Funded by the European Union

CYBER4Dev

Preparing an IT Risk Assessment

NI·CO

Republic of Estonia
Information System Authority

Foreign, Commonwealth & Development Office

Ministry of Foreign Affairs of the Netherlands

Table of Contents

Introduction

These guidelines have been prepared with the purpose of helping institutions and companies to identify and assess Information System risks related to the services that are being provided.
Current guidelines have been reviewed and translated from the Estonian government provided IT risk analysis guidelines for essential service providers and samples updated accordingly. Original guidelines were prepared by KPMG and Mr. Martin Indrek Miller from Estonian Information System Authority.

Definitions

IT risk analysis (i.e. a risk analysis of systems) – a description of the threats to the security of systems and the continuity of services and the measures implemented to manage the risks.

Critical activity – an activity/process/function performed by the service provider that is dependent on at least one system and is necessary to provide the service and in whose absence the service may be interrupted.

Network and information system (hereinafter *system*) – an electronic communications network, any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data, or digital data stored, processed, retrieved or transmitted by aforesaid elements for the purposes of their operation, use, protection, and maintenance;

Resource – all means used for maintaining and affecting the operation of systems, including premises, ventilation, cooling, and heating equipment serving the premises, equipment supplying the premises and systems with electricity, software used to operate the systems, and the staff of the service provider.

Cyber incident – an event taking place in a system that threatens or compromises the security of the system.

Threat – an event or circumstance capable of exploiting the vulnerabilities in systems or resources related to them.

Vulnerability – the lack of security in systems or systems-related resources which makes systems or systems-related resources vulnerable to threats.

Risk – an estimate based on the combination of the likelihood of a vulnerability being exploited by a threat and the consequences of a possible cyber incident.

Confidentiality – protection of data or a system from unauthorised access by third parties.

Availability – the availability and expected functioning of a system or data.

Integrity – the protection of data from unauthorised alteration or destruction.

Interruption – a negative deviation in providing the expected service, caused by foreseen or unforeseen events.

Maximum Tolerable Downtime (MTD) – a period of interruption of a critical activity, system, or the functioning of a resource, after which the company or institution is unable to provide the service under the terms set out in legislation or contracts.

Recovery Time Objective (RTO) – a period of time established by the service provider for resuming and restoring the operation of a critical activity, system, or resource.

1 Guidelines for identifying, analysing, and assessing IT risks

Assessing the risks related to the systems that are necessary for providing the service is part of the process of ensuring the continuity of the service. As a result, information technology-related threats, vulnerabilities, and dependencies which can cause interruptions in critical services are identified and the associated risks assessed. Risk assessments must be reviewed periodically and revised as appropriate, and the adequacy and cost-effectiveness of the applied security measures are analysed.

The purpose of an IT risk analysis is to:

- provide an overview of the existing IT risks;
- develop a risk treatment strategy;
- give input to service providers to ensure the continuity of the service.

Stages of risk analysis	Key activities
Identification of critical activities, systems, and resources	• Describing the activities critical for providing the service • Mapping, describing, and critically assessing important systems. • Mapping the resources related to the systems.
Identification of threats	• Identification of the threats that could lead to cyber incidents and thus compromise the security of the system or the continuity of the service. • It is important to remember that threats are not static or exhaustive.
Identification of vulnerabilities	• Identification of vulnerabilities that can lead to the realisation of threats causing harm to assets or the organisation. • Linking vulnerabilities to previously mapped systems and identified threats.
Assessment of likelihood	• Identifying existing security measures to prevent, detect, and mitigate interruptions. • Identifying the likelihood of threats
Assessment of consequences	• Identifying the business impact on the organisation when threats materialize.
Risk assessment	• Risk classification. • Creation of a risk matrix.
Risk management	• Listing the risks in order of priority with the preventive and mitigating security measures as well as the persons responsible for their implementation and the deadline.

Table 1 Stages of risk analysis

1. Critical activities, systems, and resources

The service provider must identify the **critical activities** that are dependent on at least one system and necessary for providing the service, and whose absence could interrupt the service. Maximum Tolerable Downtime and Recovery Time Objective have to be defined for each critical activity.

Then, the service provider maps the systems and related resources necessary for the functioning of the critical activities.

Identification of assets

The service provider will determine all systems that are necessary for the functioning of the critical activities, i.e. interruptions in the functioning of systems will directly or indirectly cause interruptions in the service.

It is necessary to collect the following information about each critical activity and system (the corresponding table can be found in Annex 1 to the guidelines):

- critical activity;
- system(s) necessary for the functioning of the critical activities;
- a short description of the system;
- Maximum Tolerated Downtime (MTD);
- Recovery Time Objective (RTO);
- service provider and location (internal and external);
- users and/or the owner of the system;
- the dependence of a critical activity on a system and/or ICT service.

The dependence of a critical activity on a system is determined on the following scale:

1 – the dependence is not particularly significant
2 – the dependence is significant, but there is an alternative solution;
3 – the dependence is critical (the critical activity is interrupted due to a system failure).

The service provider may include in the risk analysis, among other things, risks that are not related to providing the service but are related to the systems important for the functioning of the system.

Resource mapping

In the second stage, the service provider identifies the **resources** related to the systems.

Resources are all means used for maintaining and affecting the operation of systems, including premises and the ventilation, cooling, and heating devices of these premises; devices supplying the premises and systems with electricity; software used to operate the systems, and the staff of the service provider.

It is reasonable to group similar resources and mention them only once in the risk analysis. Similar resources may be grouped based on the following characteristics:

- the resources are of the same type;
- the resources have been and will be configured in the same way;
- the resources are connected to the web in the same way (working stations based on the same operating system);
- the resources are subject to the same administrative and infrastructure requirements;
- the resources are subject to the same protective requirements.

PRACTICAL EXAMPLE

Resources include, among other things, data storage devices, backup devices, equipment rooms, backup power devices and systems (power generators, uninterruptible power supplies (UPS), climate devices for server rooms, and their control and monitoring equipment).

In terms of resources, procedures related to the use of devices must also be considered other means. For example, to ensure the smooth operation of the servers, it is necessary to keep the temperature and humidity of the server room within the limits set by the manufacturer. In the event of a malfunction of a particular monitoring system, the system operator does not have an overview of the related indicators, and in the event of a malfunction in the cooling system, the monitoring system does not give an alarm signal in due time. The result is a server outage due to overheating. This may also cause data loss, as the data in the memory is not written to the disk due to server shutdown. Power outages have similar consequences, where, in the event of an outage of the main power supply, a backup power supply exists in the form of a UPS, but the diesel generator supporting the UPS does not start. The reason is that the diesel generator had not been tested. In addition to loss of data due to a power outage, the incident can also harm the hardware of the server.

Output:

- A list of the systems necessary for providing the service and the related resources (in accordance with Annexes 1 and 2 to the guidelines).

1.2 Identification of threats

The service provider must identify and describe the threats that they deem significant and relevant and that may cause a cyber incident, thus endangering the security of the system or the continuity of the service.
As the risk analysis mainly addresses risks related to systems, it is recommended to focus on threats related to information technology.

A threat is an event or circumstance capable of exploiting the vulnerabilities in systems or resources related to them.

When identifying threats, the following should be taken into account:

- the threat may originate from the organisation itself or be of external origin;
- the threats can be of natural or human origin and may be intentional or unintentional;
- some threats can endanger several assets and be related to different vulnerabilities. In such cases, they may have different effects on different assets;
- threats change constantly in time and when making changes to the system.

Threats are identified based on statistics, research, and expert opinions. Primary data may be collected from the owners or users of the assets, the administrator of the building, information security specialists, other organisations, national authorities, etc. Previous incidents and experience gained from earlier threat assessments should definitely be taken into account. If necessary, you may wish to consult other catalogues of threats, which may be organisation- or profession-specific, to make additions to the list of general threats.

When identifying threats, it is recommended to consult the list of threats provided in Annex 3 to the guidelines; the list is not exhaustive and every organisation can update or shorten it as necessary.

A risk analysis must include the following types of threats (causes of a cyber incident) as threat scenarios:

- physical damage (fire, water, dust, etc.)
- natural events (climate phenomena)
- power outage
- network outage
- software errors
- hardware faults
- device malfunction
- cyber attacks
- physical attacks

- user errors
- administrative errors
- external service provider errors

All identified threats are associated with previously mapped systems and the related resources (pursuant to Annex 5 to the guidelines).

Output:

- A list of threats (events) that can cause cyber incidents and thus compromise the security of the system or continuity of the service.

1.3 Identification of existing security measures and vulnerabilities

The service provider conducts an analysis to identify the vulnerabilities, through which threats compromising systems or the organisation may materialise.

> **A vulnerability** is the lack of security of systems or systems-related resources which makes systems or systems-related resources vulnerable to threats.

Based on the security measures previously applied by the service provider, vulnerabilities that could not be eliminated even after applying the measures will be identified.

Vulnerabilities in systems, procedures, policies, and infrastructures are identified by observation and using documentation. When performing a vulnerability analysis, input can be collected from various sources, such as interviews with the owners and users of the resource, questionnaires, statistics, results of security testing, (technical) security audits, documentation reviews, automated scanning tools, documentation of security measures, the existing risk management plan, etc.

The list of vulnerabilities provided in Annex 4 to the guidelines may also be consulted in identifying vulnerabilities, and the list can be amended or shortened by each organisation as necessary. Different vulnerabilities can also be found by using various public databases of vulnerabilities (e.g. ISKE, ISO 27005, and the US-CCU Cyber-Security Check List).

Vulnerabilities may be classified and grouped, for example, as follows:

- organisational vulnerabilities;
- staff-related vulnerabilities;
- infrastructure vulnerabilities;
- technological vulnerabilities.

All vulnerabilities are associated with previously mapped systems and the related resources (pursuant to Annex 5 to the guidelines).

Output:

- A list of vulnerabilities through which threats compromising systems or related resources can materialise and disrupt the functioning of the system and/or service.

4. Assessment of likelihood

The assessment of the likelihood of a threat materialising, is mainly based on previously identified vulnerabilities, considering previously applied security measures.

In making the assessment, the following must be taken into account:

- previous experience and statistics;
- in the case of intentional threats, the motivation and capabilities of the potential attackers;
- in the case of natural threats: geographic factors, such as the probability of extreme weather, as well as factors that can cause human errors and device malfunctions;
- the nature of the vulnerability;
- the effectiveness of the current security measures.

The assessment of a likelihood, identifies the existing security measures for preventing, identifying, and mitigating outages which have been applied to minimise or decrease the realisation of threats:

- **preventive measures** – for preventing the realisation of a threat;
- **identifying measures** – used constantly for identifying threats and defining and specifying situations that occur upon the realisation of a threat;
- **mitigating measures** – used for reducing or avoiding possible negative effects upon the realisation of a threat.

When mapping measures, special attention should be paid to security measures related to information technology (software and hardware) and physical (access rights, physical security) and organisational security measures (policies, procedures).

Activities necessary for identifying the existing security measures:

- revise documents that include information about the measures;
- ask for input from the employee responsible for information security (as well as from those who are responsible for ensuring physical security) about the specific measures applied on specific resources;
- perform an on-site inspection of the physical and IT measures;
- review the results of audits.

A probability assessment is given at least for the next three years in accordance with the criteria provided in Table 2. **The list provided in the table is not exhaustive and each institution must consider other specific circumstances**

of the organisation. At least one of the criteria of the probability assessment must be met.

Likelihood	Criteria of the likelihood of the threat
5 – very high	• the threat has already realised or the realisation of the threat is unavoidable; • the threat will realise within a year with a > 90% probability; • the threat may realise within days or weeks.
4 – high	• the probability of the realisation of the threat is high and there is clear evidence supporting that; • the threat will realise within a year with a > 50% probability; • the threat may realise within weeks or months.
3 – average	• the realisation of the threat is possible and there is evidence thereof; • the threat will realise within a year with a > 10% probability; • the threat may realise within a year.
2 – low	• possible, but there are few examples of occurrence; • the threat will realise within a year with a > 1% probability; • the threat may realise after several years.
1 – very low	• the realisation of the risk is more theoretical; extremely few examples of occurrence; • the threat will realise within a year with a < 1% probability; • possible but only in extreme conditions; • less than once during 100 years.

Table 2 Criteria of the likelihood of the threat

Output:

- A list of identified threats with an analysis of the likelihood of their realisation considering the vulnerabilities identified and measures in use (in accordance with Annex 5 to the guidelines).

1.5 Assessing the consequences and their severity

This step identifies the potential consequences of the realisation of the threat for system security and/or service continuity. The severity of the consequences is also determined.

Damages must be assessed based on a specified five-level scale. At least one of the possible consequences of the corresponding severity list must be identified.

In addition to the criteria in Table 3, the service provider must include in the criteria of the severity of the consequences the approximate number of people influenced by the cyber incident, the duration of the interruption of the service, the type and extent of possible damage, as well as the complexity of recovering the service. Each service provider will establish these criteria themselves according to the nature of the organisation and service.

In assessing the severity of the consequences, among other things, it is necessary to consider the combination of different types of threats (not only those related to ICT systems), i.e. the combined effect of different threats must be taken into account.

Severity of consequences	Criteria for the consequences of the realisation of a threat
Catastrophic (E)	• the materialisation of a threat causes a long-term interruption of the service or endangers national security or the lives of a large amount of people, or has catastrophic consequences for the environment, or inflicts critical financial losses; • extremely hostile public and media attention lasting for months and causing clients to stop using the service; • long-term interruptions in other vital services may occur or there is an imminent threat that such a situation may occur; • the service is disrupted to the extent of 80–100%.
Very severe (D)	• The realisation of the threat causes a significant interruption in the service or endangers national security or endangers human lives or inflicts significant economic losses; • significant negative public attention that lasts weeks and may cause clients to stop using the service; • the provision of other vital services is significantly disrupted or there is an imminent threat of such a situation occurring; • the service is disrupted to the extent of 50–80%.
Severe (C)	• The realisation of the threat may cause an interruption in the continuity of the service or endangers human health or the environment or inflicts significant economic loss;

	• negative attention that lasts for days and may reoccur at a later time; • other vital services may be disrupted or there is an imminent threat of such a situation occurring; • the service is disrupted to the extent of 30–50%.
Light (B)	• The realisation of the threat would likely cause significant obstacles to the performance of the functions of the organisation or significant economic losses; • negative attention that lasts for one day; • the service may be disrupted to the extent of 10–30%.
Minor (A)	• The realisation of the threat would not cause significant obstacles to the performance of the functions of the organisation; • brief negative attention expressed in a few messages in the media; • the service is not disrupted.

Table 3 Criteria for the consequences of the realisation of a threat

Output:

- A list of identified threats with an assessment of the severity of the consequences (in accordance with Annex 5 to the guidelines).

1.6 Determination of the level of risk and risk analysis

A risk is an estimate based on the combination of the likelihood of a vulnerability being exploited by a threat and the consequences of a possible cyber incident.

Each threat scenario is assigned a risk classification, depending on the probability of realisation and the severity of the consequences. **A threat becomes a risk**.

The level of criticality of a risk is expressed as a risk classification.

Risk classification = Consequence × Probability

For an overview of risk criticality, the risks are plotted on a risk matrix (see Annex 6).

	Risk classification	Description
	Very high risk **(R[5])**	Unacceptable risk. If the risk is deemed very high, it calls for immediate action as well as for the planning and implementing of preventive and mitigating measures. Further operation of the systems is not allowed without decreasing the risk level to at least the level of 'high risk'. The organisation must immediately lower the level of risk and normal operation is only allowed to the minimum extent necessary for providing the service at the minimum acceptable level.
	High risk **(R[4])**	Significant risk. The risk must be decreased as soon as possible. A risk mitigation plan must be prepared and implemented as a set of immediate actions.
	Average risk **(R[3])**	Unwanted risk. Measures must be planned to decrease the risk. An action plan must be drawn up and priorities must be set for activities. Measures must be applied within a reasonable time.
	Low risk **(R[2])**	Tolerable risk. The risk is acknowledged, but further measures to decrease it might not be implemented. It is necessary to consider the need for security measures for preventing and/or mitigating consequences and assess whether the application of measures is more beneficial than accepting the risk. If the risk mitigation measures are more costly than the damage resulting from the realisation of a threat, no action is needed.
	Very low risk. **(R[1])**	Insignificant risk. Applying security measures is not obligatory, but the risk must be monitored and assessed regularly.

Table 4 Descriptions of risk classifications

Output:

- A list of identified risks with classification (in accordance with Annex 5 to the guidelines).

1.7 Risk management and choice of security measures

In risk analysis, the service provider decides the way and method how risks are managed based on the risk tolerance and general strategy of the organisation.

The purpose of risk management is to bring residual risks to a level that is acceptable for the organisation.

For example, there are four possibilities to manage risks: avoiding risks, decreasing risks, dividing risks, and accepting risks.

The service provider will determine in advance **the criteria** for accepting risks; in those cases, further security measures to manage the risks will not be applied.

It is obligatory to plan and apply the security measures for:

- risks with a classification of 'very high' (R5) or 'high' (R4);
- risks that may cause a longer interruption than the previously defined Maximum Tolerable Downtime.

Decisions regarding risk acceptance must be recorded along with the justification and coordinated with the management board of the organisation.

As eliminating all risks is usually impractical or even impossible, it is necessary to plan and apply the most appropriate and relevant risk management activities (security measures for preventing, mitigating, and identifying risks) to minimise the impact of the threat. Special attention should be paid to security measures related to information technology (software and hardware) and physical (access rights, physical security) and organisational measures (policies, procedures).

Measures must be described based on the risk classification set out in chapter 1.6 of the guidelines while considering the importance of the system and the related resources as well as the severity of the related risks.

The selection of measures should take into account the cost of applying the measures, the time schedule, and technical aspects. It is also important to assess the cost-effectiveness of the measures, i.e. evaluate the cost of applying the measures used for decreasing the risk and compare it with the loss that can be prevented by decreasing the risk. If the risk classification is not 'very high' or 'high', it may be unreasonable to apply all available measures if the damage prevented is less than the cost of applying the measure.

Output:

- A list of risks in order of priority according to risk class (in accordance with Annex 7 to the guidelines).
- A list of security measures to be applied with an estimate of the costs and the persons responsible for applying the measures (in accordance with Annex 7 to the guidelines).

1.8 Monitoring of risks

In order to detect any changes in the organisation at an early stage and maintain a complete overview of risks, the service provider must ensure the continuous monitoring of risks. The service provider must update the risk analysis at each occurrence of significant risks.

Risks are never static. Threats, vulnerabilities, probability, and consequences can change unexpectedly, especially in the field of IT. Therefore, constant monitoring is required for detecting the above changes. It is necessary to apply identifying

measures and continuously monitor the activity in information systems to identify the realisation of threats (incidents) in a timely manner and respond to them immediately.

Any significant change in systems or processes must be accompanied by a risk assessment. When planning changes to an IT system, it is necessary to determine whether and how the change will affect the security of the system and the process, and to mitigate the impact of the risks inherent in the change.

1.9 Risk review

Risk review is a periodic activity that involves reviewing previously described risks and, if necessary, revising previous risk assessments as well as supplementing the described risks with new ones based on new threats, vulnerabilities, dependencies, etc. It may also be necessary to expand the list of described risks on an ongoing basis if **new critical circumstances** emerge that cannot be added to the risk matrix or, if under the new circumstances, the re-evaluation of existing risks cannot take place until the next periodic review. New circumstances may, among other things, emerge during the monitoring described in the previous section, for example, when discovering new realised threats.

The risk review must include the following:

- new systems and the related resources;
- new threats that had not been assessed before;
- new or increased security vulnerabilities, through which threats can be realised;
- vulnerabilities identified earlier which are open to new or recurring threats;
- increased exposure to threats, vulnerabilities, and risks, leading to unacceptable levels of risk;
- cyber incidents;
- all of the risks described above must reassessed and reclassified (i.e. determined whether the risk components have changed over time).

A risk review must be performed regularly, **at least once a year**.

Used sources

1. EVS-EN ISO/IEC 27000:2017. Information technology. Security techniques. Information security management systems
2. EVS-EN ISO/IES 27001:2017. Information technology. Security techniques.
3. EVS-ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management.
4. ISO 27035:2013. Information technology. Security techniques. Security incident management.
5. ISO 31000:2009. Risk management – Principles and guidelines.
6. National Institute of Standards and Technology (NIST). Risk Management Guide for Information Technology Systems. Special Publication 800-30.
   URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
7. Hanson, Vello; Buldas, Ahto; Martens, Tarvi; Lipmaa, Helger; Ansper, Arne; Tulit, Viljar. 2009. Infosüsteemide turve I: Turvarisk. Cybernetica AS.
8. Riigi Infosüsteemi Amet. ISKE rakendusjuhend ja kataloogid versioon 8.00.
   URL: https://www.ria.ee/ee/iske-dokumendid.html
9. Emergnecy Act (.RT I, 22.05.2018), 5
   URL: https://www.riigiteataja.ee/akt/103032017001?leiaKehtiv
10. Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan. RT I, 28.06.2017, 6
    URL: https://www.riigiteataja.ee/en/eli/525092017001/consolide
11. Cybersecurity Act. RT I, 22.05.2018, 1
    URL: https://www.riigiteataja.ee/en/eli/525062018014/consolide
12. The Federal Office for Information Security (BSI). BSI-Standard 100-4. Business Continuity Management. Version 1.0.
13. The Office of Government Commerce (OGC). Management of Risk: Guidance for Practitioners.
14. The SANS Institute. Information Security Risk Management training materials. Building & Running a Risk Management Program.
15. US-CCU küberturbe kontroll-küsimustik.
    URL: https://www.ria.ee/sites/default/files/content-editors/KIIK/us_ccu_kontrollkusimustik_081211.pdf

Annexes

Appendix 1 Systems that affect service continuity

Critical Activity	System necessary for critical activity	Description of a system	MTD	RTO	Service provider/ location	Users/ Owner	Critical Activity Dependence from system

Appendix 2 Resources related to systems

System necessary for the operation of a critical activity	Resources needed to run the system	Description of Resource	MTD	RTO	Service provider/ location	Users/ Owner

Appendix 3 Examples of typical threats

Type	Threats
Physical damage	Fire
	Water damage
	Heat and moisture
	Pollution
	Destruction
	Dust, corrosion, freezing
Natural events	Storm/lightning
	Flood
	Heavy rain
	Seismic phenomenon
Technical failures	Loss of power
	Equipment failure
	Equipment malfunction
	Software malfunction
	Air condition failure
	Network failure
Cyber attack	Malware distribution
	Social engineering
	Phishing
	Defacement
	System intrusion, break-ins
	System penetration
	Tampering with hardware
	Tampering with software
	Identity theft
	DDoS
	brute-force attack
	Ransomware
	Port scan
	Physical attack against infrastructure
	Unauthorized access to premises

Physical attacks	Impersonating as external service provider employee
	Theft of equipment or media
	Unauthorized copying of data/media
	Unauthorised use of equipment and/or systems
	EMP attack
	Disruption of network with interference signals
Personnel	User error
	Misconfiguration of equipment/software
	Lack of testing
	Absence of personnel
	External service provider error
	Unsupervised work by contractors
	Loss of equipment or media

Appendix 4 Examples of vulnerabilities

Type	Vulnerability
Infrastructure	Unfavourable location of the site (prone to flood etc.)
	Outdated/Depreciated infrastructure
	Inadequate or careless use of physical access to buildings and rooms
	Lack of physical protection of the building, doors and windows
	Unstable power grid
	Unprotected communication lines
	Insecure network architecture
	Insufficient network management
	Unprotected connections to the public network
Personnel	Inexperience
	Inadequate recruitment procedures (background checks)
	Incorrect use of software and hardware
	Lack of security awareness
	Ignoring security measures
	Insufficient security training
	Lack of monitoring mechanisms
	Unsupervised work by outside cleaning staff
Organization	Missing security management
	Lack of continuity plans
	Lack of management support for security measures
	Lack of resource management
	Missing documentation
	Missing security controls
	Lack of formal procedures for ISMS documentation control
	Lack of logging
	Lack of information security responsibilities in job descriptions
	Lack of proper allocation of information security responsibilities
	Missing or inadequate software testing

Technological	Missing monitoring
	Wrong allocation of access rights
	Lack of audit trail
	Poor password management
	Sensitivity to voltage fluctuations
	Sensitivity to temperature fluctuations
	Incorrect parameter setup
	Incorrect placement of equipment or data cables
	Flaws in the software

Appendix 5 Threats and weaknesses affecting Systems

Threat	Systems and resources affected	Weaknesses	The most serious consequence	Likelihood	Severity of consequences	Risk classification

Appendix 6 Risk Matrix

PROBABILITY		CONSEQUENCE				
		Minor (A)	**Light (B)**	**Severe (C)**	**Very severe (D)**	**Catastrophic (E)**
	Very High (5)	Low **(R²)**	Medium **(R³)**	High **(R⁴)**	Very High **(R⁵)**	Very high **(R⁵)**
	High (4)	Low **(R²)**	Low **(R²)**	Medium **(R³)**	High **(R⁴)**	Very High **(R⁵)**
	Medium (3)	Very Low **(R¹)**	Low **(R²)**	Medium **(R³)**	High **(R⁴)**	high **(R⁴)**
	Low (2)	Very Low **(R¹)**	Very Low **(R¹)**	Low **(R²)**	Medium **(R³)**	High **(R⁴)**
	Very Low (1)	Very Low **(R¹)**	Very Low **(R¹)**	Low **(R²)**	Medium **(R³)**	Medium **(R³)**

Appendix 7 A list of risks in order of priority according to risk class

Risk	Risk classification	Measure	Estimated cost of the measure	Responsible for implementing the measure	Deadline for implementation of the measure