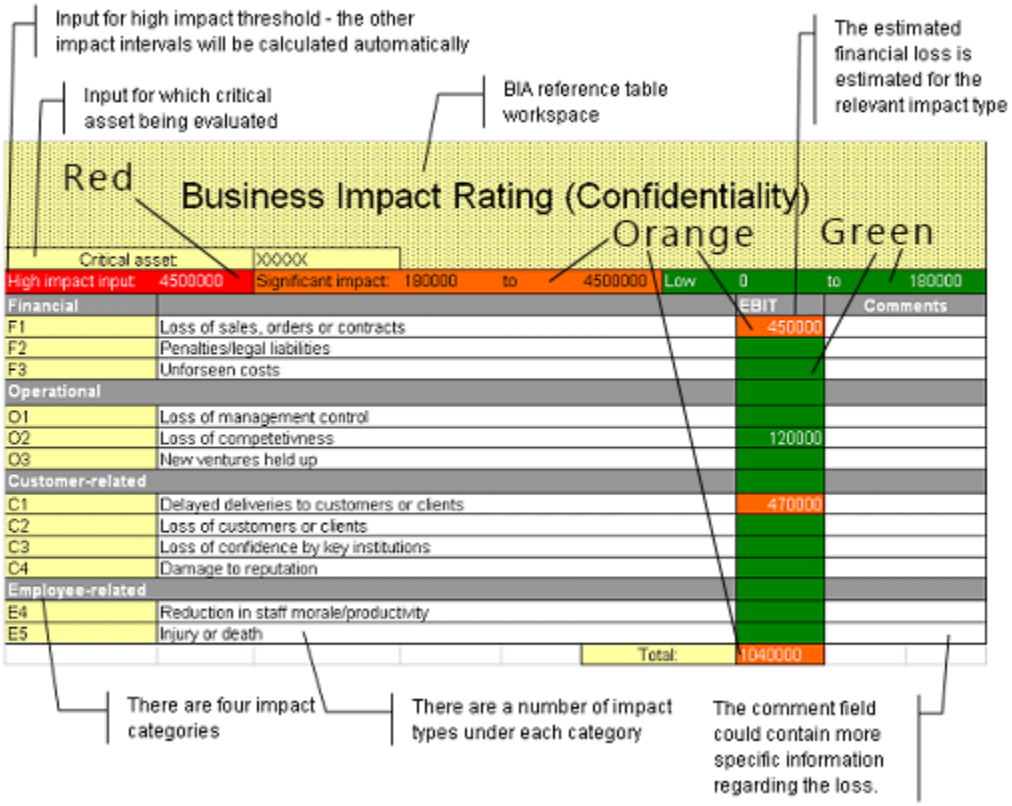


Figure 17. The figure shows the BIA reference table for estimating impacts with respect to loss of confidentiality. For each impact type chosen as relevant, the estimated impacts should be entered. The total field then sums all the impacts and indicates the criticality of the impact by changing color.

The BIA reference table for integrity is the same as for confidentiality. Financial loss is estimated based on loss of integrity. Based on the impact pick lists, the relevant impact types could be selected to perform estimations. The "total" field in *Figure 17* then sums all the values into the final estimated financial loss with respect to loss of integrity and assigns a color to the cell (green meaning low impact, orange meaning significant impact and red meaning high impact).

The BIA reference table for availability looks similar with the exception of losses being estimated with respect to time of interruption for critical assets. It is also

vital to include the RTO (consult chapter 2.7). The figure below (*Figure 18*) demonstrates the BIA reference table for availability. This reference table is a bit more complex and requires estimating losses with time. It is created such that the RTO is estimated automatically.

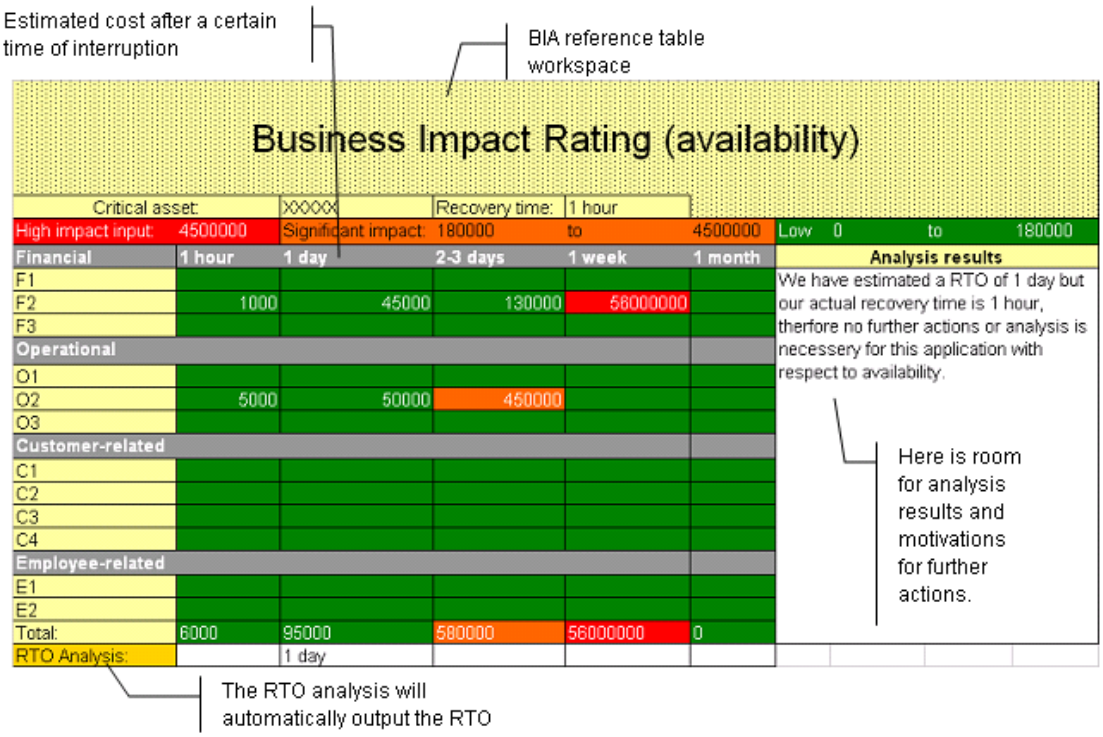


Figure 18. The figure shows the BIA reference table for estimating impacts with respect to loss of availability. For each impact type chosen as relevant, the estimated impacts should be entered for each time delay (time time of interruption). The total field then sums all the impacts for each time delay and indicates the criticality of the impact by changing color. The RTO analysis then automatically output the RTO based on the total fields.

Assessing business impact with respect to loss of availability should be done by looking at each time delay and estimating impact based on each delay. The BIA practitioners should not account for already implemented controls or "what if" scenarios when making estimations. After making estimations, purely based on a full worst-case interruption the actual recovery time must be estimated. Exactly how to estimate the recovery time demands expert knowledge about the critical asset, the IT infrastructure and current emergency plans and will not be discussed further. If one is unsure about how to estimate the recovery time, this part could be ignored. By ignoring to estimate the recovery time, one should keep in mind that performing potential pre-cautionary measures based on the risk analysis, might be extravagant measures. As stated in chapter 2.7, estimating a recovery time strictly less than the RTO would indicate that the significant or high impact would not occur. It is therefore not necessary to go further and such information would be missed if ignoring to estimate the recovery time.

3.6.4 Estimating financial losses (impacts) in a structured manner

It is important to outline, the process for estimating business impact. Based on chapter 2.2 regarding criticality, the method for estimating impact should be performed

according to the definition of the criticality criteria. The chosen method is based on discussions with SIT business division experts (Business Excellences) and the company ISO. The following will describe how to estimate business impacts for the company as whole for one critical asset. After that, it is simply a matter of repeating the procedure.

It has been decided according to chapter 2.2, to use a single (common) level for assessing criticality of impact. What this means is that only impacts for the company as whole are regarded and analyzed. For example, if one critical asset were to become interrupted and causing severe damage to the business operations of the division Oil and gas and at the same time not causing too much damage for the Gas Turbine division, it is in the end the final sum of financial loss for all divisions that will be analyzed. The downside with this approach is that individual and relatively smaller divisions such as Oil and Gas could suffer tremendously but the overall impact for the entire SIT could be less damaging (remember that the high impact threshold level is estimated based on the entire SIT EBIT) and as such, the impact would be estimated as low or significant (even though it is possibly seen as high impact from Oil and gas division's point of view).

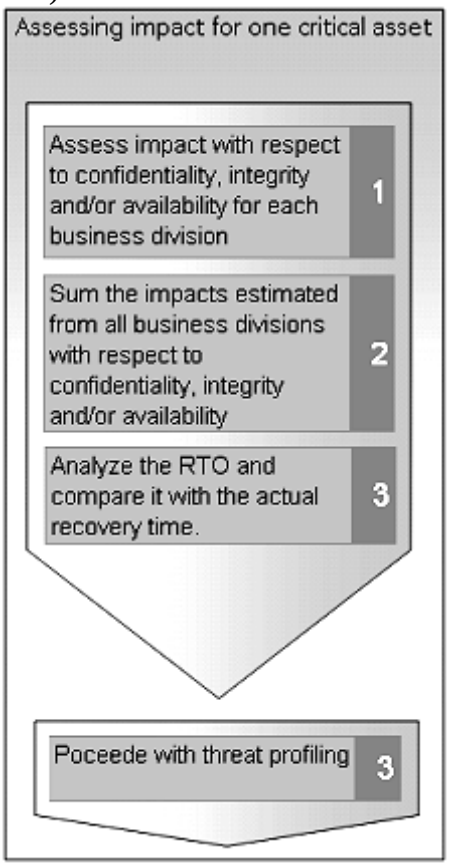


Figure 19. Process for assessing total impact for the entire SIT, for one critical asset.

The first step is for each business division to assess business impact. This could be done by using the reference tables but the RTO (with respect to availability) shown will be incorrect as each division is estimating impact for their own respective division (consult the definition of impact criticality in chapter 2.2).

For SIT it is enough to estimate impact based on loss of availability. Assessing impact could be simplified by looking at the impact type pick list for each respective division and choosing the most relevant types or type. What to look for exactly when estimating impact demands business expert knowledge and will not be discussed further. After each division has estimated their expected business impact loss, all losses should be summed (see ***Figure 20***). The RTO will be calculated automatically and should be compared to the recovery time. *If the recovery time is larger than RTO* it is necessary to analyze risks. For loss of confidentiality and integrity, it is enough to sum the estimated impacts and proceed accordingly (if estimating significant or high impact for the company as a whole).

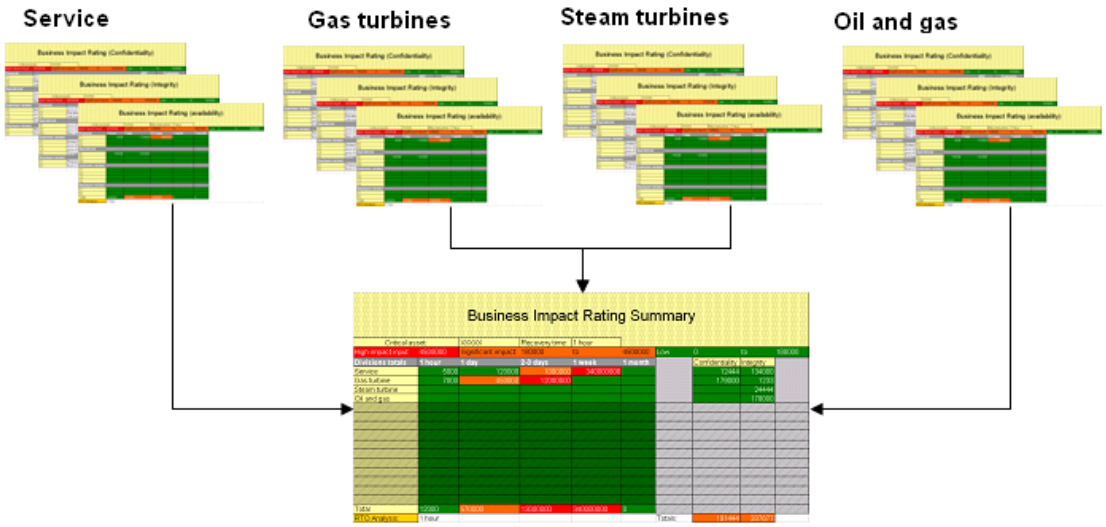


Figure 20. The figure visualizes the process described in Figure 19. Every business division estimates their own potential impacts. These estimations are then summed (in the summary sheet) in order to get the total impact for the entire SIT, for one critical asset. This approach is necessary because the criticality of impact is only measurable on the company level as whole according to the definition of criticality criteria.

3.7 Threat profiling and assigning risk-levels

In order to determine pre-cautionary measures that need to be taken for each critical asset, one must analyze the financial damage on business given loss of confidentiality, integrity and/or availability for the critical assets, and consequently determine the recovery-time objective (RTO) for each asset as described in chapter 3.6. It is however not enough to determine the impact and the RTO. Threat-scenarios must be derived together with their estimated probabilities and estimated vulnerabilities with respect to critical assets as shown in *Figure 21*. The risk-analysis method used in this part is partly built on [*17*].

Based on the impacts derived for each critical asset, together with the probabilities for various threats determines the level of risk involved (in other words determines the necessity to reduce, manage, plan or accept the risk) according to the following [*17*]:

Equation 5

$$Risk\ level = Impact \times Probability\ [17]$$

This risk level is extended to include how vulnerable a critical asset is with respect to identified threats according to the following formula [Siemens DRA]:

Equation 6

$$Risk\ level = Impact \times Threat \times Vulnerability\ [17]$$

Observe that the equations above are not correct in any way if looking at it from a purely mathematical perspective. They are simply used as an informal way to present security risk as a function of threat, vulnerability and impact [*32*].

This allows a more realistic assessment of the risk that remains after implementing pre-cautionary measures (possible to estimate the risk level after pre-

cautionary measures have been implemented by adjusting the vulnerability accordingly). "Threat" in the formula, is a prediction of the likelihood of the threat occurring and causing the impact (derived in chapter 3.6). Vulnerability describes to what extent the threat scenario will damage the business, meaning how likely it is that the threat leads to the worst case (expected) damage (maximum estimated impact) [*17*].

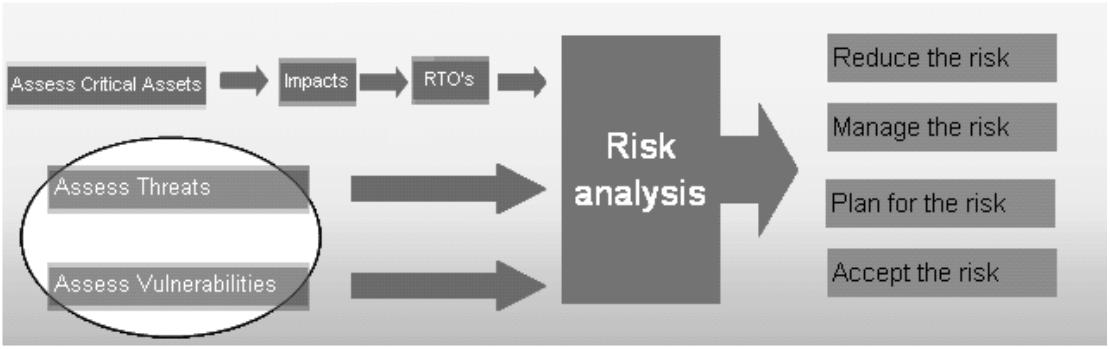


Figure 21. The figure visualizes which core part of the process that is treated. The part of the process that is marked in the figure is about deriving threat scenarios required in the risk analysis.

The threats determined as relevant in chapter 3.3 do not alone provide enough information in order for the BIA practitioners to be able to make estimations on threats and vulnerabilities. There is a need to scrutinize each threat into several threat scenarios.

3.7.1 Identifying threat-scenarios using OCTAVE

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) is an information risk evaluation methodology [*15*,*31*]. By fully following the OCTAVE method, organizations can implement pre-cautionary measures based on risks to confidentiality, integrity and availability of company critical assets [*15*,*31*]. The method consists of three phases, but only a limited part of the first phase will be utilized in this process in order to identify and analyze threat-scenarios to SIT's critical assets. The rest of OCTAVE will not be explained.

Using OCTAVE, at the end of phase one, the most critical assets to the company are identified and are scrutinized using threat profiles. Threats can be represented visually using tree structures, with one tree structure for each threat category. The advantage of using this approach enables one to group together threats with similar themes. Furthermore, threat scenarios are derived based on known sources of threat and typical threat outcomes (loss of confidentiality, integrity and availability). It is also important to mention that OCTAVE is a method with respect to information technology assets but will be extended within this process to also include threats to the types of assets described in chapter 3.4.1.

3.7.2 Properties and categories of threats

Within OCTAVE, threats are defined with the following properties [*15*].

- **Asset** – generally something of value to a company but will only be used in this process for Critical Assets (as determined in chapter 3.5 and defined in chapter 2.1.3).
- **Actor** – the threat source as explained in chapter 3.2.4.

- **Motive** – this part is according to [*15*] optional and provides with the property of deliberate or accidental intentions.
- **Access** – this part is according to [*15*] optional and defines how the asset will be accessed by the actor.
- **Outcome** – the result in loss of confidentiality, integrity, availability and/or destruction.

Within OCTAVE, the following standard (somewhat modified) categories of threats are provided [*15*].

- **Human actors using network access** – Threats in this category are network-based threats to critical assets. The actor's intention could be deliberate or accidental.
- **Human actors using physical access** – This category of threats represents physical threats to critical assets. The actor's intention could be deliberate or accidental.
- **System and other resource problems** – This category originally treats problems with organizations information systems. Examples are malicious code, hardware defects and other system-related properties. As mentioned earlier, there is a need to extend the analysis to cover additional types of threats, going beyond information systems. Consequently, additional threats regarding technical problems to resources other than information systems can be included in this category. An example is technical failure of heavy machinery (see appendix chapter B3).
- **Other problems** – The threats within this category are in the generic category usually outside the control of the organization. Examples are natural disasters, external power outages and telecommunications failures. This category will also be modified to include internal disasters. An example is fire arising from within SIT.

These standard (somewhat modified) threat categories are available visually as tree structures in appendix B and collectively correspond to a threat profile model. As mentioned earlier, one threat profile should be created for each asset. The generic (unmodified) threat profile addresses a standard range of threats to critical assets and is sufficient for some organizations. For other companies like SIT, the profile needs to be tailored for the organization like the one in appendix B. Tailoring the profile is possible by [*15*]:

- Adding a new threat category
- Adding new threats to an existing category (which was done for the last two categories system and other resource problems and other problems).
- Deleting unsuitable threats from a category.
- Adding depth to a category, e.g. the actor property can by default be "internal" or "external", meaning someone outside the company or someone inside. One could increase depth by including employees, terrorists, spies, vandals etc.

The categories of threat are based on the context on which a company operates and must therefore be adjusted accordingly. The following threats were identified as relevant as described in chapter 3.3 and should be mapped to appropriate categories. If

a threat does not match in one of the already existing categories then additional categories should be created or existing categories modified in the threat profile model.

Table 9. The threats included within this table, have been determined as relevant using the approaches described in chapter 3.3.

Natural threats	Criminal threats	Accidental
Extreme rainfall	Theft of proprietary business information	Fire in buildings
Storms	Distributing computer viruses (and worms).	Technical failure of important and costly machinery
Floods	Modifying software or inserting software without authorization	Errors by IT/network staff.
		Malfunctions of software and services developed in-house
		Loss of power
		System overload

The threats within the first column "Natural threats" fit nicely in the category **Other problems**. This is because natural disasters are included in that category. In the second column "Criminal threats", the first threat "Theft of proprietary business information" fits into the categories **Human actors using physical access** and also **Human actors using network access.** Regarding the latter, should also hold "Distributing computer viruses (and worms)" and "Modifying software or inserting software without authorization".
The **Other problems** category has been extended and should contain the threats "Fire in buildings" and "Loss of power (external)" and will be put in the category accordingly. The threats "Errors by IT/network staff" belongs in **Human actors using network access** and "Malfunctions of software and services developed in-house", "System overload", "Technical failure of important and costly machinery" and "Loss of power (internal)" belongs in the category **System and resource problems.** The following table contains a summary.

Table 10. The threats identified as relevant in Table 9, are analyzed using the tree structures in appendix B. By doing so, enables one to derive several unique threat scenarios.

Human actors using network access	**Human actors using physical access**	**System and other resource problems**	**Other problems**
Theft of proprietary business information	Theft of proprietary business information	Malfunctions of software and services developed in-house	Extreme rainfall
Distributing computer viruses (and worms)		Technical failure of important and costly machinery	Storms
Errors by IT/network staff		System overload	Floods

Modifying software or inserting software without authorization		Loss of power (internal)	Fire in buildings
			Loss of power (external)

The threats in *Table 9* can fall in more than one category in *Table 10*. For example, when inserting the threat "Loss of power" this threat could fit in **System and other resource problems** as well as **Other problems** which contributes with more than one specific threat scenario.

It is now possible, based on the summarized table (*Table 10*) and the tree structures in appendix B to derive threat-scenarios with their unique properties. These threat-scenarios will be used in the risk-analysis, explained further in chapter 3.7.3. The standard threat profile is available in appendix D.

3.7.3 Performing the risk-analysis

The following chapter will describe the risk-analysis process on how to derive decision-basis for the various threat-scenarios in the standard threat profile model, in order to perform pre-cautionary measures.

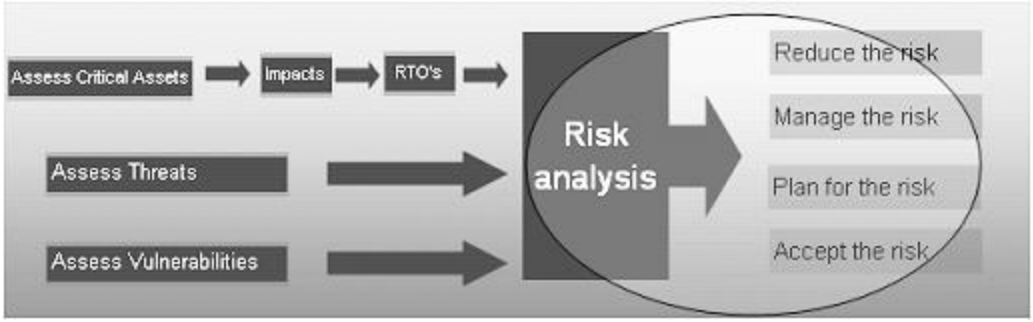


Figure 22. The figure visualizes which core part of the process that is treated. The part of the process that is marked is about the risk analysis process necessary in order to derive decision basis for pre-cautionary measures. This part of the process is where all the other previous parts coincide.

The formula for risk-level (see *Equation 6*), as mentioned earlier is used in order to estimate the level of risk involved with respect to each critical asset, the maximum possible damage (impact) and each relevant threat-scenario which will be explained further. Each critical asset must be evaluated separately using the standard threat-profile model which includes a number of threat-scenarios derived using the approach described in chapter 3.7.2. In order to demonstrate and simplify this part of the process, a risk-analysis tool has been created. The tool makes use of a Microsoft Excel spreadsheet.

The risk-analysis tool needs some input in order to estimate risk-levels. Firstly, one must input the maximum damage (impact) in EBIT (as described how to derive in chapter 3.6) with respect to loss of confidentiality, integrity and/or availability. The current high-impact threshold level in EBIT is also necessary (consult the definition of "High impact" in chapter 2.2.2). These inputs (see *Figure 23* and *Figure 24*) are needed in order to determine risk-levels for each potential threat-scenario included in each

spreadsheet (remember that each critical asset is profiled individually in its own sheet which contains a number of different and unique threat-scenarios).

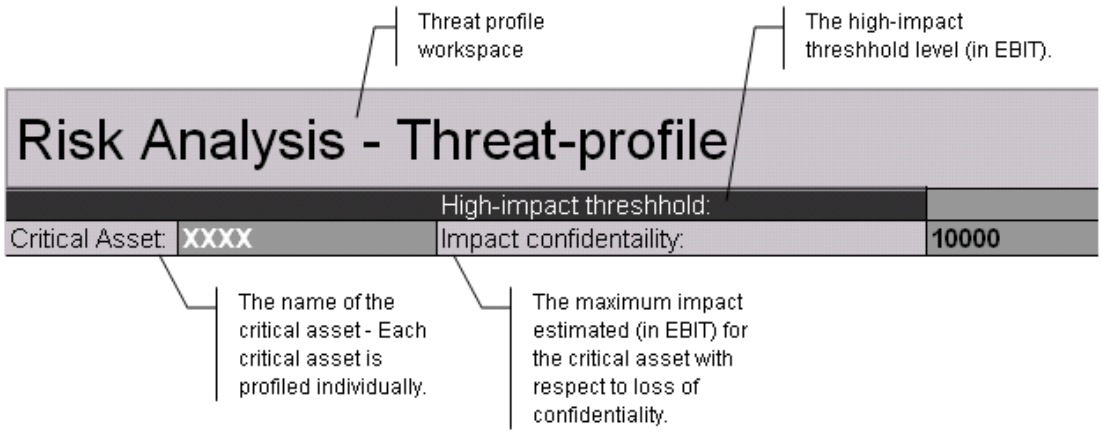


Figure 23. The figure visualizes a part of the Risk analysis Tool where required input is given.

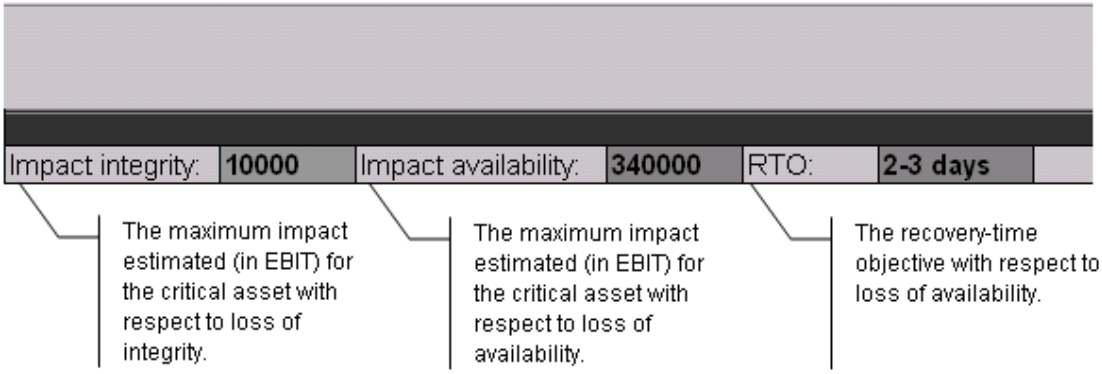


Figure 24. The figure visualizes a part of the Risk analysis Tool where required input is given.

There are a number of derived threat-scenarios based on the threat profile tree structures in appendix B and table summary. These scenarios are placed under their respective categories (see *Figure 25*) and each threat-scenario is pre-defined with the properties described in chapter 3.7.2 and an example to clarify the scenario. The examples given are quite general. For each scenario, one should state “Yes” or “No” in the “in scope” column to indicate if the scenario is applicable with respect to the critical asset, e.g. a physical binder (earlier assessed as a critical asset) containing confidential information is not a target for network-based attacks and such attack scenarios are consequently out of scope for that critical asset.

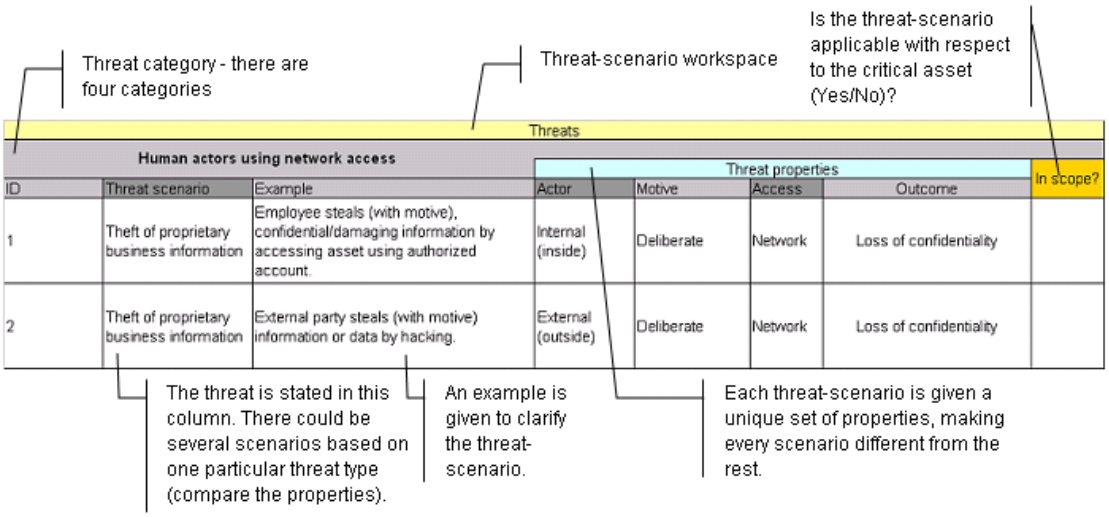


Figure 25. The figure visualizes a part of the Risk analysis Tool where the derived threat scenarios are described with their unique properties. These threat scenarios, altogether constitutes as the standard threat profile model. Each critical asset should be analyzed against every threat scenarios included.

Each threat-scenario must be evaluated by setting a threat-level and a vulnerability-level (see *Figure 26*). The threat-level is the probability of the threat occurring and the vulnerability-level describes the potential extent to which the threat will damage the business with respect to the critical asset being evaluated [Siemens DRA], in other words an estimated measurement of the extent of loss of the previously estimated maximum impact. Furthermore, each threat-scenario can only contribute with one outcome, loss of confidentiality, integrity or availability. This means that if a threat-scenario for example, has the outcome "Loss of confidentiality, then the risk-level calculation will automatically use the "Impact confidentiality" input (see *Figure 23*).

The critical asset should be evaluated against every potential threat-scenario. The end results are one threat-profile for each critical asset containing risk-levels for a number of "in scope" threat-scenarios in which the risk involved should be reduced immediately, managed, planned or simply accepted for the critical asset (see *Figure 26*).

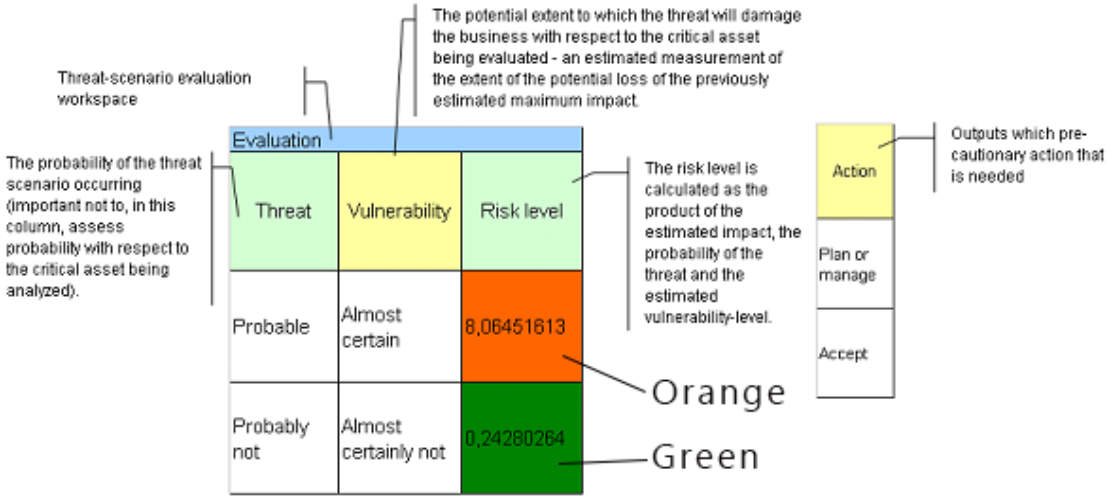


Figure 26. The figure visualizes a part of the Risk analysis Tool where for each scenario, determined as "in scope" should undergo a risk evaluation with respect to the critical asset being analyzed.

In order to assess threat-levels and vulnerability-levels, two classification tables have been developed in order to assist the BIA practitioners to select threat and vulnerability

levels. The threat classification table (see *Figure 27*) and vulnerability classification table (see *Figure 28*) is partly created based on [Siemens DRA], the WEP-table and the CiA-table from chapter 3.2.5.

Indicators	Almost certain	Probable	Chances about even	Probably not	Almost certainly not
Phrases of probability	Virtually certain Highly likely All but certain Odds overwhelming	Likely Probable	Chances about even	Unlikely Low probability	Extremely unlikely Virtually impossible Slight chance Little prospect Highly unlikely Highly doubtful
Probability	93% (give or take 6%)	75% (give or take 12%)	50% (give or take 10%)	30% (give or take 10%)	7% (give or take 5%)
Incidents to date	Very large number of incidents to date	Significant number of incidents to date	Moderate number of incidents to date	Few incidents to date	Extremely few or no incidents to date
Indications of threat-scenario ocurring	Clear signs of occurence	Several signs of occurence	One or two signs of occurence.	Few signs of occurence	No signs of occurence
Confidence in assessment	High confidence	High/medium confidence	Medium confidence	Medium/Low confidence	Low confidence
Expected occurence of threat	Expected within the next year	Expected within the next year or two	Expected within the next two or three years years	Expected within the next three to five years	Expected within the next nine to fifty years

Figure 27. The figure presents the threat classification table which provides indicators for each probability level (starting from "Almost certain" to "Almost certainly not"). The table is created to support decision making, for when estimating threat scenario probabilities.

The threat classification table (*Figure 27*) contains six indicators that could simplify the choice of an appropriate threat-level. There is no requirement that all six indicators must comply with respect to each other in order to select an appropriate threat-level, e.g. there could be clear signs of occurrence but the number of incidents to date may be significant or moderate and in such a case, one may choose the level "Almost certain", disregarding the other indicators. The vulnerability classification table (see *Figure 28*) consists of indicators with respect to probability of damage occurring, already implemented controls and pre-cautionary measures which could simplify the choice of an appropriate vulnerability-level. The same argument, regarding the indicators holds as for the threat-level indicators meaning that all indicators for one level do not necessarily need to comply.

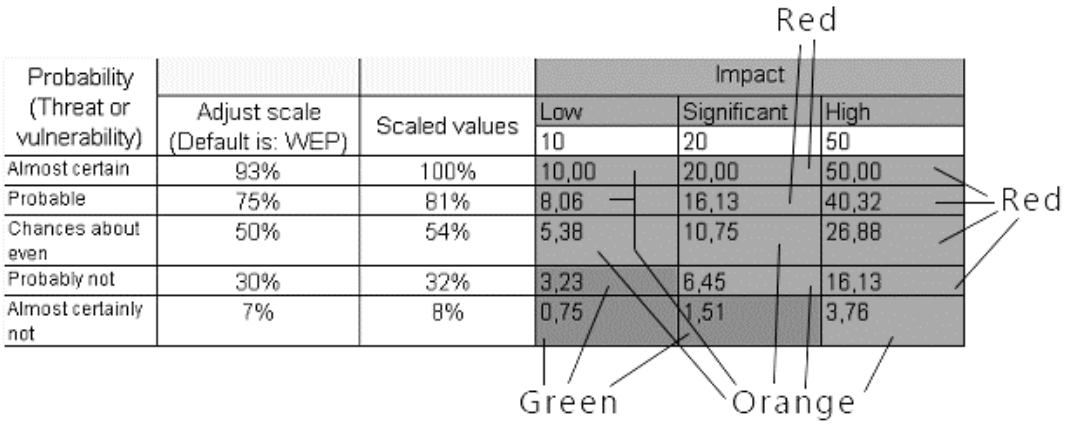
Indicators	Almost certain	Probable	Chances about even	Probably not	Almost certainly not
Pre-cautionary measures implemented	No pre-cautionary measures - damage virtually inevitable	Few pre-cautionary measures - damage probable	Some pre-cautionary measures - damage is possible	Significant pre-cautionary measures - minimal damage possible	Sufficient protection - damage is virtually impossible
Redundancy	Insufficent redundancy	Low redundancy	Some redundancy	Almost sufficient redundancy	Sufficient redundancy
Emergency/incident planning	No plans availabile	One or two plans available and never tested	Several plans available but not tested	Planning is nearly sufficient, plans have not been tested or tested to some extent	Planning is sufficient and have been fully tested
Impact of threat-scenario on damage to business	Expecting virtually the maximum possible damage	Expected damage is around 70 % of the maximum estimated damage	Expected damage is around 50 % of the maximum estimated damage	Expected damage is around 30 % of the maximum estimated damage	Expected damage is very little and/or negligible

Figure 28. The figure presents the vulnerability classification table which provides indicators for each probability of damage level (starting from "Almost certain" to "Almost certainly not"). The table is created to support decision making, for when estimating to what extent a certain threat scenario could damage a critical asset.

The risk-level is then estimated based on a 3x5 matrix, named within this process as the BIA decision matrix.

3.7.4 The BIA decision matrix

The BIA decision matrix decides how the levels of threat, vulnerability and impact together could be adjusted and interpreted with respect to a certain choice of scale of severity (the adjust scale which will be explained in the following) and pre-defined thresholds (see *Figure 30*) for risk-levels. The matrix and the method are based on [*17*] and give the BIA practitioners control over the BIA decision matrix such that the severity of each probability-level could be defined and adjusted as well as each risk-level, altogether providing control of the overall risk strategy.



Probability (Threat or vulnerability)	Adjust scale (Default is: WEP)	Scaled values	Impact		
			Low	Significant	High
			10	20	50
Almost certain	93%	100%	10,00	20,00	50,00
Probable	75%	81%	8,06	16,13	40,32
Chances about even	50%	54%	5,38	10,75	26,88
Probably not	30%	32%	3,23	6,45	16,13
Almost certainly not	7%	8%	0,75	1,51	3,76

Figure 29. The figure visualizes how decisions are made based on impact, threat scenario probability and vulnerability probability. The colors indicate if risk needs to be reduced (red color), managed or planned for (orange) or accepted (green).

The adjust-scale defines how each "Probability" is quantified (and consequently defining the severity of each level, and in this case quantification is made according to the WEP-table). If desirable this scale could be adjusted but changing the values in the scale will automatically change the severity of some or all risk-levels. For example, changing **only** (in its current state) the "Probably not" value from 30% to 20% (which could be interpreted as reducing the severity for "Probably not") will reduce the risk-level in the "High" column (same row) from red to orange. The colors define the strategy, meaning that the red color indicates a need to reduce the risk immediately, orange indicates the need to manage or plan for the risk and green indicates that the risk should be accepted. The threshold values (see *Figure 30*) define how the risk-levels, and consequently the colors are set (i.e. larger than 0.01 gives the green color, larger than 3.5 gives the yellow color and larger than 16 gives the red color), and are chosen based on the desired strategy accordingly (adjusted such that the colors fit the desired strategy presented in *Figure 31*). These values together with the adjust scale have been adjusted to achieve the desired strategy. Reducing for example the "red" value will contribute to the expression "less being more", meaning that if earlier estimated risk-levels resulted in the necessity to manage or plan for risks now would result in the necessity to reduce the risks immediately because we decreased the demand to achieve the reduce risk-level. Additionally, when adjusting these parameters (described) the BIA decision matrix will automatically change colors of the cells.

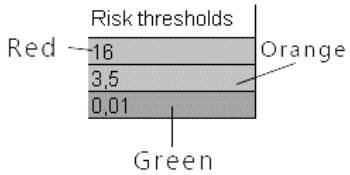


Figure 30. The risk threshold levels presented in the figure are adjustable parameters which will affect the overall strategy in the BIA decision matrix. The current numbers are chosen such that they comply with the desired strategy in Figure 31.

The scaled values column contains scaled percentage values [*17*] which are calculated for each probability-level by taking each respective value from the adjust scale (remember that quantification is made according to WEP) and then dividing that value with the highest value from the adjust scale (which in this particular case is 93%) and thus deriving scaled percentage values compatible with the decision matrix with respect to the assigned impact values (i.e. Low = 10, Significant = 20, High = 50 should be the upper starting levels for the most serious risk estimations). Each risk-cell is then calculated by multiplying each impact (10, 20 and 50) with each respective scaled percentage value.

The desired strategy is based on the previous decision matrix (used in previously performed BIA's and is part of Siemens corporate policy regarding preventive IT crisis management) and is used to define what pre-cautionary measures to take based on risk-levels. *Figure 31* demonstrates the desired strategy.

Impact / Probability	Low	High
High	Manage	Reduce
Low	Accept	Plan

Figure 31. The figure presented is the desired strategy of risk for SIT. E.g. If estimated impact is high and estimated probability (constitutes within this process as the product of threat probability and vulnerability probability, compare Equation 5 with Equation 6) is high then the desired strategy is to reduce the threat immediately.

As one can see the, the BIA decision matrix in *Figure 29*, follows the desired strategy demonstrated in *Figure 31*. For example low impact and almost certain probability (or "chances about even" or "probable") will demand the action to "Manage" the risk. The difference is that there are now probabilities to consider between "Low" and "High". However, the BIA decision matrix does not indicate if one should specifically manage or specifically plan for the risk (in the case of orange color indication). This is however something that one could make a judgment based on if impact is estimated as more tilting towards low or more tilting towards high. A low probability and high impact indicates that the risk should be planned for, in contrast to a low impact but high probability in which the risk should be managed (according to the desired strategy). It is however more difficult to consider a significant impact and a probability of 50% (phrase of probability converts to "chances about even"). In such a case it is assumed reasonable to choose manage or plan arbitrarily and freely. Furthermore, if estimating the lowest possible threat and vulnerability level (which is 0.49 %) will contribute with

the “accept” risk-level, regardless of if the impact is estimated as low, significant or high. With such low extremes (extremely low probabilities), the desired strategy is not fulfilled according to *Figure 31*.

3.7.5 Reduce, manage, plan or accept the risk

The pre-cautionary actions needed with respect to reducing the risk, managing the risk, planning for the risk or accepting the risk will be outlined partly according to Siemens corporate policy [*32*,*33*].

- In case the BIA practitioners estimated it necessary to reduce risk; actions are needed to be taken immediately without delay to reduce the risk by, as a suggestion, reducing vulnerability. By reducing the vulnerability, one could as earlier mentioned re-estimate the risk that remains and act accordingly (after reducing the risk, a certain risk may still remain in which one could manage or plan for the remaining risk if necessary).
- In case the BIA practitioners estimated it necessary to manage risk; actions are only needed during normal business operations to deal with the problem.
- In case the BIA practitioners estimated it necessary to plan for risk; actions are needed to develop a disaster recovery plan.
- In case the BIA practitioners estimated that the risk could be accepted; no actions are needed, the risk is negligible.

4 Results and conclusion

A process for performing a business impact analysis has been developed within the limitations of this project. Methods and tools have been developed and put in context in order to determine which assets that are critical to the company, how to analyze risk and how to determine the risk-levels needed in order to determine the appropriate risk strategy in order to perform pre-cautionary measures. The project has also included a list of assets determined as critical, they were derived in order to validate the data gathering method for the BIA.

4.1 Future work

Performing a comprehensive BIA requires a lot of work. The data gathering approach within this process requires updates to the already existing Deficiency Analysis. But even if such an update would be realized, there would still be potential issues when analyzing and compiling all that data. One suggestion is to develop a Business Continuity Management system [*34*], in which the data gathering process and the analysis process would become automated. Such a solution could reduce the time needed in order to identify critical assets and possibly reduce the time needed in all other or at least in some parts (such as analysis of the gathered data) of the BIA process described within this report.

References

[1] Siemens SIT, Process for Business Impact Analysis, 2008, Specification and proposal document for master thesis project.

[2] Andreas Malm. (2009, Feb.) Krisberedskapsmyndigheten. [Online]. http://www.krisberedskapsmyndigheten.se/upload/11148/kontinuitetsplaneringintroduction_priv-o__2007.pdf

[3] Swedish Security Service. (2009, Jan.) Official site of the Swedish Security Service. [Online]. http://www.sapo.se/download/18.7671d7bb110e3dcb1fd80009904/foretagsspionage32005.pdf

[4] Krisberedskapsmyndigheten. (2009, Feb.) Official site of Krisberedskapsmyndigheten. [Online]. http://www.krisberedskapsmyndigheten.se/upload/15713/rsa_likheter_och_skillnader_2007.pdf

[5] Doughty Ken, *Business Continuity Planning*. Florida, USA: Best Practices Series, 2001.

[6] Ronald L. Krutz and Russell Dean Vines, *The CISSP Prep Guide: Gold Edition*. Indianapolis, USA: Wiley Publishing, 2003.

[7] Siemens Business Services. (2005) Critical IT Resources (Business processes and applications) Method Description. PDF Document.

[8] Information Security Forum. (2004, June) Information Risk Analysis Methodologies (IRAM) project: Business Impact Assessment. PDF Document.

[9] The institute for continuity management (DRI). (2008, July) DRI International: Professional Practices. [Online]. https://www.drii.org/professionalprac/prof_prac_details.php

[10] Disaster Recovery Journal. (2007, Aug.) Disaster Recovery Journal: Generally Accepted Practices. [Online]. http://www.drj.com/index.php?option=com_content&task=view&id=761&Itemid=454

[11] Siemens Group. (2009, Jan.) Manual on Internal Control over Financial Reporting and Disclosure. PDF Document.

[12] Wikipedia. (2009, Apr.) Wikipedia. [Online]. http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

[13] Siemens Corporate Information Office. (2007, Nov.) Checklist for Deficiency Analysis. DOC document.

[14] JDBIGGS & Associates. (2008, Feb.) JDBIGGS. [Online]. http://www.jdbiggs.com/Downloads/tabid/61/Default.aspx

[15] Christopher Alberts and Audrey Dorofee. (2005, Oct.) CERT. [Online]. http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf

[16] Marshall D Abrams, "NIMS Information Security Threat Methodology," The MITRE Corporation, Virginia, Technical report 1998.

[17] Siemens Corporate Information Office. (2007, Sep.) Downtime Risk Assessment Methodology. PDF Document.

[18] SANS Institute InfoSec Reading Room. (2003, Dec.) SANS. [Online]. http://www.sans.org/reading_room/whitepapers/auditing/using_vulnerability

_assessment_tools_to_develop_an_octave_risk_profile_1353?show=1353.php&cat=auditing

[19] Wikipedia. (2009, May) Wikipedia. [Online]. http://en.wikipedia.org/wiki/Words_of_Estimative_Probability

[20] Central Intelligence Agency. (1964, Sep.) Central Intelligence Agency Library. [Online]. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays/6words.html

[21] Criminal Intelligence Service Canada. (2007) Criminal Intelligence Service Canada. [Online]. http://www.cisc.gc.ca/products_services/ita_methodology/document/ita_methodology_2007_e.pdf

[22] Office of Director of National Intelligence. (2007, Nov.) Office of Director of National Intelligence ODNI NEWS ROOM. [Online]. http://www.dni.gov/press_releases/20071203_release.pdf

[23] Wikipedia. (2009, May) Wikipedia. [Online]. http://en.wikipedia.org/wiki/Weasel_word

[24] Wikipedia. (2009, May) Wikipedia. [Online]. http://en.wikipedia.org/wiki/Words_of_Estimative_Probability

[25] Nancy A. Renfroe and Joseph L. Smith. (2008, May) WBDG Resource pages. [Online]. http://www.wbdg.org/resources/riskanalysis.php

[26] Google Definitions. Google. [Online]. http://www.google.se/search?hl=sv&defl=en&q=define:probability&ei=MMAdSvzCCZeQsAb21JTNCg&sa=X&oi=glossary_definition&ct=title

[27] Google Definition. Google. [Online]. http://www.google.se/search?hl=sv&defl=en&q=define:natural+event&ei=ecAdSrvhGMLesgbGz7DICg&sa=X&oi=glossary_definition&ct=title

[28] Räddningsverket. http://www.srv.se/. [Online]. http://www.raddningsverket.se/

[29] Madeleine Blixt, *En lokal uppföljnings- & prognosprocedur i problemorienterat arbete mot brott*. Stockholm, Sweden: Elanders Gotab AB, 2001.

[30] Bråttsförebygganderådet. Bråttsförebygganderådet statistikdatabas. [Online]. http://statistik.bra.se/solwebb/action/index

[31] Carol Woody, "Risk Methodology K-12," NOVA Southeastern University, Florida, PhD Thesis 2004.

[32] Siemens Corporate Information Office. (2006, Jan.) Preventive Crisis Management. Powerpoint.

[33] Siemens Corporate Information Office. (2007, Feb.) Policy "IT Disaster Recovery Planning". PDF Document.

[34] TechRepublic Newsfeed. (2006, Aug.) TechRepublic. [Online]. http://search.techrepublic.com.com/search/business+continuity+management+system.html

[35] Jeff Lowder. (2015, Februari) BlogInfoSec. [Online]. http://www.bloginfosec.com/2010/08/23/why-the-risk-threats-x-vulnerabilities-x-impact-formula-is-mathematical-nonsense/

Appendix A Identifying Critical Assets, Operations and Impacts

This chapter contains the created questionnaire and descriptions for all questions in the questionnaire. The questionnaire is used to gather data and information for when performing the BIA.

Critical Assets Identification Template	**Part of Business Division(s):** ☐ E S SO ☐ E S SU ☐ E S GT ☐ E S OS

E S SO: Service Division, E S SU: Steam Turbine Division, E S GT: Gas Turbine Division, E S OS: Oil and Gas Division.

A.1 Possible target group

The possible target group for identifying CA's should have knowledge within their respective business processes. The aim is not to analyze each business process, but to derive *Critical Assets (CA)* with respect to certain processes, sub-processes and/or business operation activities (classifiable as *Operations (O)*). It is however assumed that there exist circumstances in which the assets can't be bound to specific activities.

A.2 Type of asset

Select type of asset based on the various groups below. The selection can also be combinational. For example some information resource holding sensitive information could be classified as being a "Software/Information asset".

- **Systems assets** which include information systems that store information. The components of systems are software, information and hardware. Examples are networks, embedded systems (special purpose computer systems) and devices which supports Siemens Sit's IT-infrastructure.

- **Hardware assets** consisting of physical workstations and servers.

- **Information assets** which consist of electronic or paper documentation. Intellectual assets belong in this group. These are closely related to Systems which store, process and transmits critical information that drives the organization.

- **Software and services assets** consisting of applications which could be operating systems, database applications, custom applications or office applications. When for example identifying a software application, it is appropriate to thoroughly explain if the software as whole is the asset or the connected database.

- **Other resources** consisting of for example certain heavy machinery in the workshop.

- **Personnel** who carries important knowledge, training and experience.

A.3 Description of asset
Describe the asset, not too little detail and not to much detail (adequate granularity). The description should be with respect to your department and/or business division. In some cases it is necessary to combine assets, for example all workstations within some limited physical area could constitute as an asset.

A.4 Physical location
Describe the location of the asset if possible and applicable. If the asset is part of for example an IT-platform then mention which platform if not already done in question 2.

A.5 Loss properties
Information which could cause considerable damage if it were to fall into the wrong hands must be identified. Such damage can arise when for example competitors find out about the contents of an important bid or when strategic planning or business figures become known prematurely. Mark the **confidentiality** box if you answer yes to any of the following questions.

- Could the asset (or information held in by the asset) cause damage to Siemens SIT if disclosed to the wrong people (either accidentally or deliberately)?
- Has the asset (for example information) been classified as confidential or strictly confidential?
- Does the law (such as local data protection laws) require that the asset (for example data) be kept confidential?
- Will punitive measures be taken or recourse be sought in the event of the dissemination of the asset (for example information)?
- Will the prohibited, unwanted or premature publication of the sensitive asset (for example information) result in damage to the company?
- Can the dissemination of the confidential asset (for example information) weaken the company's competitive position?
- Can the asset (for example data) be used such that a third-party (e.g. competitors) could profit financially?
- Can the asset (for example information) potentially be used for illicit personal gain?

Information and data can be deleted and modified accidentally or maliciously. There are several threats. For example, fraudulent modification of accounts, and complete wipeout of hard drives by viruses. Mark the **integrity** box if you answer yes to any of the following questions.

- Is your department or division dependent on the consistency of the information held in by the asset?

- Would noticeable damage occur if decisions were to be made based on the asset being corrupt (for example corrupt data)?
- Can the asset (for example data) which affects financial performance be manipulated enough so as to cause immense financial damage?
- Does the law require data integrity?
- Given that the asset became corrupt; could it in an application result in errors in other applications?
- Can invalid or errored data result in lower product quality?
- Can financial damage occur as a result of the asset being corrupt (for example corrupt data)?

What would happen if services and resources became inaccessible, lost or destroyed? Would the business suffer if IT-systems, networks, workstations etc broke down for extended periods? Mark the **availability** box if you answer yes to any of the following questions.

- Is your department dependent on accessing the asset and being able to use it in order to continue functioning normally?
- Would the customers be affected if the asset (for example some information system) crashed?
- Are stockkeeping, production, sales or similar areas negatively affected by the asset (for example a system) failing?
- Are financial losses, for example due to delayed payments, incurred as a result of the asset (for example systems) failing?
- Can the asset (for example a system) failing result in insolvency or penalties?
- Are any deadlines endangered by extended asset (for example some system) failure?

A.6 Criticality

This is a criticality assessment. It provides a high-level view of the confidentiality, integrity and availability requirements of the asset to be determined and contributes with the possibility of comparing relative importance. Given the scale (low, significant and high), enter one of them in each box to indicate maximum possible level of harm. By selecting low criticality, you imply that the maximum damage would be somewhat unnoticeable, your department could continue in a normal fashion. By selecting significant criticality you imply that you don't know the maximum possible damage but can not rule out high damage. By selecting high criticality you estimate that the maximum possible damage could be high. In order to understand the meaning of high damage, one could compare it with approximately 5% of EBIT in loss.

A.7 Elaborate potential losses as described in A.5

Describe the asset with respect to the loss concepts, not too little detail and not too much detail (adequate granularity). Could you give some example scenario that has occurred? Are there any existing areas of concerns for which you have thought of as futuristic possibilities?

A.8 Part of *Operations (O)* (if applicable)

Which business process, sub-process or business operation activity (or activities) is/are directly supported by the asset (e.g. "1. The delivery process" – "2 with respect to availability. The sales process" or "1. All our core processes")? There are no restrictions on how to explicitly answer this question. One approach could be to explain it according to your department's process structure and point out which processes that are highly dependent on the asset for normal continuance and functioning.

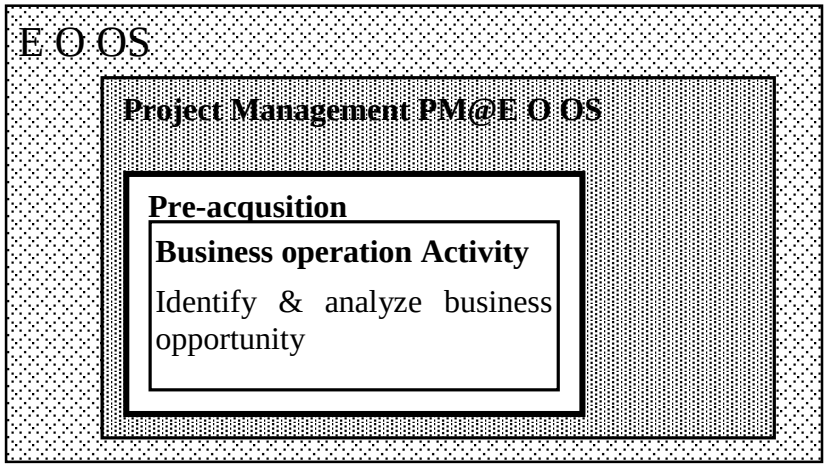


Figure 32. The figure presents an example of how to utilize Siemens SIT's business process structure in order to describe Operations. The example above identifies a business operation activity located within the sub-process "Pre-acquisition" which is located within the process "Project management" within the business division Service.

A.9 (Optional) What kind of pre-cautionary measures (controls), if any, exists for the asset, with respect to confidentiality, integrity and/or availability?
What controls already exists for the asset? How are confidentiality, integrity and/or availability protected?

A.10 Given loss of confidentiality, integrity and/or availability, with respect to potential dependent *Operations (O)* (if derived in 4) would result in…
In the scenario in which the asset became lost, stolen, falsified, rendered unavailable etc with respect to its security requirements, what type of losses can be expected? For each category, tick yes if applicable or not applicable. For each applicable impact type, tick confidentiality, integrity or availability if that particular loss is connected/related to the given loss concept. Also if answered question 4, write which Operations (O) that would be the source of the/connected to the loss *with respect to loss of availability* (tick availability). The following table shows some examples of each business impact type.

Table 11. The table contains business impact categories (marked in gray on the left) and respective business impact types under each category. On the right are examples for each impact type and how to measure each respective impact type (is located in parenthesis).

Business impact type/category	Examples of business impact type
Financial	
Loss of sales, orders or contracts	Sale opportunities missed, orders not taken or contracts that cannot be signed (Financial impact %).
Loss of tangible assets	Fraud, theft of money and lost interest (Financial impact EBIT€).

Penalties/legal liabilities	Breach of legal, regulatory or contractual obligations (Financial impact EBIT€).
Unforeseen costs	Recovery costs, uninsured losses, increased insurance (Financial impact EBIT€).
Operational	
Loss of management control	Impaired decision-making, inability to monitor financial positions, process management failure (Extent of loss of control).
Loss of competitiveness	Repetitive production line failures, degraded customer service, introduction of new pricing policies (Targets underachieved %).
New ventures held up	Delayed new products, delayed entry into new markets, delayed mergers/acquisitions (Extent of delay time).
Breach of operating standards	Contravention of regulatory standards, quality or safety standards (Extent of sanctions imposed).
Customer-related	
Delayed deliveries to customers or clients	Failure to meet product delivery deadlines, failure to complete contracts on time (Extent of delay time).
Loss of customers or clients	Customer/client defection to competitors, withdrawal of preferred supplier status by customer/client (% of customers lost).
Loss of confidence by key institutions	Adverse criticism by investors, regulators, customers or suppliers (Extent of loss of confidence).
Damage to reputation	Confidential financial information published in media, compromising internal memos broadcast by media (Extent of negative publicity).
Employee related	
Reduction in staff morale/productivity	Reduced efficiency, lost time, job losses (Extent of loss of morale/productivity).
Injury or death	Harm to staff, customers or suppliers associated with the organization (Number of incidents).

Table 12. The table contains the Critical Asset Identification Template questionnaire. These questions were used in the interviews conducted to gather assessment data and to validate the questionnaire. Each question if referred to the paragraphs above for clarification (e.g. see A2).

1. Type of asset (***see A2***)			
System asset	☐ Yes ☐ No	Hardware asset	☐ Yes ☐ No
Information asset	☐ Yes ☐ No	Software or service	☐ Yes ☐ No
Personnel asset	☐ Yes ☐ No	Other resource	☐ Yes ☐ No
If other, specify			

2. Description of asset with adequate granularity (***see A3***)

Physical location (if applicable, ***see A4***)			
Loss properties (***see A5***)	☐ Confidentiality	☐ Integrity	☐ Availability

3. Criticality (Only answer if C, I or A is ticked in "Loss properties") – Approximately, what is the maximum level of harm that the business could suffer if key information held in, processed or transmitted by the information resource were to be accidentally or deliberately (***see A6***):
Use the following scale to mark each box: L (the maximum level of harm is **Low**) – S (The maximum level of harm is somewhat uncertain, and thus **Significant**) – H (the maximum level of harm is **High**)

Disclosed to the wrong people:		Loss of confidentiality
Falsified or otherwise corrupted:		Loss of integrity
Rendered unavailable for:		
One hour		Loss of availability
A day		
2-3 days		
A week		
A month		

4. Elaborate potential losses as described in A5 (***see A7***)

5. Part of *Operations (O)* **(highly recommended if applicable, see A8)**

6. What kind of pre-cautionary measures (controls), if any, exists for the asset, with respect to confidentiality, integrity and/or availability? (***see A9***)	
7. Given loss of confidentiality, integrity and/or availability, with respect to potential dependent *Operations (O)* **(if derived in question 4)** would result in (***see A10***):	
Financial	
Loss of sales, orders or contracts C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Loss of tangible assets C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Penalties/legal liabilities C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Unforeseen costs C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Operational	
Loss of management control C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Loss of competitiveness C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
New ventures held up C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Breach of operating standards C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Customer-related	
Delayed deliveries to customers or clients C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Loss of customers or clients C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Loss of confidence by key institutions C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Damage to reputation C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Employee-related	
Reduction in staff morale/productivity C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable
Injury or death C☐ I☐ A☐	*Operations (O) (**if yes and A-loss**):* ☐ Yes ☐ No ☐ Not applicable

Appendix B Threat profile trees

This chapter contains OCTAVE threat profile categories. Some are unmodified standard categories and some are modified.

B1 Human actors using network access

The following threat profile tree is generic for humans using network access. Threats with human actors using network access can be analyzed with the tree in order to derive a number of possible unique threat scenarios. One first needs to identify a specific threat, for example "Theft of proprietary business information". By looking at the tree structure we can identify two different threat scenarios. One in which the perpetrator works from within the company and causes the outcome "Loss of confidentiality" and another scenario in which the perpetrator is some external party, stealing the information from outside the company (hacking the network). There are no other scenarios based on the tree structure. For example, the threat could not be accidental because it explicitly states "Theft" and it could not cause the loss of availability or loss of integrity because the perpetrator is after stealing the information, and not causing any other problems.

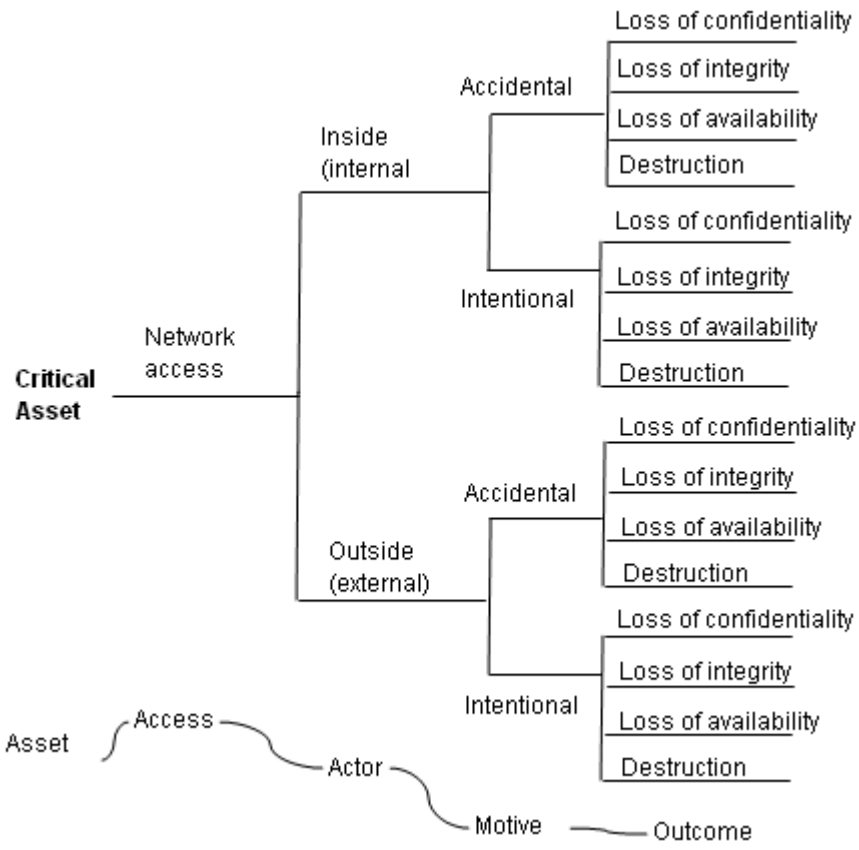


Figure 33. This figure presents the threat profile category "Human actors using network access".

B2 Human actors using physical access

The following threat profile tree is generic for humans using physical access. Threats with human actors using network access can be analyzed with the tree in order to derive a number of possible unique threat scenarios. This category is basically the same as the previous in appendix chapter B1. The only difference is that the access property states "Physical access". Using the same threat example used in B1, contributes with two scenarios by looking at this tree structure. Furthermore, the outcome "Destruction" is only a supplement property which could be used to mark that a specific threat involves physical destruction of an asset, but can only be used in combination with one of the other outcomes. For example, let us say that one would like to analyze the threat "Employee intentionally causing server failure". The employee could physically smash a server causing the outcome "loss of availability". To mark that physical damage to server is involved; the "Destruction" outcome would supplement the overall outcome of the threat.

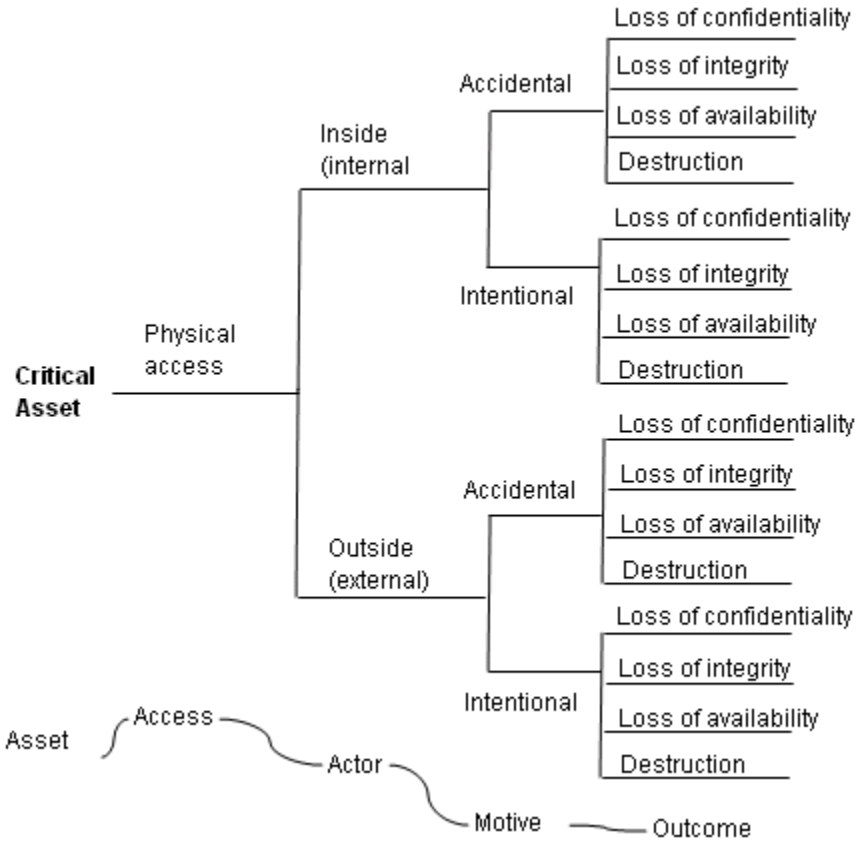


Figure 34. This figure presents the threat profile category "Human actors using physical access".

B3 System and other resource problems

The following threat profile tree is a modified generic tree for systems and other resource problems. The generic category (unmodified) is originally named "System problems" and treats information systems [threat profile trees]. Within this process, this category has been extended to also support technical (malfunctions) problems of for example heavy machinery, going beyond information systems. As a result of this, the name of the category was changed from "System problems" to "System and other resource problems". Furthermore, the original generic category did not include the "motive" property. That has been modified within this category. The motive property has been included to indicate that the category treats threats that are of accidental nature (meaning accidental circumstances). For example, the threat "Malfunctions of software and services developed in-house" fits within this category and five scenarios can be derived by looking at the tree structure (following the actors "Software defects", "Hardware defects", and "Malicious code" with the latter actors contributing with three different and unique scenarios based on differing outcomes). All of these applicable scenarios indicate that the threat is non-malicious. Even the actor "Malicious code" is followed by the motive "Accidental" in order to indicate that the malicious code causing the outcome exists by accident (e.g. accidentally written by well-intentioned employee).

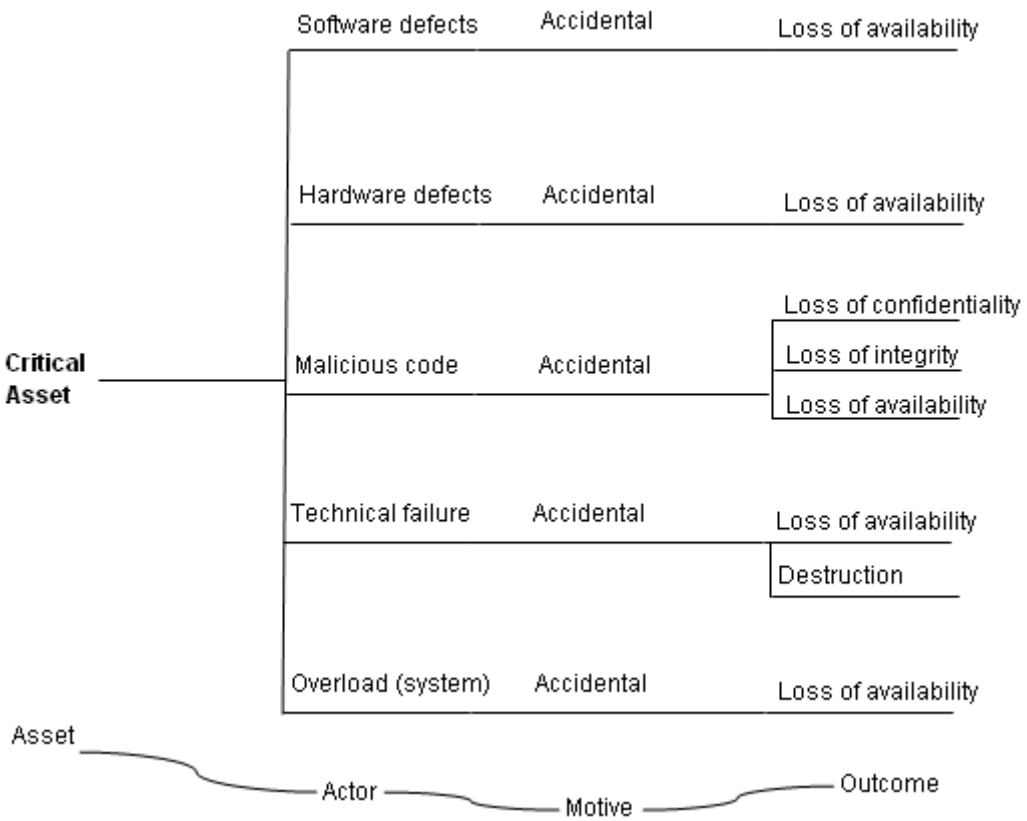


Figure 35. This figure presents the threat profile category "System and other resource problems".

B4 Other problems

The following threat profile tree is a modified generic tree for the "other problems" category [threatprofiles]. This category has also been extended. The category originally treats threats that are outside the control of an organization, meaning for example natural disasters. The source of this analysis, [threat profiles] is a bit unclear regarding what "outside the control of the organization" explicitly refers to. For example, in the generic tree "fire" is included in one of the actors "Natural disasters", but it is unclear if the authors are referring to fire outside the organization or accidental fire occurring and beginning from within an organization. It is however assumed, because referring to "out of organizational control" that they refer to fire occurring outside an organizations physical perimeter. However, this category has been extended to also include, for example fires occurring accidentally within Siemens SIT as well-as outside by introducing a new actor named "Internal disaster". Furthermore, some actors were removed from this category (compare this tree with [threat profile]) because they are covered in previously mentioned categories (which were modified).

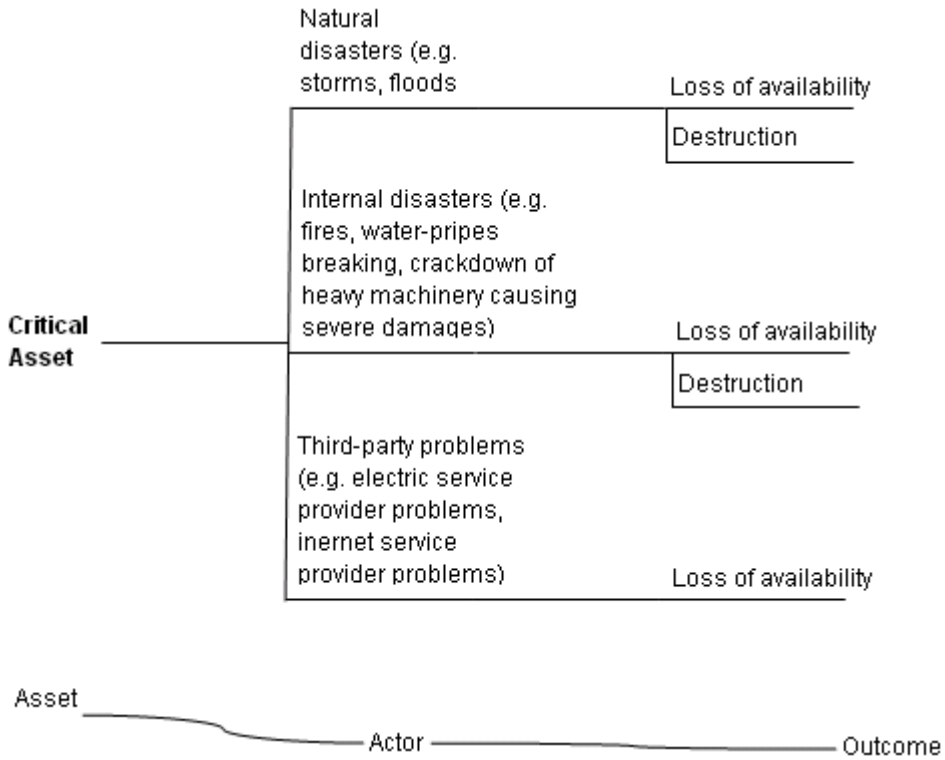


Figure 36. This figure presents the threat profile category "Other problems".

Appendix C Threat-profile summary

Threats								Evaluation			
Human actors using network access			Threat properties				In scope?	Threat	Vulnerability	Risk level	Action
ID	Threat scenario	Example	Actor	Motive	Access	Outcome					
1	Theft of proprietary business information	Employee steals (with motive), confidential/damaging information by accessing asset using authorized account.	Internal (inside)	Deliberate	Network	Loss of confidentiality				#VALUE!	#VALUE!
2	Theft of proprietary business information	External party steals (with motive) information or data by hacking.	External (outside)	Deliberate	Network	Loss of confidentiality				#VALUE!	#VALUE!
3	Distributing computer viruses (and worms).	Employee have been traveling with laptop which have been infected with virus/worm and returns to office in which virus/worm infects other assets and causing disclosure.	Internal (inside)	Accidental	Network	Loss of confidentiality				#VALUE!	#VALUE!
4	Distributing computer viruses (and worms).	Employee have been traveling with laptop which have been infected with virus/worm and returns to office in which virus/worm infects other assets and causes modification/corruption.	Internal (inside)	Accidental	Network	Loss of integrity				#VALUE!	#VALUE!
5	Distributing computer viruses (and worms).	Employee have been traveling with laptop which have been infected with virus/worm and returns to office in which virus/worm infects other systems and interuppts the asset.	Internal (inside)	Accidental	Network	Loss of availability				#VALUE!	#VALUE!
6	Distributing computer viruses (and worms).	Disgruntled employee spreads virus/worm which causes disclosure of information/data.	Internal (inside)	Deliberate	Network	Loss of confidentiality				#VALUE!	#VALUE!
7	Distributing computer viruses (and worms).	Disgruntled employee spreads virus/worm which causes modification/corruption of data/info.	Internal (inside)	Deliberate	Network	Loss of integrity				#VALUE!	#VALUE!
8	Distributing computer viruses (and worms).	Disgruntled employee spreads virus/worm which causes interruption.	Internal (inside)	Deliberate	Network	Loss of availability				#VALUE!	#VALUE!
9	Distributing computer viruses (and worms).	External party accidentally spreads virus/worm (e.g. by email) to Siemens SIT and causing disclosure of data/info.	External (outside)	Accidental	Network	Loss of confidentiality				#VALUE!	#VALUE!
10	Distributing computer viruses (and worms).	External party accidentally spreads virus/worm to Siemens SIT and causing modification/corruption of data/info.	External (outside)	Accidental	Network	Loss of integrity				#VALUE!	#VALUE!
11	Distributing computer viruses (and worms).	External party accidentally spreads virus/worm to Siemens SIT and causing interruption.	External (outside)	Accidental	Network	Loss of availability				#VALUE!	#VALUE!
12	Distributing computer viruses (and worms).	External party deliberately spreads virus/worm to Siemens SIT and causing disclosure of data/info.	External (outside)	Deliberate	Network	Loss of confidentiality				#VALUE!	#VALUE!
13	Distributing computer viruses (and worms).	External party deliberately spreads virus/worm to Siemens SIT and causing modification/corruption of data/info.	External (outside)	Deliberate	Network	Loss of integrity				#VALUE!	#VALUE!
14	Distributing computer viruses (and worms).	External party deliberately spreads virus/worm to Siemens SIT and causing interruption.	External (outside)	Deliberate	Network	Loss of availability				#VALUE!	#VALUE!
15	Modifying software or inserting software without authorization	Employee/internal personnel deliberately changing software to produce unauthorized system behavior of actions, for example creating backdoor in order for thirdparties to get access or ensuring access after employment.	Internal (inside)	Deliberate	Network	Loss of confidentiality				#VALUE!	#VALUE!
16	Modifying software or inserting software without authorization	Employee/internal personnel deliberately changing software to produce unauthorized system behavior of actions, for example, with time causing inconsistencies for data/info.	Internal (inside)	Deliberate	Network	Loss of integrity				#VALUE!	#VALUE!
Human actors using physical access											FALSE
17	Theft of proprietary business information	Employee/internal personnel steals (with motive) confidential/damaging information by accessing the asset physically (for example binder) and causing disclosure.	Internal (inside)	Deliberate	Physical	Loss of confidentiality				#VALUE!	#VALUE!
18	Theft of proprietary business information	External party steals (with motive) confidential/damaging information by accessing the asset physically (for example binder) and causing disclosure.	External (outside)	Deliberate	Physical	Loss of confidentiality				#VALUE!	#VALUE!
System and other resource problems											FALSE
19	Malfunctions of software and services developed in-house.	Incorrect execution or failure of software developed or integrated in-house (e.g. software bug).	Software defects	Accidental		Loss of availability				#VALUE!	#VALUE!
20	Malfunctions of software and services developed in-house.	Incorrect execution or failure of software developed or integrated in-house (e.g. overheating of server or component failure causing software or service to fail).	Hardware defects	Accidental		Loss of availability				#VALUE!	#VALUE!
21	Malfunctions of software and services developed in-house.	Incorrect execution or failure of software developed or integrated in-house (accidental creation of malicious code).	Malicious code	Accidental		Loss of confidentiality				#VALUE!	#VALUE!
22	Malfunctions of software and services developed in-house.	Incorrect execution or failure of software developed or integrated in-house (accidental creation of malicious code).	Malicious code	Accidental		Loss of integrity				#VALUE!	#VALUE!
23	Malfunctions of software and services developed in-house.	Incorrect execution or failure of software developed or integrated in-house (accidental creation of malicious code).	Malicious code	Accidental		Loss of availability				#VALUE!	#VALUE!
24	Technical failure of important and costly machinery.	Machinery in the workshop breaks or fails immensely.	Technical failure	Accidental		Loss of availability				#VALUE!	#VALUE!
25	System overload	System unable to handle exessive traffic (e.g. due to exessive volume of traffic).	Overload	Accidental		Loss of availability				#VALUE!	#VALUE!
26	Power supply failure	Power supply failure from within (internally).	Technical failure	Accidental		Loss of availability	Yes			#VALUE!	#VALUE!
Other problems											FALSE
27	Extreme rainfall	Extreme rainfall causing road inaccessibility, telecommunication disruptions and/or electronic disruptions.	Natural disaster			Loss of availability				#VALUE!	#VALUE!
28	Storm	Severe storm causing road inaccessibility, telecommunication disruptions and/or electronic disruptions.	Natural disaster			Loss of availability				#VALUE!	#VALUE!
29	Flooding	Severe precipitation causing rivers, lakes and other water buffers to increased water levels, causing flooding. Damages to real estate and infrastructure (including interruption of electric and telecommunications).	Natural disaster			Loss of availability				#VALUE!	#VALUE!
30	Fire in buildings	Some accidental circumstance causing severe fire in building.	Internal disaster			Loss of availability				#VALUE!	#VALUE!
31	Loss of power	Power supply failure from electric company (interdependency failure).	Third-party problems			Loss of availability				#VALUE!	#VALUE!

Figure 37. The figure presents the Risk analysis tool which includes the standard threat profile model containing the threat scenarios derived.