



# Risk Assessment



DEPARTMENT/UNIT:

# 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 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)	Completed by:
Person responsible: (Head of Department/Unit)	Dato: dd-mm-yy

Risks/threats	Risk level			Procedure	Prepared		
	HIGH RISK	MODERATE RISK	LOW RISK		COMPLETELY	PARTIAL	NOT YET
IT-nedbrud							

Figur 2: Extract from form 2: Identification of necessary procedures

# 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 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.

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



# 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.



SDU Risk matrix

Probability	Very probable (5)	More than 10 occurrences per year				
	Fairly probable (4)	1 – 10 occurrences per year				
Probable (3)	Less than one occurrence per year					
Fairly improbable (2)	Less than one occurrence every 10 years					
Very improbable (1)	Less than one occurrence every 25 years					
High risk						
Moderate risk						
Low risk						
		Minor (1)	Moderate (2)	Critical (3)	Very critical (4)	Catastrophic (5)
		Consequences				
People	Insignificant damage	Minor injuries, few people	More than five injured/some seriously injured	Few seriously injured/dead	Several dead/many injured	
Loss /damage to property	< 10,000 kr.	10,000 – 100,000 kr.	100,000 – 1 million kr.	1 – 10 million kr.	> 10 million kr.	
Environment	Insignificant effect	More substantial effect	Risk of permanent damage	Minor permanent damage	More substantial permanent damage	
Society	No/minor disruption, loss of function for less than one day	Brief disruptions, loss of function for less than one week	Significant disruptions, loss of function for more than one month	Serious disruption, loss of function for more than three months	Critical for retention of function	
Internal processes	No/minor disruption, loss of function for less than one day	Brief disruptions, loss of function for less than one week	Significant disruptions, loss of function for more than one month	Serious disruption, loss of function for more than three months	Critical for retention of function	
Reputation						

Figure 2: Risk matrix