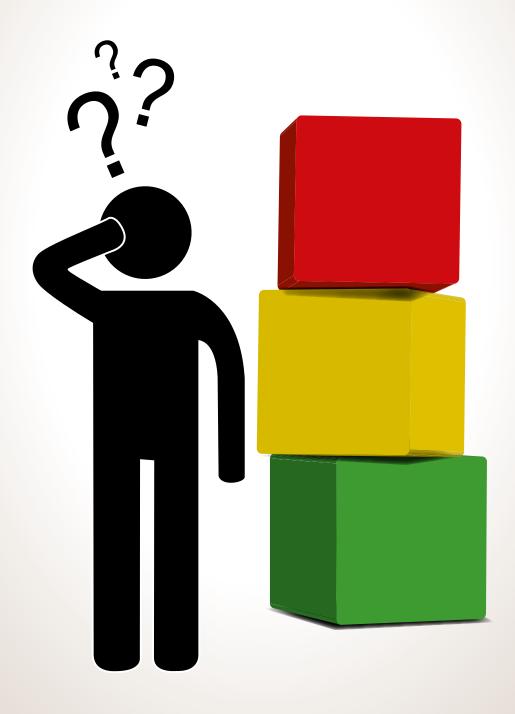


## **Risk Assessment**



### INTRODUCTION

The purpose of identifying risks and threats is to be in a position to confront them in order to minimise their consequences and as far as possible secure the continuing function of the unit. In the risk assessment no distinction is made between risks and threats, since these two concepts are often closely related.

The risk assessment addresses risks and threats at the level of the unit, which means that individual units identify those risks and threats that could potentially affect continuing function within its own area. In this context it is important to bear in mind that this may relate both to services the unit receives and to services it provides for others.

In the following the various elements are described.

### STEP 1: ASSESSMENT OF RISKS/ THREATS TO CONTINUING FUNCTION

#### Risks/threats

In the column 'Risks/treats' in form 1 enter the risk or threat the unit might be exposed to. There can be various forms of risk. Some can be associated with maintaining the function of the individual unit or area. Others can be associated with a breakdown of functions within the organisation that mean that everyday working processes cannot be maintained.

In Appendix 1 you can see the catalogue of potential threats, which is a list of the Emergency Planning Committee's suggestions of threats and risks.

#### **Risk level**

#### High risk, moderate risk, low risk

The risk level should be assessed for each of the risks/threats identified in relation to their probability and their consequences, see Risk matrix in appendix 2.

#### **Explanation**

In this column you should describe why each risk/threat has been mentioned and what the consequences might be if the unit were to be subjected to this risk/threat.

Form 1: Assessment of risks/threats to continued functioning

Organisation: (Name of Department/Unit)	Completed by:
Person responsible: (Head of Department/Unit)	Date: dd-mm-yy



Risks/threats	Risk	leve	Justification

Figur 1: Rxtract from form 1: Assessment of risks/threats to continuing function

## STEP 2: IDENTIFICATION OF NECESSARY PROCEDURES

#### Risks/threats

The risk identified under Step 1 is transferred to form 2.

All risks/threats with a moderate or **high risk** level should have procedures for countering or dealing with them, but procedures or instructions can also be worked out for addressing risks/threats with a **low risk** level.

#### **Procedures**

In the column 'Procedures' on form 2 you should describe or list the procedures that have been prepared to counter individual risks/threats. You should also indicate here if the procedures are not sufficient.

Form 2: Identification of necessary procedures								
Organisation: (Name of Department/Unit)		t/Unit)	Completed by:					
Person responsible	e: (Hea	d of [	Depar	tment/Unit)	Dato: dd-mm-yy			
	HIGH RISK	MODERATE RISK	LOW RISK			COMPLETELY	PARTIAL	NOT YET
Risks/threats	Risk	leve		Procedure			Prepa	ared
IT-nedbrud								
							1	
								$\Box$
	1					+	1	
	1					+	1	$\vdash$
							1	$\vdash$
	t					+	T	$\vdash$
						+	t	$\vdash$
						+	+	$\vdash \vdash \vdash$
						+		$\Box$

Figur 2: Extract from form 2: Identification of necessary procedures  $% \left( 1\right) =\left( 1\right) \left( 1\right$ 

## STEP 3: PROCESS FOR DEVELOPING A BASIS FOR EMERGENCY PLAN

This step has been divided into two parts.

**Part 1**. The first part of form 3 should be completed in the unit, and all members who have contributed to the assessment should go through the result together. Agreement should be reached as to which risks are covered by the unit's emergency plan, which should be dealt with elsewhere, and which should not be dealt with.

- Emergency Management Plan: It must be managed in the Emergency Management Plan
- Not to be dealt with: Should not be managed as a risk
- Elsewhere: Should be managed in APV (Workplace Assessment), maintenance etc. (You should affix a comment in the Excel sheet as to where and how the risk should be managed elsewhere)

**Part 2**. After this, a decision should be taken as to how the risks pinpointed should be managed in the Emergency Management Plan. This part of Step 3 takes place as a workshop, so it should not be completed in advance:

- 1. **Covered by the template:** If the risk is already managed in the template and there is no need for further information.
- 2. Chapter: If the risk is to be managed as a general procedure
- 3. *Appendix 2.x:* If the risk should be managed as an operational instruction
- 4. *Link:* If the risk is complex in nature or is administered in another context such as 'Kemibrug', a link can be made to the electronic site of relevant instructions. Instructions can be placed on the S-drive if there is a need for restricted access.
- 5. *Display:* If the risk can be managed by placing local displays where necessary.
- 6. **'Filed':** Confidential information retained by trusted staff.

  The Emergency Management Plan indicates who holds the relevant information.

# STEP 3: PROCESS FOR DEVELOPING A BASIS FOR EMERGENCY PLAN

Form 3 has been created to assist with this part of the process: Basis for Emergency Plan

Skema 3: Plangrundlag								
Organisation: (Name of Department/Unit)	Completed by:							
Person responsible: (Head of Department/Unit)	Dato: dd-mm-yy							

EMERGENCY MANA-ON GEMENT PLAN
NOT TO BE DEALT
COVERED BY TEM-PLATE
CHAPTER
APPENDIX 2.X
LINK
DISPLAY
FILED

Risks/threats		Comments on "Elsewhere"	To be placed				

Figur 3: Extract from form 3: Basis for Emergency Management Plan.

## STEP 4: PREPARATION OF PROCEDURES AND INSTRUCTIONS

On the basis of decisions taken under Step 3, existing plans and procedures should be reviewed to ensure the quality of materials that have already been developed.

New plans and procedures should be prepared for those areas that are not already covered, and documents should be added to the Emergency Plan in accordance to decisions made and noted in form 3. As a basis on which to supplement the preparation of instructions or procedures, you can use documents prepared by the Health & Safety Department: 'Chapter for Emergency Management Plan' or Appendix 2.x. for Emergency Management Plan'. The documents will be forwarded to participants after the workshop.

All Emergency Plans should be sent to the Working Environment Office for review. The subsequent practical process of incorporating the Emergency Management Plan's procedures and instructions can be seen in 'Guidance for preparation and revision of Emergency Plans'.

### **APPENDIX 1: CATALOGUE OF THREATS**

As an aid to identifying what might be a risk or a threat, the Emergency Planning Committee has prepared the following catalogue of threats. The risks/threats listed here are meant only as an aid.

☐ Labour dispute	☐ Major strike/boycott	☐ Transport accident (road, rail, sea, air)
☐ Fraud	☐ Snowstorm	□ Power Cut
☐ Bomb threat	□ Bullying	☐ Breach of food safety
☐ Fire or explosion	☐ Misuse of data	☐ Youth criminality
☐ Breach of workplace safety	□ Nepotism	☐ Accident caused by lethal/pollutant materials
☐ Drinking water pollution	Overall negative reaction from the public	☐ Violence against staff
☐ Drowning accident	☐ Overall negative media coverage	☐ Armed robbery
☐ Poor citizen service	☐ Failure of care for cildren/elder- ly/handicapped	☐ Destruction of important buildings or installations
☐ Poor communication with the media	☐ Malicious rumours	☐ Breach of IT security
☐ Mistaken interference from authority	☐ Riots/breakdown of public order	☐ Loss of key staff
☐ Faulty or mistaken article, radio or TV feature	☐ Organised crime	☐ Terror - biological or chemical weapons
☐ Accident caused by poison	☐ Hurrica/violent storm	☐ Terror - conventional weapons
☐ Hostage-taking	□ Flooding	☐ Outbreak of infectious disease among domestic animals
☐ Heat wave	☐ Infringement of the law or regulation	☐ Staff invovled in serious accident at work
□ Vandalism	□ Sudden death	☐ Outbreak of particularly dangerous disease, epidemic or pandemic among humans
☐ A hard winter	□ Political scandal	Leak of confodential information
☐ Sheet ice	☐ Problems in restructuring	☐ Cloudburst
□ Cyber attack	☐ Problems related to inviting tenders	☐ Corruption
☐ IT breakdown	□ Sabotage	

### **APPENDIX 2: RISK MATRIX**

#### Risk matrix

The underlying thought behind the matrix is that the extent of a risk is always estimated on the basis of the probability of the occurrence taking place and the consequences of the occurrence. The greater the probability and the consequence a risk/threat has, the more serious it is.

The parameters given in the matrix are only to be seen as guidelines. It will be possible to identify risks/threats that do not immediately comply with them.

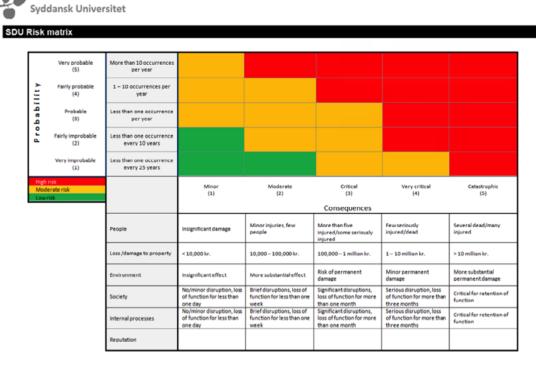


Figure 2: Risk matrix