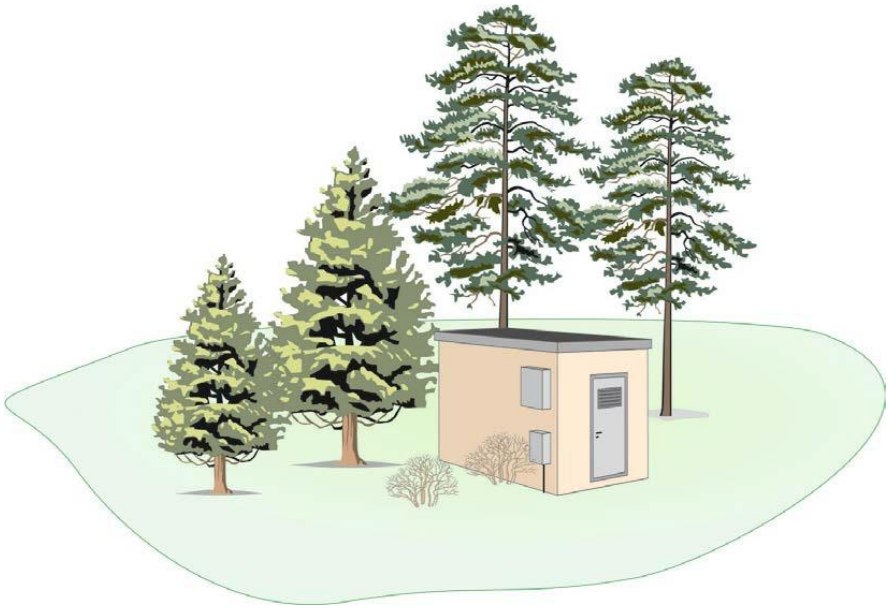
Robust fiber

# Robust sites for digital critical infrastructure protection

## Sub-appendix 4.1.2 Routine and guidance for Risk and vulnerability analysis (RSA)

### Ver 1.3.2



# CONTENTS

# 1. INTRODUCTION

This document constitutes a routine and a guide for Risk and Vulnerability Assessments (RSA) regarding Robusta sites for socially important digital infrastructure.

Note. Names and designations that may be unique to different network owners are indicated by (company-specific).

# 2. REFERENCES

## 2.1 Reference document

The following reference documents must be prepared before the work with risk and vulnerability analyzes is carried out.

| Referencs | Document number, date |
|---|---|
| Business analysis (company specific) | |
| Documentation and classification of sites and nodes (company-specific) | |
| Summary Incident reports (company specific) | |

## 2.2 Audit history

| Utgåva | Datum | Handläggare | Beskrivning |
|---|---|---|---|
| Ver 0.1 | 2020-07-03 | J Persson | Sub-appendix to 4.1 Robusta siter … |
| | | | |

# 3. SCOPE AND PURPOSE

## 3.1 Scope

The analyzes shall include:

- Identification of all relevant threats to the site in question and its assets.
- Qualified assessment of consequences in the event of identified risk occurring.
- Qualified assessment of the probability of identified risks occurring.
- Qualified weighted assessment of the probability of identified risks occurs and the consequences it may cause if they occur (risk assessment).
- Proposed measures for identified risks.

When conducting risk analyzes, contractors must take into account experiences from previous incidents.

## 3.2 Purpose

The purpose of risk and vulnerability analyzes is to reduce the vulnerability of the company's electronic communications network and electronic services.

# 4. BOUNDARIES

The risk and vulnerability analyzes in this document do not concern:

- customers' equipment or their handling / action,
- the operating and management organization's internal systems and resources,
- planned changes that affect a smaller number of active connections.

# 5. RECYCLING RSA

At least once a year, a review and assessment must be made of and whether changes in the external environment and / or technical environments affect the electronic communications network and the electronic services and thus the need for renewed risk and vulnerability analyzes. This risk assessment must be a balance between what may occur, what consequences this may have and how likely it is that it will occur. The risk assessment must be in writing. An ongoing schedule shall be established for recurring RSA.

# 6. PLANNED CHANGES

In the event of changes in the company's electronic communications network and / or electronic services, a risk assessment must be carried out. This risk assessment must be a balance between what may occur in terms of functional impact, what consequences this may have and how likely it is that it will occur.

The method for the risk assessment is the same as for recurring RSA with the addition that the risk assessment must be in writing and be available before the change is implemented. This applies to both the change introduced in the facility and the job itself. Execution technicians or clients are responsible for carrying out a risk assessment.

# 7. CONFIDENTIALITY

The risk and vulnerability analyzes must be classified as "Internal". Internal means that the information must only be available to those who need the information in order to be able to fulfill their obligations regarding ownership, operation and management of analyzed assets and relationships.

# 8. AUDIT AND LIABILITY

The risk and vulnerability analysis is revised once a year or when significant changes have been made in the electronic communications network and / or the electronic services. The operations manager is responsible for ensuring that this is done.

# 9. MANUAL RISK AND VULNERABILITY ANALYSIS

## 9.1 General

The risk and vulnerability analysis must clarify the causes and effects of various types of events that may adversely affect the functionality of the networks and services. The purpose is to increase awareness of one's own risks, vulnerabilities and the ability to resist them, as well as provide a basis for any possible improvement measures that can be taken to prevent disturbances and interruptions.

Risk analyzes can be done in many different situations and at many different levels. For a business as a whole, for a special information asset, for a specific application, for a server hall, for a business process and so on. This tutorial focuses on the electronic communications network.

There are many different methods for doing a risk analysis and it is largely a craft that simply must be performed by the people who know how the fiber networks are laid out, how operation and maintenance are managed and have knowledge of the management of networks and services. Having good knowledge of the surroundings and the risks that these can pose to the functionality of the fiber networks is also important when a risk analysis is performed.

## 9.2 Preparations

In order for the results of the risk and vulnerability analysis to be good and lead to correct preventive measures and improvement measures, preparations are required.

### 9.2.1 Analysis group

An analysis leader must be appointed who then leads the analysis group that is put together to carry out the risk and vulnerability analysis.

The analysis leader should be aware of:

- How the business and the object of analysis work on an overall level.
- How the method works
- Who should be included in the analysis group
- What documentation is needed for the analysis
- What result is expected

Experts of various kinds may be needed in the group, for example technicians, security coordinators, economists and lawyers.

The size of the analysis group can vary but should not be more than eight participants as it can be difficult to handle.

A documentation manager should be appointed and is the one who holds the pen or IT support, and who must know the method and the aids used in the analysis.

Before a risk analysis, it is important to have access to the information needed to solve the task. The task of the analysis leader is to ensure that the members of the analysis group have prepared for this and have found out all the necessary facts.

Necessary information prior to the risk and vulnerability analysis is:

- Constitutional requirements, regulations and other governing documents that can directly affect the risk analysis.
- Statistics that facilitate the analysis group's assessment.
- Similar risk analyzes that can be of great value to the work.
- General threat images that can be of support and help in identifying threats.
- Documents and documentation that describe current assets and connections.

### 9.2.2 Local and equipment:

- Good if there is a whiteboard and / or flipchart.
- Good if there is computer support and projector.
- Feel free to choose a room with a good environment where you can work undisturbed.
- Print or write down concepts and definitions visible in the room.
- Print or draw the matrix in a suitable size.

### 9.2.3 Time planning

Develop a realistic schedule for the analysis work. Some parts may turn out to take longer than expected, but it is still important to have a "basic schedule" to fall back on to be safely completed on time.

Set aside time for several short breaks, but make sure that the participants do not run away and work on other things during the breaks. The focus of the analysis group is absolutely decisive for the result.

Example of schedule for the analysis:

- Introduction with presentation of the participants 5–10 minutes
- Review and description of the method 10–20 minutes
- Description of selected analysis object 10–30 minutes
- Review hot list, add, delete, describe 30–60 minutes
- Risk assessment - consequence and probability 120–240 minutes
- Preparation of proposed measures 30–60 minutes
- Compilation of report 60–240 minutes

The time schedule for an RSA can be very variable depending on the object and the analysis group's level of ambition.

## 9.3 Method for RSA

The method presented in this document describes how to systematically identify various adverse events, assess how likely it is that the events will occur, assess the immediate negative consequences, analyze the vulnerabilities of the electronic communications network and services and assess the ability to handle various stresses.
The method is based on the requirements of the 27001 standard and on data from MSB (the Swedish Agency for Civil Protection and Emergency Planning).

### 9.3.1 Before implementation

Experience shows that the methodology is not the difficult part of an analysis, but the administration. Therefore, it is very important to follow up that the participants are prepared and have set aside time for the analysis.
Before carrying out risk and vulnerability analyzes, it is also necessary to establish certain starting points that will form the basis for further analysis work. In summary, the starting points of the risk and vulnerability analysis should clarify:

**Role and area of responsibility**
Operations manager and administration managers for the analysis objects as well as, depending on the analysis objects, experts such as technicians, safety coordinators, economists and lawyers.

**Delimitations and perspectives**
It is also important to understand the concepts of risk and vulnerability in order to be able to set correct boundaries and start from a correct perspective. The following definitions have been taken from PTS, the Swedish Post and Telecom Agency's Risk and Vulnerability Analysis for the electronic communications sector in 2015.

Risk = The effect of uncertainty on goals
Risk analysis = Process for understanding the nature of the risk and for determining the level of risk.
Vulnerability = Critically dependent on an asset or lack of protection of an asset exposed to threats.
Resulting vulnerability = Vulnerabilities remaining after the imposition of safeguards

## 9.3.2 Parts of the method

When the analysis group is assembled, the analysis is carried out using the following steps, which are described in more detail under each point and in Chapter 9.4.

- **Select and describe analysis objects**
- **Identify threats**
- **Classification model**
- **Carry out a risk analysis**
- **Compilation and report**
- **Action plan - action list**
- **Risk management**
- **Continuity planning**

#### *9.3.2.1 Select and describe analysis objects*

The first step in the work with a risk and vulnerability analysis is to select and describe the object for the analysis, the description must be concise but clear enough for others to understand outside the analysis group.

Current objects consist of defined assets and liabilities in accordance with the document Documentation and classification of all assets and liabilities (company-specific).

#### *9.3.2.2 Identify threats*

An important step is to identify the threats that exist against the objects of analysis. In PTS Risk and Vulnerability Analysis for the Electronic Communications Sector 2015, there is an overview of threats based on SS-ISO / IEC 27005: 2008. The table is a good starting point for further work and includes most threats that are also relevant for a city network.

Based on the scope of the electronic network, a selection is made of which threats can be considered relevant and these will then form the basis for the risk and vulnerability analyzes. The selection of base threats should be made for each new analysis object. See figure 1 Table bashot below.

If you want to identify the threats yourself, you can use "brainstorming" where each participant on a piece of paper writes down threats that may occur or things that have already happened. All threats are then collected and reviewed.

It is important that participants try to describe the threats so that everyone understands. It will then be easier to assess the risk in the next steps. Everyone must understand and agree on the meaning of the threats.

When working with identifying threats, keep the following in mind:

- Listen extra carefully to the people who work actively with the business concerned.
- What has happened that can happen again?
- Focus on the threats - avoid thinking in solutions!
- Avoid too long discussions about the existing protection.
- Let everyone have their say.
- Experts must remember to speak so that everyone understands.

***Grouping of threats***

With the help of the analysis leader, the group will try to describe the threats in a structured way. The goal is to group similar threats with each other, remove duplicates and clarify certain threats if necessary.

*Figure 1. Table of base threats.*

| Sheet name | | Definition of the threats that form the basis for the predefined threat tabs in the workbook | |
|---|---|---|---|
| Prefix | Index | Group | Threats |
| FS | 1 | Physical damages | Fire |
| FS | 2 | | Water damage |
| FS | 3 | | Contamination (such as radiological or biological contamination) |
| FS | 4 | | Major accident occurs (S) |
| FS | 5 | | Destruction or theft of equipment |
| FS | 6 | | Dust, corrosion and freezing |
| FS | 7 | | Excavation of cables |
| SF | 1 | Errors in support functions | Loss of functions for indoor climate (heating, air conditioning, cooling) |
| SF | 2 | | Loss of power supply including manual disconnection in power shortage situations |
| SF | 3 | | Deficiencies or errors in troubleshooting functions (alarms, monitoring, etc.) |
| EO | 1 | Electromagnetic or thermal causes | Electromagnetic radiation including antagonistic threats such as active interference, electromagnetic pulse (EMP) and space weather |
| EO | 2 | | Conductive disturbances |
| EO | 3 | | Thermal radiation |
| EU | 1 | PTSFS 2020: 1 Risk analyzes specially selected | Weather |
| EU | 2 | | Intrusion |
| EU | 3 | | Sabotage |
| EU | 4 | | Other external influences |
| EU | 5 | | Information provided by the Swedish Post and Telecom Agency about threats |
| LH | 1 | Logical Threats | Listening to information |
| LH | 2 | | Theft of information |
| LH | 3 | | Disclosure of sensitive information (such as position information or other information worthy of protection) |
| LH | 4 | | Receiving and using information from unreliable sources |
| LH | 5 | | Manipulation of networks, hardware and software through IT-related attacks such as viruses, worms, Trojans and congestion attacks targeting critical logical functions such as border routing and DNS. |
| TF | 1 | Technical errors | Faults in equipment where the intended capability is lost or not achieved |
| TF | 2 | | Network and hardware overload |
| TF | 3 | | Loss of ability to monitor and control information assets and network functions |
| OH | 1 | Unauthorized handling | Unauthorized use of equipment |
| OH | 2 | | Unauthorized copying of software |
| OH | 3 | | Corruption of information assets |
| OH | 4 | | Illegal or illicit (within your own organization) handling of information |
| FK | 1 | Errors or omissions in critical functions | Improper use of equipment |
| FK | 2 | | Inaccessibility for staff |
| FK | 3 | | Presence of deficiencies in preventive work, including deficient routines when upgrading software |
| FK | 4 | | Existence of shortcomings in management functions (crisis and business management) |
| FK | 5 | | Deficiencies in network monitoring |

### *9.3.2.3 Classification model*

In order to be able to assess the risk of a threat, a balance is made between the consequence of the threat occurring and an assessment of the probability that the threat will occur. To do this, it is required that the criteria for consequences and probability are defined and described so that everyone in the analysis group understands and agrees on the meaning.

The probability indicates how likely it is that the threat will occur according to the following categories with examples of definitions of the criteria:

- **Very low**
  *The event is not expected to occur in the next 20 years alternative Once in 20 years or non-existent probability that the event will occur at all.*

- **Low**
  *The event is not expected to occur in the next 10 years or once in 10 years or very rarely.*

- **Average**
  *The event can occur alternatively Once in 5 years or rarely.*

- **High**
  *The event will most likely occur alternatively annually or regularly,*

- **Very high**
  *The event will almost certainly occur alternatively More than once a year or often.*

The consequence is a measure of how much the business is damaged if the threat becomes a reality. Influence can, for example, be direct or indirect, financial or humane. The model contains the following five levels with examples of definitions of the criteria:

- **Very low**
  *If the event occurs, it is unlikely that the event will have negative consequences or negligible damage.*

- **Low**
  *If the event occurs, it is possible that the event will have negative consequences or moderate damage.*

- **Average**
  *If the event occurs, it is almost certain that the event will have negative, simpler consequences and may be a moderate injury.*

- **High**
  *If the event occurs, it is likely that the event will have negative consequences can be a significant injury.*

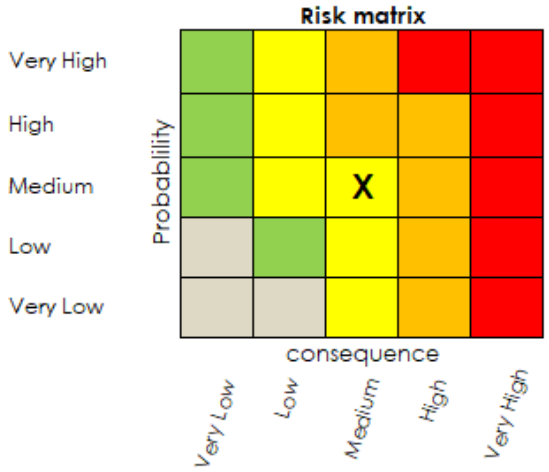
- **Very high**
  *If the event occurs, it is almost certain that the event will have negative consequences and could be a serious injury.*

The definitions of consistency and probability are a benchmark and can be changed, and it is important that the group goes through the definitions and changes if necessary. Any changes must be documented and included in the final report.

#### 9.3.2.4 *Risk analysis*

When all criteria for probabilities and consequences have been determined, the analysis group must assess the risk (consequence and probability) of a threat, eg by using a Consequence and probability matrix (Fig. 2) where colors indicate the severity of a threat occurring, from green (acceptable risk to red (must be remedied) The results of the matrix may later form the basis for, among other things, the prioritization of various measures.

Figure 2. Consequence and probability matrix




#### 9.3.2.5 *Compilation and report*

The results are then taken care of by the analysis manager who compiles a final report. In addition to the analysis result itself, it is important that the report contains all conceivable information, all deviations that the group has made from the analysis object and any new definitions. The report may also include other important information, such as control documents, product descriptions and drawings that are valuable to the result.

It is important to write a good and concise summary that in a simple way describes the risks that the analysis group has found. The compilation shall also contain any proposals for measures and recommendations to the person who is to make the decisions.

The report may contain general parts for different types of facilities and specific parts for individual facilities with a special threat picture.

The completed final report will be sent out for "consultation" to the participants, who will be given the opportunity to give their views.

## 9.4 Risk management and continuity planning

### 9.4.1 Risk management

With the risk analysis as a starting point, an assessment is made as to whether the risk should be limited by protective measures or whether it should be accepted and managed in the continuity plan. Proposals for measures must be documented in a document, Action plan risk analysis, where a risk manager is specified and, if possible, an estimated cost for each measure.

There are two ways to work with the measures.

**Option 1: The risks must be managed later**
An alternative is that the risks should not be met with any measures yet, but only prepared by documenting how the threat is to be handled if it should occur, ie a continuity planning, see section 9.4.2. But if the participants have good suggestions for measures, you can still document them.

**Option 2: The risks must be managed now**
The second option is to take care of the risks at once. The developed matrix shows which threats are the most serious - those with the highest probability and the greatest consequences. With that information as a starting point, it is time to discuss possible proposals for action and the order of priority for them. The analysis group draws up a proposal for appropriate measures and indicates the order in which they should be handled.

Decisions on the implementation of action should be preceded by a risk management process, i.e. to assess the way in which identified risks are to be managed in the business.

Only after an assessment of the cost of implementing measures has been weighed against the cost of dealing with a threat that has occurred should a decision be made.

If a decision is made not to take measures, a continuity plan must be drawn up to minimize the effects should the threat occur.

### 9.4.2 Continuity planning

Continuity planning shall take place in accordance with the document Continuity planning.

# 10. APPENDIX 4.1.1 RSA RISK AND VULNERABILITY ANALYSIS TEMPLATE

This section describes the handling of a tool for risk and vulnerability analysis (Appendix, RSA Template) that can be used to document the analysis work and for support during implementation. Below is a tutorial on using the tool.

Stadsnätsföreningen has received permission from Finspångs Stadsnät, Finet AB and Maintrac AB to provide the tool to Stadsnätsföreningen's members.

**Workflow**

***Analysis object***

Start by identifying and prioritizing the objects to be analyzed.

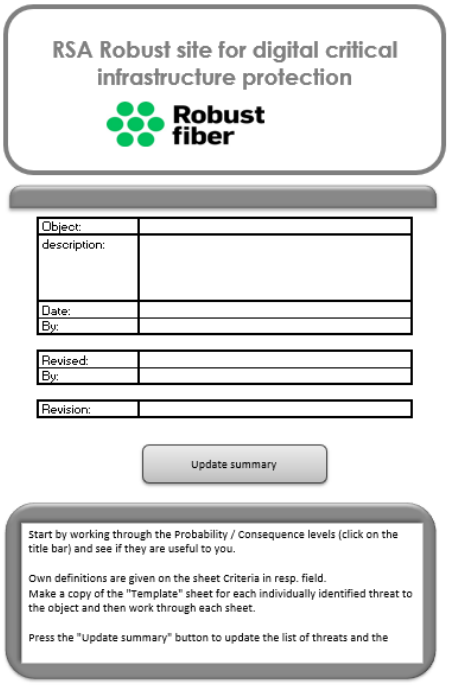
***Working document***

Make a copy of Appendix 1, Tools RSA for each object to be analyzed.

***Summary tab***

Under the tab Summary, the selected object must be described, it must also appear when it has been created and who has created it. There are also fields for the revision date, who revised the document and an audit number.

Figure 3. Summary tab




| SUMMARY OF THREATS | | |
|---|---|---|
| Threats | Risk | Probability |
| Weather (PTSFS 2020:15§) | Medium | Medium |
| Tresspassing (PTSFS 2020:15§) | Medium | Medium |
| Sabotage (PTSFS 2020:15§) | Medium | Medium |
| Other external impact (PTSFS 2020: 15§) | Medium | Medium |
| Information provided by the Swedish Post and Telecom Agency on threats (PTSFS 2020: 15§ | Medium | Medium |
| Fire | Medium | Medium |
| Water damage | Low | Medium |
| Contamination (such as radiological or biological contamination) | Very Low | Low |
| Major accident occurs (S) | Very Low | Very Low |
| Destruction or theft of equipment | Low | Low |
| Dust, corrosion and freezing | Medium | Medium |
| Excavation of cables | Medium | Medium |
| Loss of functions for indoor climate (heating, air conditioning, cooling) | Very Low | Very Low |
| Loss of power supply including manual disconnection in power shortage situations | Low | Medium |
| Deficiencies or errors in troubleshooting functions (alarms, monitoring, etc.) | Medium | Low |
| Electromagnetic radiation | Low | Low |
| Conductive disturbances | Medium | Medium |
| Thermal radiation | Medium | Medium |
| Listening to information | Low | Low |
| Theft of information | Low | Low |
| Disclosure of sensitive information | Very Low | Low |
| Receiving and using information from unreliable sources | Medium | Medium |
| Manipulation of networks, hardware and software | Very Low | Low |
| Faults in equipment | Low | Low |
| Network and hardware overload | Very Low | Very Low |
| Loss of ability to monitor and control | Medium | Very Low |
| Unauthorized use of equipment | Medium | Medium |
| Unauthorized copying of software | Medium | Medium |
| <Ingen benämning> | Medium | Medium |
| Illegal or illicit (within your own organization) handling of information | Medium | Medium |
| Improper use of equipment | Medium | Medium |
| Inaccessibility for staff | Medium | Medium |
| Presence of deficiencies in preventive work | Very high | Very high |
| Existence of shortcomings in management functions (crisis and business management) | Medium | Medium |
| Deficiencies in network monitoring | Medium | Medium |

***Criteria tab***

Review the criteria under the "Criteria" tab and check that they are relevant. Update as needed. During the work, the definitions for the criteria can be retrieved by double-clicking on Consistency or probability in the risk matrix.

***Base threats tab***

In the tool, each threat is listed in the "Base threat " tab. For each such basic threat, there is then a separate tab that is handled in accordance with the heading Analyze threats below.

Go through and remove the threats / tabs that are not relevant to the analysis, document changes and additions under the tab "Bashot" and then go to the tab "Summary" click on the button Update summary and the column Summary of threats for the objects is updated.

To create a new base threat, add a line (Figure 4) using "Insert" in Excel, Ex. FK 6.

**Figure 4.** Insert new base threat under the "Base threat " tab


Then you create a new tab (Figure 5) with the same name, eg FK 6 and write the same Name of the threat that you wrote under the tab "Bese threat ". You can advantageously copy an existing tab. Then go to the "Compilation" tab (Figure 6) and press the **Update Compilation** button and the new base threat will be posted in the Compilation of threats column for the objects.

**Figure 5**. New tab, eg FK 6, Name and Tab name.

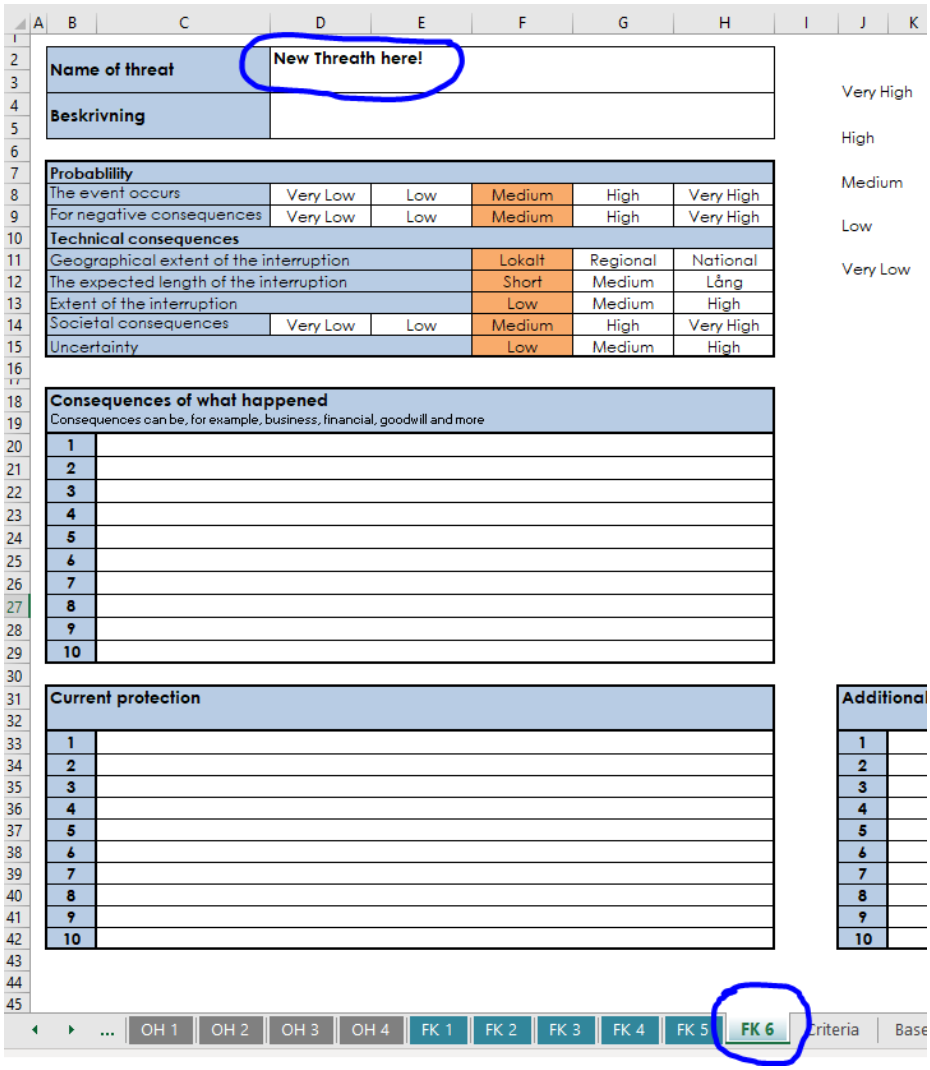
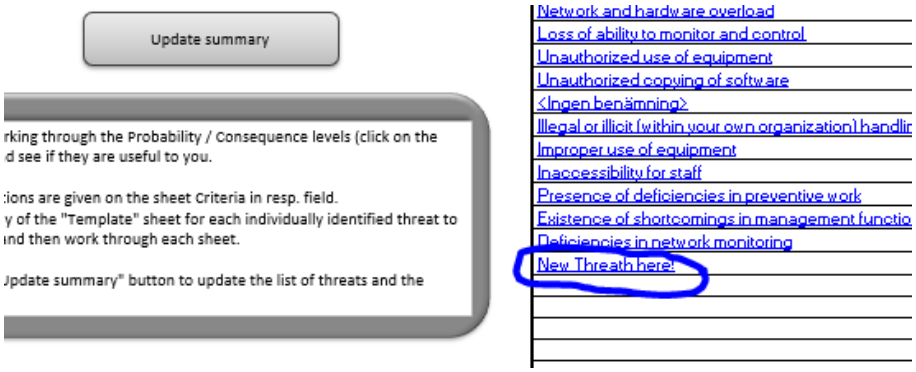


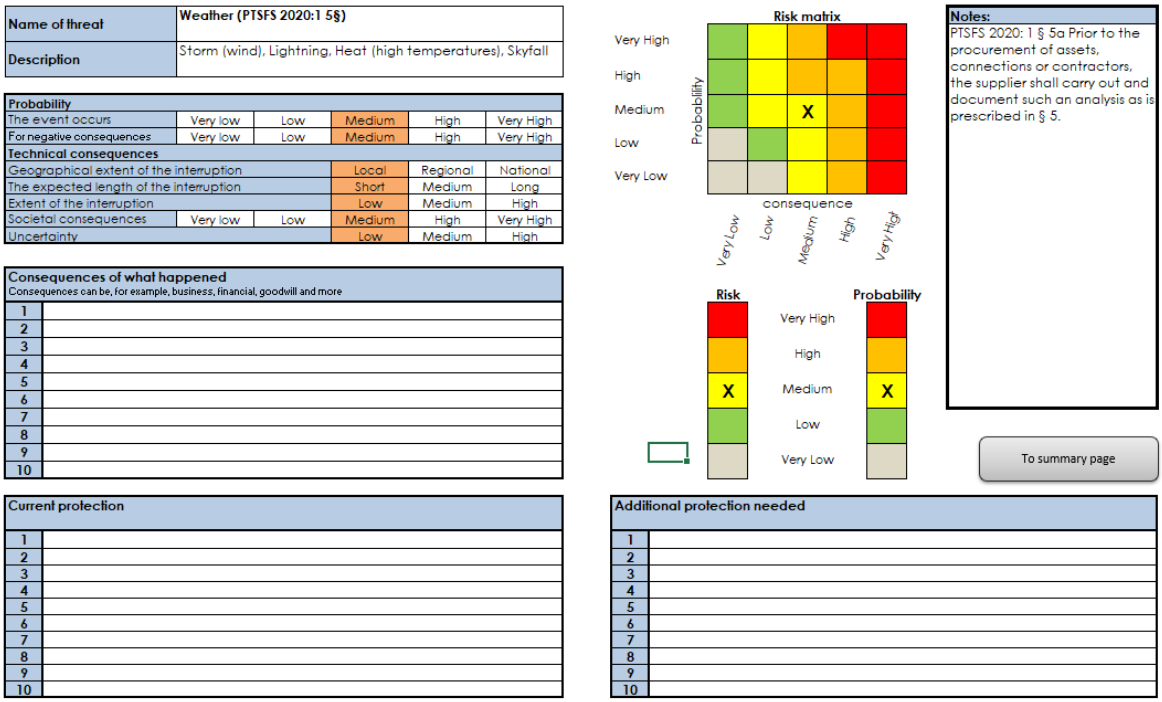

**Figure 6.** New base threat is displayed in the list



### *Analyze threats*

The name and description of the threat are entered (Figure 7).
The table with probability and consequences is filled in and in the Risk Matrix, a cross will automatically be placed in the right place in the matrix and provide guidance on how low or high the risk is.
You can get a summary of the threat by looking at the Risk and Probability bars under the Risk matrix.
The greater the societal impact of the threat, the greater the risk. Everything except green requires an action immediately (red) or later (orange or yellow), the same applies to Probability red, orange, yellow or green.

**Figure 7.** Threat tab




The table Consequences of what happened documents the consequences of a threat occurring.

The tables Current protection and Additional protection indicate current protection and if additional protection is needed to manage the risk. The notes in the Additional Protection table will form the basis for actions that are automatically compiled into a list under the **Action List tab**. The notes in the Current Protection table are also compiled automatically under the **Current Protection tab.**

In the field for memoranda, important things can be noted about the assessments, e.g. how to arrive at the assessment of the probability.

When the analysis is complete, click on the **To Home button** and click on the **Update Summary button**, updating the Risk and Probability columns.

***Risk management and continuity planning***

*After the analysis, use the basis for continued risk management in accordance with Chapter 9.4, Risk management and continuity planning.*