UPPSALA UNIVERSITET

Dnr UFV 2018/211

Risk management

Procedures for information security

Ratified by the Chief Security Officer	2018-01-29
Latest revision date	2021-08-15
Translation date	2021-10-06

Table of contents

1 Introduction

The following procedures describe a process for assessment and addressing of security risks in information systems or other information management.

The procedures are part of the university's overall routines for information security (UFV 2017/93), which are based on the Swedish Civil Contingency Agency's regulations on information security for governmental authorities (MSBFS 2020:6).

These procedures replace previous procedures for risk management of information systems (UFV 2015/322).

2 Definitions

Organization refers in this document to an organizational unit, e.g. department or equivalent, or a project, a project management system etc.

Information or *information assets* include all digital, paper-based, verbal or in other ways stored or communicated information.

Information resource refers to information as defined above as well as the information systems (hardware and software) and communication solutions that handle the information.

Threat. A possible unwanted event which would have negative consequences for the business.

Probability. A measure of how likely it is that a threat results in a negative event.

Consequence. The result of a threat resulting in a negative event. May be financial, reputational or e.g. legal impact.

Risk. The probability and consequence of a threat resulting in a negative event.

Gap analysis. Identification of the difference between implemented security measures and the security measures that are identified as necessary.

3 Purpose

These procedures are intended to provide practical and domain-specific support for continuous risk management of the university's information resources with regard to confidentiality, integrity and availability.

4 Goal

That the university's information resources are protected in accordance with the university's current procedures for information security (UFV 2017/93).

5 Process

The risk management process in its entirety is carried out in the steps described below. Each of the steps can also be performed separately or in a combination with other steps. It is important to note that the result from the information classification always is a prerequisite in order to be able to proceed to the subsequent steps.

1. Scoping
2. Consequence analysis (with regard to system failure)
3. Information classification
4. Requirement analysis
5. Risk analysis
6. Management of identified security vulnerabilities

6 Approach

It is recommended that the process is carried out in one or more workshops with representatives from the relevant department, division or working group, preferably with a process leader from the university's security division.

The form of work that is recommended is one or more workshops with representation from the relevant organization or working group, preferably with a representative from the university's security department leading the workshop.

7 Implementation

7.1 Scope

Before information classification and the subsequent steps can begin, the scope must be defined. If the information and the information resources that are going to be risk-assessed are relatively homogeneous, all or parts of the process can be used for groups of systems, an e-area, a research project, a development or procurement project, etc.

If the systems are deemed to be more heterogeneous, it is recommended that the risk assessment is conducted for one system at a time. The process can also be used for risk assessments that go beyond the scope of relevant system environments, for example to analyze the overall information management at one department.

7.2 Consequence analysis

When conducting a consequence analysis, an assessment of the consequences that system failure causing different lengths of downtime can have for the area of operation is done. This step is not a mandatory step in the risk management process, but can be advantageous to carry out for systems with high demands on availability.

The template in Appendix 1 can be used as support for carrying out the consequence analysis.

7.3 Information classification

Information classification is the basis for secure information management – a process where the required level of protection of the information is determined based on the aspects of confidentiality, integrity and availability.

Confidentiality	Information must not be made available or disclosed to unauthorized parties, systems or processes.
Integrity	Information must not be modified or destroyed, either by unauthorized parties, by mistake, or due to system failure.
Avaliability	Information must be accessible and available for use in the expected manner, and within the desired time.

Information classification is carried out by the organization that owns the information.

The required level of protection with regard to each of the information security aspects mentioned above, must be classified in one of the levels between 0 and 3. The classification value of an information asset is expressed in a three-digit number combination, for example 321, where the initial digit refers to the assessment for the confidentiality aspect, the second digit for the integrity aspect and the third for the availability aspect.

Appendix 2 can be used as support for carrying out information classification. Appendix 6 is a tool for implementing and documenting classification results.

NB! A copy of results from completed information classifications must be sent to the Security Division. Contact security@uu.se for more information.

7.4 Requirement analysis

The requirement analysis is closely associated with information classification since requirement analysis is aimed at a system or a group of systems. In the requirement analysis step, the result from the information classification is mapped against the system or systems that are relevant in the context. In this step classification values for the information assets in question are initially transferred from Appendix 6 to Appendix 3.

The highest classification value for each of the aspects (confidentiality, integrity and availability) among the information assets that the system handles is used to select the correct set of requirements to place on/have on the system.

Example: a system handles information assets A, B and C - classified as follows:
Information asset A: 132
Information asset B: 331
Information asset C: 222
In this example, the current system being analyzed needs to meet the requirements corresponding to the security level 332.

The step of selecting requirements from the list of all requirements is carried out with the support of the appendix specified below.

In the requirement analysis, the level of compliance with the university's routines for information security (UFV 2017/93) is assessed/examined.

The security areas covered by the guidelines and objectives for the security measures in these areas are described below.

procedures/guidelines	The university's guidelines for information security are known within the organization.
Organization and responsibilities	Responsibilities and areas of responsibility for information security work are stated within the organization.
Employee safety	Employees and other related parties are aware of their own responsibilities for information security.
Asset management	The information resource(s) are protected in an appropriate manner.
Access control	Only authorized users have access to the information resource(s).
Encryption	Sensitive information is protected by encryption.
Physical and environmental security	Premises and system equipment are protected against unauthorized access, damage and interference.
Operations security	The operation of the information resource(s) takes place in a correct and secure manner.
Communications security	Data transmission to and from the information resource(s) is protected in an appropriate manner.
Procurement, development and maintenance of systems	Information security is managed as an integral part of the information resource(s) over its entire life cycle.
Provider relations	Information security requirements according to the university's guidelines are regulated in agreements with external providers.
Incident management	Procedures for handling information security incidents are known within the organization.

Continuity management	The organization has a documented and verified plan for access to the information in a crisis or disaster situation.
Compliance	The organization complies with regulatory and contractual information security requirements and obligations.

NB! A copy of the results of the completed requirement analysis must be sent to the Security Division. Contact security@uu.se for more information.

7.5 Risk analysis – A method for risk assessment

The risk analysis assesses the threats that the organization faces due to previously known or suspected security vulnerabilities or the vulnerabilities that are detected during the implementation of the requirement analysis. For each of the identified threats the consequences that the threat resulting in a negative event could have on operations as well as the probability of the threat resulting in a negative event is assessed.

For each identified threat, a *risk factor* is calculated balancing the assessed levels of consequence and probability. The risk factor categorizes the risk into one of the following groups that indicate how the risk is to be managed by the organization.

Negligible risk (försumbar risk)	Accept
Low risk	Monitor
Medium risk	Plan to implement a risk mitigation measure at the appropriate time, e.g. version upgrade or equivalent.
High risk	Immediate action is required.

Appendix 4 can be used as support for carrying out the risk analysis.

7.6 Management of the identified security vulnerabilities

In a situation where security vulnerabilities have been identified in connection with a requirement analysis, there is a clear indication that the analyzed system does not meet the required level of security. Every identified vulnerability therefore needs to be analyzed and assessed by carrying out a gap analysis. The results from the gap analysis provide a basis for appropriate risk-mitigating measures.

Appendix 5 describes how identified vulnerabilities should be handled and reported.

8 Incident management

All incidents must be reported to the University Service Desk (servicedesk@uu.se).

This applies to all the incident types described below:

- An incident that has affected the confidentiality, integrity or the availability of the information deemed to be in need of extended protection, or
- meant that information systems that process the information that is deemed to be in need of extended protection have not been able to maintain the intended functionality, or
- affected the authority's ability to carry out its mission, or
- may otherwise seriously affect the security of the information management for which the authority is responsible, or in services that the authority provides to another organization.
- has affected the confidentiality, integrity or availability of personal data. An incident has occurred if personal data has been destroyed, unintentionally or illegally, lost or altered or disclosed to any unauthorized person.

The service desk will then assess which incidents, if any, that are to be reported to MSB or to the Swedish authority for privacy protection (IMY), in accordance with current regulations.

9 Appendixes

Appendix 1 – working document for carrying out consequence analysis

Appendix 2 – instructions for carrying out information classification

Appendix 3 – working document for carrying out requirement analysis

Appendix 4 – working document for carrying out requirement analysis

Appendix 5 – working document for management of identified security vulnerabilities

Appendix 6 – working document for carrying out information classification