ORIGINAL TEXT - FULL TEXT

Approved by order No 105 of 29.04.2024 of the Director for Administration

In force from: 29.04.2024

Guidelines for Information Security Risk Management

Table of Contents

1 General provisions

Risk management (hereinafter referred to as “risk management”) is a set of coordinated activities to direct and control an organization with regard to risk.

The purpose of risk management is:

- to maintain the lowest level of economically justified risk that ensures the business continuity and long-term competitiveness of the university;
- to identify and manage risks associated with the university’s activities, taking into account the scope and complexity of the processes and the existing experience;
- to establish a foundation for self-assessing risks and implementing measures to prevent losses caused by risks.

Information security risk management focuses on information systems and IT assets (by addressing risks related to confidentiality, integrity, and availability). **Risk management** supports the information security risk management (ISRM) process. Risks affecting the university are systematically and continuously identified, assessed, treated and monitored.

2 Risk management process

The risk management process consists of the following stages:

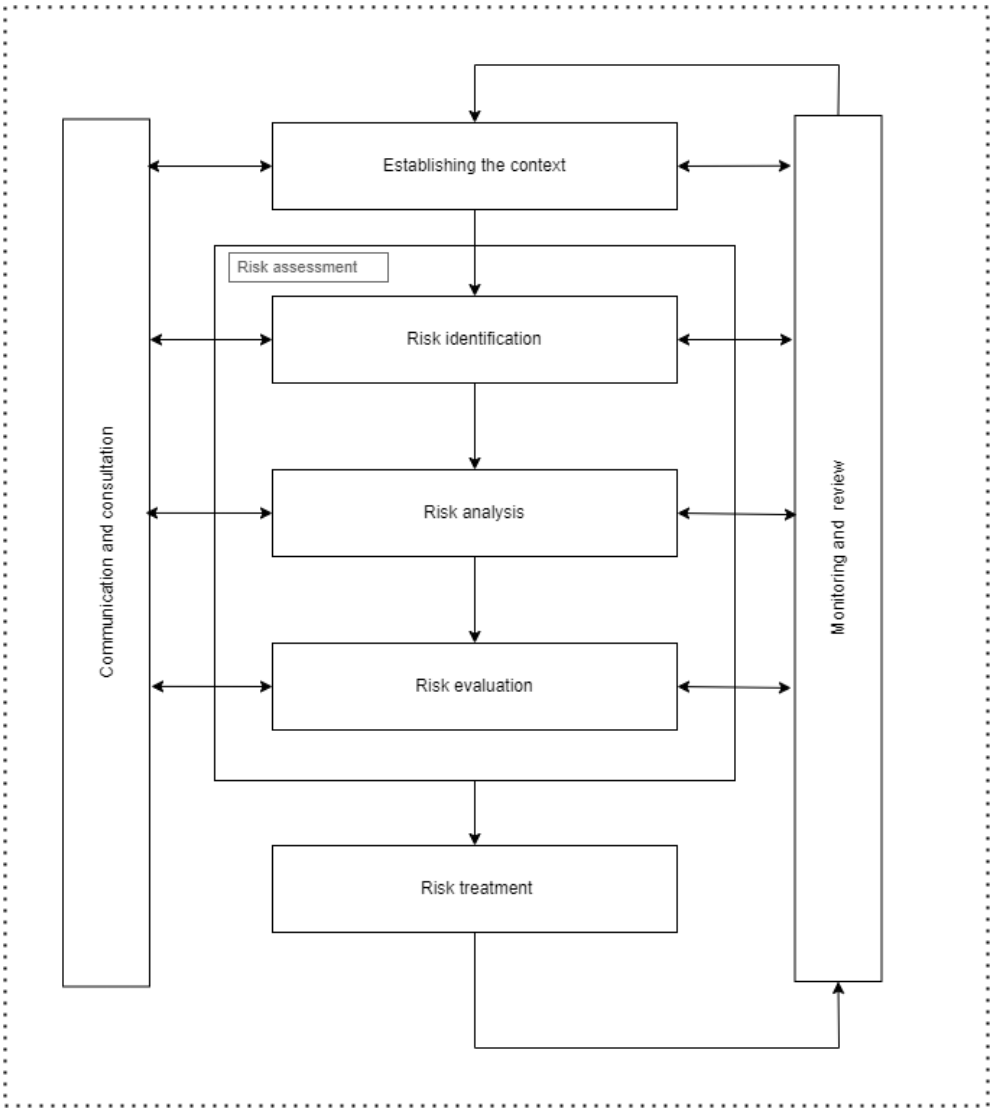

Figure 1 Risk management process

2.1 Establishing the context

The framework for managing risks shall be designed considering both the internal and external context of the university.
Examining the external context should include the following:

- the social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;
- key drivers and trends affecting the objectives of the organisation;
- external stakeholders' relationships, perceptions, values, needs, contractual relationships and commitments;
- the complexity of networks and dependencies.

Examining the external context should include the following:

- the organisation's vision, mission and values;
- governance, organisational structure, roles and accountabilities;
- strategy, objectives and policies;
- the organisation's culture;
- standards, guidelines and models adopted by the organisation;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);
- data, information systems and information flows,
- relationships with internal stakeholders, taking into account their perceptions and values;
- contractual relationships and commitments.

2.2 Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk assessment is performed based on the information system and information assets. **Risk assessment is performed at least once a year.** In addition, risk assessment is performed in the event of any significant change to a system.

RISK IDENTIFICATION

The purpose of risk identification is to identify any incidents or situations that may affect the achievement of the university's objectives, the performance of its tasks and its planned operations. A risk exists when there is a threat that can exploit a vulnerability in the university. Depending on the specific field, there may be a variety of threats and vulnerabilities that must be identified, documented, and analysed.
The following sources may serve as input for identifying risks:

- public or internal statistics,
- survey results,
- expert assessments,
- recorded incidents, their analysis and experience gained,
- experience gained from previous risk assessments,
- external party experience and/or materials, assessments.

Each identified risk is assigned a unique identifier and documented in a reproducible format. In subsequent stages of risk management, this information will be supplemented with additional details. Risks are recorded in the risk register (in JIRA).
Risks are defined using the following structure: **a 'risk factor' induces a 'risk event', which causes 'loss or impact resulting from the risk'.**

Identifying risks within information systems and IT assets

When identifying risks to information systems and IT assets, an impact analysis is first conducted based on the nine categories outlined in Annex 1. The results of the impact analysis are documented in JIRA in the information system or IT asset map.
Further risk identification and analysis for information systems is not required if the following conditions are met:

1. the average score across the nine categories of the impact analysis is less than 3;
2. none of the nine impact categories receive a score of 4 or 5.

In case of an information system or IT asset with an average impact analysis score of 3 or higher, or a score of 4 or 5 in one or more categories, the risks contributing to the high score must be identified. Both internal and external risks — those occurring within information systems the university has control over, as well as those beyond its control—must be identified. In the course of identifying risks, the potential impact of a confidentiality, integrity, and/or availability breach on assets must be ascertained.
Vulnerabilities can be found in the following areas: organisational structure, processes and procedures, administrative routines, personnel, physical environment, configuration of the information system , hardware, software or communication devices, dependency on external parties. Source data shall be provided by the owners of the information systems or information technology assets, process managers, IT project managers, superusers, IT project managers, partners and other related parties.
The output of identifying information systems and IT assets is a list of risks, which includes the following:

- the name of the information system or IT asset;
- the name of the information system or IT asset component (such as a server, database, etc.);
- the vulnerability, i.e. the weak point, in an IT asset, information system, or process, or the inadequacy or absence of a security measure (security gap). (The existence of a weakness does not cause any losses in and of itself);
- the attacker and the attack method capable of exploiting the weakness/vulnerability (who, how, and what). These threats can cause significant loss and are realistic for a specific application and use. According to the Estonian Information Security Standard (E-ITS): elementary threats, module threats, or external threats);
- the risk factor (i.e., when a threat exploits a vulnerability);
- the risk event (confidentiality, integrity and availability);
- the description of the risk impact (effects, damage, consequences).
- the largest possible loss (loss of service, financial loss, loss of reputation,
- the risk (risks are defined using the following structure: a ‘risk factor’ induces a ‘risk event’, which causes ‘loss or impact resulting from the risk’.)
- risk owner (the business project manager of the information system or the owner of the IT asset).

Each identified risk is assigned a unique identifier and recorded in the risk register in Jira. In subsequent stages of risk management, this information will be supplemented with additional details.

RISK ANALYSIS

The purpose of risk analysis is to provide information for risk evaluation in order to determine how to manage identified potential risks and allocate the available resources effectively to address the most critical risks.
During the risk analysis, the **risk owner** determines the **probability of occurrence** of the identified event and the possible consequences, i.e. losses, or the **risk impact**.

Upon impact assessment, or analysis of the consequences, the risk owner shall describe the potential losses that accompany the materialisation of the risk, or exploitation of a vulnerability. The consequence analysis must identify all potential consequences should the risk materialise. When assessing the impact of consequences, it is essential to consider the different types of risks addressed by risk management in combination, taking into account the cumulative effect of multiple risks.
A probability analysis identifies the likelihood of the risk materializing. To assess the likelihood, information can be gathered from various sources, including:

- incident history, i.e. statistics;
- prognosis, considering the age of the devices, etc.;
- expert assessment;
- comparison with other similar organizations.

If information about potential consequences and/or the likelihood of occurrence is unavailable, creating uncertainty, the nature of this uncertainty must be considered in decision-making (the decision-makers must be informed thereof). The likelihood of risks shall be assessed based on the scores in table 2.

Table 1 Risk impact assessment

Impact assessment	Score	Criteria
Negligible impact	1	If the risk materialises, the university's operations are only minimally disrupted (the operation of minor services, information systems, or IT assets is affected or their use is hindered temporarily or over a longer period, a few dissatisfied and concerned users, the potential financial losses are minimal, and no additional resources are required). If the risk materialises, personal data are not at risk, the information systems and IT assets process public information, and the integrity of the data is non-critical. Does not affect the achievement of the university's objectives.
Minor impact	2	If the risk materialises, operations are partially disrupted (the performance of several services is affected, and there are service disruptions, but the disruptions can be managed and resolved operationally (within one to three working days). A few users (10-100) are affected and express dissatisfaction; financial losses are minor; regulators express interest by making inquiries should the risk materialise. If the risk materialises, information intended for internal use may be exposed to the public, but personal data is not at risk. The achievement of the university's objectives is not at risk.
Moderate impact	3	If the risk materialises, the university's operations are significantly disrupted (several services are affected, and the disruptions cannot be resolved operationally (within three working days); a moderate number of persons (100-500) are affected and express dissatisfaction; the financial losses are moderate (up to 50,000 euros), there may be a single negative media article; regulators take a keen interest in the organisation's activities; there are legal disputes between the parties). If the risk materializes, sensitive or critical restricted data (e.g., individuals' salaries) could be exposed to the public, and personal data may be compromised. Additional resources may be required to restore the original situation, but the university's objectives can still be achieved.
Major impact	4	If the risk materializes, the university's operations are significantly disrupted (several critical and essential services are affected and the disruptions

		cannot be resolved operationally (within three working days); a significant number of users (500-5,000) are affected and express their criticism publicly; there is a substantial financial loss (up to 100,000 euros), occasional negative media articles; regulators are highly interested in intervening in the organization's activities; there are ongoing extrajudicial disputes between the parties; sanctions have been partially imposed). If the risk materialises, special categories of personal data or classified data are at risk, and there is a likelihood of breach of processed personal data. Significant additional resources are required to restore the original situation. As a result, the university's core activities may be halted, preventing the achievement of its established objectives.
Critical impact	5	If the risk materializes, the university's operations are critically disrupted (long-term disruptions of critical services that cannot be resolved within a week); more than 5,000 users are affected, expressing openly their dissatisfaction and desire to opt out; resulting in huge financial loss (exceeding 100,000 euros); significant damage to the organization's reputation due to extensive negative media coverage, regulators have extreme interest in interfering with the organization's activities; accompanied by court action, legal proceedings, sanctions. If the risk materializes, the university's most critical data are at risk (can be exposed, destroyed, or otherwise compromised) with a high likelihood of a personal data breach. Restoring the original situation requires significant additional resources, and in some cases, restoration may be impossible If the risk materializes, the university's core activities can be halted, preventing it from achieving its set objectives.

Table 2 Risk likelihood assessment

Likelihood assessment	Score	Criteria
Highly unlikely	1	The risk is primarily theoretical and occurs very rarely in practice; likely to occur less frequently than once every 10 years.
Unlikely	2	The risk could materialize, though practical examples are rare. It can occur within the next 2–3 years.
Possible	3	There is evidence that the risk is likely to materialize and can occur within the next 2–3 years.
Likely	4	There is evidence that the risk is likely to materialize and can occur within the next year.
Certain	5	The risk has occurred in the past or is considered inevitable, with potential to materialize within days or weeks.

When analysing a risk and assessing its impact, it is essential to consider not only the risk itself but also the underlying causes, the source, and the motivational forces driving the source's behaviour. To analyse a risk realistically, it is important to consider the controls and measures already applied to mitigate it.
As a result of risk analysis, the risk level is defined, which is essential for prioritising the approach to risk treatment in subsequent steps.

Risk level

The risk level is calculated by multiplying the impact score by the likelihood score. Based on the risk level, a risk matrix is created, and all risks are prioritized from the highest to the lowest. **When several risks have the same level, priority is given to the risk with the higher impact score.** Risks are identified and the risk level is determined based on table 3 below.

Table 3 Risk level calculation

Likelihood						
Impact		Highly unlikely (1)	Unlikely (2)	Possible (3)	Likely (4)	Certain (5)
	Critical impact (5)	5 – low	10 – medium	15 – medium	20 – high	25 – critical
	High impact (4)	4 – very low	8 – low	12 – medium	16 – high	20 – high
	Moderate impact (3)	3 – very low	6 – low	9 – low	12 – medium	15 – medium
	Low impact (2)	2 – very low	4 – low	6 – low	8 – low	10 – medium
	Negligible impact (1)	1 – very low	2 – very low	3 – very low	4 – very low	5 – low

Risk level = Impact score * Likelihood score

Adjusting the risk level

The level of risk may be adjusted subjectively when there is a valid reason to do so, but it is essential to document the rationale for this decision in writing.

RISK EVALUATION

The purpose of a risk evaluation is to ensure that an organization effectively allocates its resources to address the most critical risks. It is important to remember that multiple small, frequent risks can collectively have a significant overall impact.

Risk evaluation involves comparing the risk level identified in risk analysis against accepted risk thresholds. (Table 4 The university's risk thresholds and corresponding actions for each risk level). The whole risk assessment process must be documented.

The university's risk thresholds, i.e. risk acceptance criteria

Table 4 The university's risk thresholds and corresponding actions for each risk level

Risk level		Action
1-4	Very low	The risk is accepted, monitored at least once a year.
5-9	Low	The risk is accepted, monitored at least once a year.
10-14	Medium	The risk will be addressed when possible. If the decision is made to accept the risk, the risk owner must provide a written justification. The risk is monitored at least once a year
15-19	High	The risk needs to be addressed. The risk owner must prepare an action plan. The risk is monitored at least once every 6 months.
20-25	Critical	The risk requires an immediate decision by the Rector's Office and action. The risk owner must inform the Rector's Office of the risk, provide an explanation, and propose measures for managing the risk. The risk shall be monitored, and actions shall be taken in accordance with the deadlines set out in the decision of the Rector's Office.

The actions and the frequency of risk assessments for different risk levels are outlined in Table 4. Risk acceptance is allowed only when the risk score is below 10 and further mitigation measures are not feasible or practical.

3 Risk treatment

All risks that do not meet the risk acceptance criteria must be reduced to an acceptable level through alternative measures. To achieve this, the appropriate risk treatment measure must be selected for each identified risk. The Chief Information Security Officer shall prepare a risk treatment plan. The goal is to reduce identified risks so that the residual risks are acceptable (at least low or moderate). Depending on the nature of the risk, the appropriate risk treatment measures must be selected and defined for each risk, including the required actions, deadlines, and responsible parties.

3.1 Risk avoidance

Risk avoidance involves avoiding activities or conditions that pose the risk, such as discontinuing the use of certain equipment, relocating to another area, etc. During the risk avoidance process, new risks may arise as a result of the changes implemented, which will require additional risk management measures.

3.2 Risk mitigation

Risk mitigation involves implementing additional measures/controls, or eliminating or modifying existing ones, to decrease the impact and/or likelihood of the risk, resulting in an accepted risk level when reassessed. (For example, E-ITS or ISO 27001 information security controls can be implemented).
Risk mitigation measures must be selected to ensure that the risk level is reduced to an acceptable level after implementation of the measure. In addition, factors such as time, budget, technical constraints, etc. must be taken into consideration when selecting a measure. The conditions and options for accepting risks are set out below.

3.3 Risk sharing/transfer

Risk sharing involves transferring a risk to a another (external) party who can best manage that particular risk (e.g. insurance, outsourcing, etc.). It is important to remember that while risk management activities can be shared or transferred to another party, ultimate responsibility still remains with the risk owner. Risk sharing may generate new risks, which will require additional risk management measures.

3.4 Risk acceptance

Risk acceptance involves a deliberate decision to take no further action with regard to the risk and accepting the risk. Accepted risks must also be monitored. If the risk level does not meet the risk acceptance criteria but accepting and retaining is still preferred, the decision must be justified and documented. Such a decision must be approved by the Rector’s Office. In this case the status of the risk is marked as ‘Open’.

RESIDUAL RISK

As a rule, some residual risks remain at a certain level after risk treatment. In most cases, the residual risk is at a level that can be accepted under the risk criteria. There is no residual risk if the threat or vulnerability is eliminated entirely, meaning the risk no longer exists.

4 Monitoring and reviewing risks

Risk owners must consistently monitor identified risks, the effectiveness of the treatment measures, and any new risks that may have emerged.
Process managers, business project managers of information systems, IT project managers, IT asset owners, and other stakeholders conduct continuous monitoring to identify new risks and shall promptly notify the Chief Information Security Officer when a risk is identified. Once a new risk is

identified, the risk assessment process is carried out by the relevant risk owner, with guidance from the Chief Information Security Officer as needed.

5 Communicating. Informing. Consulting

Risk management associated with information systems and IT assets is centralized, with risks recorded in a shared tool that ensures timely communication of risk related information to relevant parties, while maintaining transparency throughout the risk management process.
Risk information is provided through consultations, training sessions, and informational materials. Risk communication guarantees the harmonisation of the values and the repeatability of risk management steps in an organisation. Risk communication ensures the coordination of various impressions of risks so that the entire organisation is aware of the process and the results of the risk management.

6 Roles

6.1 The Director for Administration:

- approves the information security risk management procedure;

6.2 The Chief Information Security Officer:

- is responsible for the development and implementation of the information security risk methodology;
- provides advice, guidance, and training;
- compiles a comprehensive overview of information security risks based on recorded incidents;
- analyses incidents and related information security risks;
- if needed, requests additional information about the circumstances of an incident from the person who recorded and/or the person who resolved it;
- provides the Rector (the Rector's Office) with an annual overview of the organization's information security risk management;
- recommends improvements to the risk management process.

6.3 The risk owner

- A risk owner is a person (a business project manager for information systems or an IT asset owner) who assesses and manages risks, prepares a risk treatment plan, and is responsible for its implementation within his/her area of responsibility.
- The owner shall assess the impact and the likelihood of the occurrence of the risk, decide on the treatment measures and the persons responsible, incl. agrees on the persons responsible and mitigation actions also outside of his/her area of responsibility if these are required to manage the risk.

7 Annex 1

Impact analysis

Tabel 5 Impact assessment

Consequences	Minor impact	Limited impact	Moderate impact	High impact	Critical impact
Score	1	2	3	4	5
Achievement of the university's objectives	Operations are minimally affected, but the objectives can be achieved without requiring additional resources.	Operations are significantly disrupted, but the objectives can be achieved by reallocating resources within the university, without compromising the achievement of other objectives.	Operations are significantly disrupted, but the objectives can be achieved by reallocating resources within the university, though this may partially compromise the achievement of the objectives.	Operations are significantly disrupted, and significant additional resources are required to achieve the objectives.	The university's objectives cannot be achieved, and its core processes are not functioning.
Reputational damage	Negative rumours circulating among a small group of customers, a few customer complaints.	• Negative rumours circulating among customers, partners, the public. • Regulators express interest in the organisation's activities by making inquiries.	• A single negative media article. • Regulators' keen interest in the organisation's activities. • The university's credibility is called into question.	• Occasional negative media articles. • Many users openly express criticism. • Regulators' keen interest or interference in the organisation's activities. • A substantial decline in the university's credibility.	• Significant harm to the organization's reputation due to extensive negative media coverage. • Many users express criticism and a desire to opt out. • Regulators' extreme interest or interference in the organisation's activities.

					• A critical decline in the university's credibility.
Affected parties	1-10 users	10-100 users	100-500 users	500-5,000 users	More than 5,000 users
Legal obligations	An oral warning.	A written warning.	Extrajudicial disputes, an agreement between the parties is possible.	Extrajudicial disputes, an agreement between the parties is possible, partial sanctions.	Followed by legal proceedings, litigation and sanctions.
Accompanying costs	up to 2,000 euros	2,000 – 10,000 euros	10,001 – 49,999 euros	49,999 – 100,000 euros	More than 100,000 euros
Availability	The operation of individual minor services is affected or temporarily disrupted, but the overall functioning of the university remains unaffected.	The expected performance of several services is affected, with service disruptions that can be addressed operationally, without affecting the overall functioning of the university.	Several services are affected, and the disruptions cannot be resolved operationally (within three working days). The university's several key processes have been affected, causing partial disruption to the university's operations.	Several critical and essential services are affected, and the disruptions cannot be resolved operationally (within three working days). The university's core activities are affected, leading to significant disruption to its operations.	Long-term disruptions to critical services that cannot be resolved within a week. The university's core processes have been severely affected, causing a partial disruption to its operations.
Integrity	Data integrity is not a priority, and no separate integrity checks or logging operations are required.	Data integrity is important, and it is essential to track any changes made.	Data integrity is important, and it is essential to track changes, including the identity of the person making the changes, the timestamp, the source and destination of the request, the request details, and the response received.	Data integrity is crucial, and it is essential to track changes, including the identity of the person making the changes, the timestamp, the source and destination of the request, the request details, and the response received.	Data integrity is crucial; and it is essential to track changes, including the identity of the person making the changes, the timestamp, the source and destination of the request, the request details, and the response received. It is also crucial to verify the integrity

					of data, i.e. to perform data integrity checks using cryptographic techniques and to implement control processes to confirm data integrity.
Confidentiality	The information assets are associated with or process information intended for public use.	The information assets are associated with or process data and information intended for internal use.	The information assets are associated with or process sensitive or critical restricted data (e.g. salaries, etc.)	The information assets are associated with or process special categories of personal data and/or the university's secret information.	The information assets are associated with or process the university's critical secret information.
Privacy	No personal data.	A breach of processed personal data is unlikely.	A breach of processed personal data is possible.	A breach of processed personal data is likely.	A breach of processed personal data is highly likely.