Stockholms universitet

Rektor

DECISION
26/01/2017

Ref. no. SU FV-2.11.2-1923-16

Administrator:
Benita Falenius Information
Security Coordinator IT Services

Guidelines for Information Security at Stockholm University

Stockholms universitet

Table of contents

Stockholms universitet

Stockholms universitet

1. Introduction

Information security – *A state of protection with regard to the confidentiality, availability, integrity and traceability of information*.

Information and associated information technology constitute a resource that is extremely important to the operations at Stockholm University. Good information security safeguards the information that is of importance to the University. Work on information security is about protecting information assets (assets related to information and information processing resources) against various types of threat.

One prerequisite for information security work to be performed in a structured manner is the existence of a list of these information assets and their owners as well as compliance with applicable laws and regulations. This is secured through an operations analysis that includes a risk and vulnerability analysis.

Information security work is based on established standards. These contain a number of security categories that are to support the work of information security. Work on these security categories is a part of the operations analysis. Each organisation makes an assessment of the safety categories that are relevant to their operations and that are to form the basis for their information security work. Information security work also includes incident management and business continuity management in the case of a serious event and disruption.

The following describes how the work on operations analysis, security categories, incident management and business continuity management is to be performed.

As regards physical security, please refer to *Guidelines for Physical Security*.

1.1. Purpose

Inadequate information security can have both serious and immediate consequences both for staff and students and for the University as a whole. The University currently manages a large quantity of highly important information. This information needs to be protected against unauthorised access (*protection of information confidentiality*) but also needs to be available to authorised persons at the time it is to be used (*protection of information availability*). In certain cases, the need for availability is so high that in practice no disruptions are acceptable. The information also needs to be protected against unauthorised changes (*protection of information integrity*). In order to ensure that these needs continue to be met, it is of fundamental importance that it is subsequently possible to trace who has done what in the University's systems (*protection of information traceability*) – something also required in existing legislation.

Stockholms universitet

1.2. Responsibility

The Vice-Chancellor has the overall responsibility for information security at Stockholm University.

The Director of Administration makes decisions in matters concerning the University's security, including information security. The Director of Administration has, however, delegated the decision-making power in questions concerning the University's IT security and responsibility for coordination and consultation on the University's information security work to the head of IT Services. However, matters of principle are determined by the Director of Administration.

At each department/equivalent[1], the head of department/equivalent[2] is responsible for information security. Heads of department are to ensure that instructions and procedures exist within their own organisations and that these are, among other things, based on the security categories and associated security measures. Where the department uses central IT services, the head of IT Services is responsible for ensuring that instructions and procedures exist.

Every member of staff is obligated to maintain an adequate level of information security and to point out deficiencies in information security to a superior.

All employees, students, visitors and partners are to comply with the laws, rules, regulations and guidelines that are applicable to the University.

1.3. Central support

To provide departments with support and guidance in questions concerning information security, IT Services has a central information security function. The role of this function is to provide consultation with respect to all operations at Stockholm University. It can, for example, be consulted on the production of guidelines and procedures and participate in the work on the operations analyses that are a part of information security work. The information security function is to continuously plan, train, support, evaluate and improve information security work at the University.

1.4. Evaluation and follow-up

Every year, IT Services is to make a university-wide compilation of the assets and risks concerning information and information technology. Evaluation and follow-up of the work on information security is based on the work on the security categories and

[1] Department hereafter also refers to centres and institutes that are at the same organisational level as departments and to divisions within the University Administration.
[2] Head of department hereafter also refers to the directors of centres and institutes that are at the same organisational level as departments and to heads of division within the University Administration.

Stockholms universitet

the security measures. This then forms the basis for calculating key risk indicators (KRI), which show the general risk level at the department and at the University as a whole. This calculation is performed by IT Services.

1.5. Governing document

Guidelines for Information Security is one of the University's governing documents and is supplemented by underlying instructions and procedures. The guidelines give concrete expression to the University's security policy and are intended to create conditions for a systematic work on information security at the University. They are based on the following ordinances, regulations and standards.

- SFS 2015:1052 Ordinance on Emergency Preparedness and Surveillance Responsible Authorities' Measures at Heightened Alert
- MSBFS 2016:1 Regulations and general advice on the information security of central government agencies
- MSBFS 2016:2 Regulations and general advice on the IT incident reporting of central government agencies
- SS-ISO/IEC 27001:2014
- SS-ISO/IEC 27002:2014
- SS/ISO 22301:2012

2. Operations analysis including risk and vulnerability analysis

2.1. Purpose

Operations analysis is to lead to a structured list of information assets and their owners and is to ensure compliance with applicable laws and regulations[3]. This list is to classify the most important information assets of operations based on the capability to maintain *confidentiality*, *integrity, availability* and *traceability*.

Risk and vulnerability analysis is to provide good insight into local threats and risks and to help give an aggregate picture of the information security risks and of the needs for security measures at a university-wide level. It can be useful to make this analysis a part of the annual process for operations planning as the risks we wish to eliminate might entail a cost and should then be able to be taken into account in the annual budget process.

[3] Public Access to Information and Secrecy Act, Personal Data Act, Archives Act, Archives Ordinance, the National Archives' regulations and general advice on electronic documents, etc.

Stockholms universitet

Together with risk and vulnerability analysis, operations analysis defines the protection needs that information assets of operations have.

2.2. Responsibility

The head of department is responsible for the implementation of an operations analysis including risk and vulnerability analysis. IT Services supports heads of department in the implementation of analysis via the information security function.

2.3. Activities

Operations analysis is a composite analysis made up of the following activities:

- *Inventory of the most important information assets of operations and their owners*
  The purpose of the inventory of information assets is to identify the operations' important assets and supporting resources. The owner of the information asset is also to be identified. Examples of important assets are research information, educational material, documentation for examinations and administrative information, such as various agreements and budgets.
- *Information classification*
  The purpose of information classification is to evaluate identified information assets based on the capability to maintain confidentiality, integrity, availability and traceability. In light of this classification, assets are to be given an appropriate level of security measures, e.g. procurement documents are to be treated with confidentiality until a contract award decision has been issued.
- *Risk and vulnerability analysis for the identification of risks to information assets and of the consequences of these risks and the probability of their occurring*

  The purpose of risk and vulnerability analysis is:

  - to identify and assess risks, on a scale from 1 to 4, based on the consequences that they have for operations and on how great the probability is of their occurring
  - to prioritise the order in which risks are to be managed and measures taken
  - to involve stakeholders when decisions about the management of risks are made and to keep them informed of the status of risk management and its effect
  - regularly monitor and review risks and the risk management process
  - to train managers and staff at the department about the risks and the measures taken to manage them
  - to gather information in order to identify university-wide risks

Stockholms universitet

- *Inventory of legal requirements and requirements of operations*
  The purpose of the inventory of legal requirements and requirements of operations is to identify all internal and external requirements that concern operations and their management of information assets. External requirements are all relevant legal requirements, such as the Personal Data Act (1998:204), the Public Access to Information and Secrecy Act (2009:400), etc. Internal requirements are the University's internal rules that are contained in the University's Rule Book.
- *Observance of security categories and their security measures*
  As regards the security categories, there is a number of recommended security measures that are to have been observed (see Chapter 3). These categories and measures, which are based on established standards, are such as the University assesses to be relevant to the University as a whole. The owners of the information assets need to take a position on whether these are relevant to their own operations. The security measures assessed to be relevant are graded according to the degree to which they have been implemented. The goal is for the security measures that are assessed relevant to be 100% implemented and for it to thereby be ensured that the necessary instructions and procedures exist. The measures that are relevant but not implemented are to be included in the plan of measures. The assessment of the degree to which a measure has been implemented is made by the asset owner.

  The security categories are:

  - acquisition, development and maintenance of systems
  - access control
  - operational reliability
  - communications security
  - supplier relations

Operations analysis is to result in a report showing status and the measures that are intended to be taken. Departments are to update the operations analysis with an appropriate periodicity, but at least every two years. Operations analysis is preferably performed with the support of IT Services.

Risk and vulnerability analyses are to be performed on the following occasions:

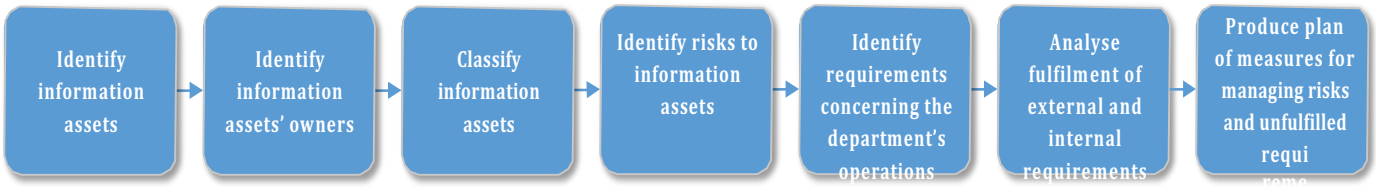
- in conjunction with major changes to operations (e.g. organisational change or relocation)
- ahead of the procurement of cloud services
- ahead of signing a personal data processor agreement with an external supplier

The performance of an operations analysis varies in scope and is to be adapted to its purpose. The normal expenditure of time is about 3 hours. The expenditure of time for only performing a risk and vulnerability analysis is about 1 hour.

Stockholms universitet

2.4. Process for operations analysis

As it is essential to the whole of Stockholm University to maintain good information security, it is important that the guidelines in this document are complied with. A guidance process has been produced in order to facilitate a systematic work on information security.



The purpose of this process is to provide a common procedure in order to achieve a systematic work on information security. The process is always carried out on the basis of the department's perspective. For a more detailed description of the process see Appendix 1.

3. Security categories and associated security measures

As mentioned above, work on the security categories is a part of the operations analysis. The established standards forming the basis for information security work contain a large number of security categories that function as a support for the information security work. These security categories vary in relevance depending on operation. Stockholm University has identified five security categories that are essential to the University's operations: *Acquisition, development and maintenance of systems*, *Access control*, *Operational reliability*, *Communications security* and *Supplier relations.*

Each security category has recommended security measures. Depending on operation, the security measures from some or all of the security categories might be relevant. For this reason, each department is to identify relevant security measures for its own operations. The work on the security categories encompasses the selection, introduction and administration of security measures taking into account the risks that exist regarding the University's information security. The owners of the information assets need to take a position on whether the security measures have been observed and ensure that instructions and procedures exist.

The scope of the information security requirements and the measures is to reflect the assessed value of the information and the negative impact on operations that a lack of adequate security might lead to. In other words, if it is assessed that inadequate security can have major consequences for operations, the information security requirements are to be high and the measures more extensive than if it is assessed that inadequate security will not have such major consequences. In order to identify the risks that exist and to assess the consequences of these risks and the probability of their arising, a risk and vulnerability analysis is to be performed.

Stockholms universitet

Where the department uses central IT services, it is the head of IT Services who is responsible for the identification of the risks and the work on the security measures.

3.1. Acquisition, development and maintenance of systems

3.1.1 Purpose

The purpose of this security category is to ensure that information security is an integrated part of the information system[4] throughout its life cycle, during development, construction, testing, operation and phase-out.

3.1.2 Responsibility

The head of department is responsible for the acquisition, development and maintenance of IT services at the department. Ahead of such a decision, a dialogue is to be conducted with IT Services and the Finance Office. A risk and vulnerability analysis is also to be performed, preferably with the support of IT Services.

Where the department uses the University's central IT services, the head of IT Services is responsible for acquisition, development and maintenance of the IT services.

3.1.3 Security measures

There are several security measures concerning the acquisition, development and maintenance of systems, including documenting procedures regarding requirements concerning information security for new information systems or improvements to existing information systems and documenting procedures regarding the development of programs and systems. A list of all measures is contained in Appendix 2.

3.2. Access control

3.2.1 Purpose

The purpose of access control is to ensure that only authorised users have access to information and information processing resources. Rules for the control of access are to be drawn up, documented and followed up on the basis of requirements of operations and information security requirements. The asset owner is to establish appropriate rules for the control of access, rights and restrictions for specific roles. The level of detail and the requirements in the security measures are to reflect the security risks associated with the information. Access controls are both logical and physical, and these are to be taken into account jointly. Users and service providers are to be provided with clear information on the requirements of operations that are to be fulfilled through access controls.

---

[4] An information system or IT system is often defined as a system that provides IT support and is used to gather, store, process and distribute information for a domain, thereby supporting communication and work within and between organisations.

Stockholms universitet

3.2.2. Responsibility
The head of department is responsible for access control for the information and IT environment at the department. IT Services provides support in order to ensure good access control.

Where the department uses the University's central IT services, the head of IT Services is responsible for access control. The head of IT Services is responsible for joint technical IT infrastructure and its access control.

3.2.3 Security measures
Examples of security measures concerning access control are review of users' access rights, documented procedures for current access rights and systems for password management. A list of all measures is contained in Appendix 2.

3.3. Operational reliability

3.3.1. Purpose
The purpose of the security category operational reliability is to ensure that a relevant level of operational reliability is maintained with regard to the operation of information processing and communications resources (IT resources that are carriers of information and that are used for the transfer of data).

3.3.2. Responsibility
The head of department is responsible for operational reliability concerning the IT environment at the department. IT Services provides support in order to ensure good operational reliability.

Where the department uses the University's central IT services, the head of IT Services is responsible for operational reliability. The head of IT Services is responsible for operational reliability in the central IT environment.

3.3.3. Security measures
There are to be documented procedures for, e.g., the operation of information processing and communications resources, such as start-up and take-down procedures, backup, maintenance of equipment, management of media, data centres and the management of email and security. A list of all measures is contained in Appendix 2.

3.4. Communications security

3.4.1. Purpose
The purpose of security measures for communications security is to ensure the protection of information in networks and to protect connected services.

3.4.2. Responsibility
The head of department is responsible for the control of communications security at the department. IT Services provides support in order to ensure good communications security.

Stockholms universitet

Where the department uses the University's central IT services, the head of IT Services is responsible for the communications security of these.

3.4.3. Security measures

There are several security measures concerning communications security. For example, there are to be documented procedures for the management and control of networks and documented procedures for the requirements that are to be included in agreements. A list of all measures is contained in Appendix 2.

3.5. Supplier relations

3.5.1. Purpose

The purpose of the security category supplier relations is to ensure protection of the information assets to which suppliers have access.

3.5.2. Responsibility

The head of department is responsible for the supplier relations that are unique and relevant at the department. The head of IT Services is responsible for supplier relations that are university-wide.

3.5.3. Security measures

Information security measures are to be identified and established in a set of regulations in order to specifically manage supplier access to the information of operations. These security measures are to address both processes and procedures within their own operations, but also the supplier's processes and procedures.

An example of a security measure concerning supplier relations relates to verification of the supplier's service delivery, which means that there are to be documented procedures to secure this. A list of all measures is contained in Appendix 2.

4. Incident management

4.1. Purpose

The purpose of incident management is to:

- make risks visible and take measures in light of negative events and near-events that have occurred in operations
- reduce negative impact on operations and strengthen resilience and to prevent incidents from occurring
- provide support for prioritisation
- provide documentation to increase awareness of the importance of incident management
- provide documentation for decisions on changes to operations and associated governing documents

Stockholms universitet

4.2. Responsibility

The head of department is responsible for incident management at the department. IT Services provides support in order to ensure good procedures for incident management.

The head of IT Services is responsible for the coordination of reported information security incidents.

All employees, students and persons working on behalf of Stockholm University are to report incidents concerning information security. The procedures are therefore to have been described and communicated in an appropriate manner.

4.3. Definition

An incident is an event (or a near-event) that can have a negative impact on Stockholm University's operations. An incident can be the result of an intentional act or something that has happened unintentionally. The common denominator is that the operations are threatened, e.g. through unauthorised management of information, operational disruption, fire, theft, etc.

4.4. Identification, reporting and management of incidents

It is important that there is a good knowledge within the organisation of the measures that are to be taken and how incidents and near-events are to be reported at the University. In order to ensure that any incidents have a minimal impact on the University's operations, there is to be a formalised process for the reporting and management of incidents. Through this process, it is to be ensured that incidents and near-events are reported in such a way that appropriate measures can be taken both in the short and in the long term.

All employees, contractors and third-party users are to note and report observed or suspected incidents. If the incident is of a more sensitive nature, reporting can be made directly to IT Services by telephone. IT incidents concerning the central IT services are reported via Serviceportalen. If local incident management exists, there are to be processes and procedures for this, and IT Services is to have knowledge of how these incidents are managed in order to gain an overall picture of the University's total quantity of incidents.

Incidents are to be managed with the necessary promptness so that the University's information assets are not damaged.

4.5. Escalation of incidents of information

In the event of incidents that are assessed to potentially have a major impact on the University's operations (in the case of uncertainty – contact IT Services), IT Services is also to be immediately informed through an email being sent to infosakfunktionen@su.se. Emails sent to this address are handled with a high degree of confidentiality, and only a limited number of people at the University have access to the information. IT Services can also be contacted by

Stockholms universitet

telephone. The head of IT Services is responsible for ensuring that those concerned are informed of the incident, its impact and consequences and of which measures have been taken. The head of IT Services is also responsible for the Senior Management Team receiving the necessary information.

According to a government decision, central government agencies under the Government are, as of April 2016,
to report IT incidents that seriously affect security to the Swedish Civil Contingencies Agency. This is in order to provide a better overview of the threats that exist at the national level. IT Services reports IT security incidents and is the University's point of contact with respect to the Swedish Civil Contingencies Agency. This means that IT Services is to be contacted immediately, via infosakfunktionen@su.se or by telephone, when an IT security incident has occurred. IT Services is a support in the assessment of whether
or not a report is to be made.

If the department transfers a part of its information management to a non-central government actor, the department's transfer agreement is to ensure that the counterparty undertakes to report IT incidents to the department. The department is to forward the information to IT Services without delay.

4.6. Analysis of incidents

All cases that have been classified as incidents shall, after being dealt with, be analysed with regard to cause and effect. This is because there might be a link between different incidents that is not immediately visible. A number of minor incidents can together indicate extensive security deficiencies that are difficult to identify without a thorough analysis.

5. Continuity in the case of a serious event and disruption

5.1. Purpose

Business continuity management is about reducing the University's vulnerability and increasing its resilience to various events that might affect operations that are assessed to be critical. MSBFS 2016:1 The Swedish Civil Contingencies Agency's regulations on the information security of central government agencies requires the University to conduct business continuity management, for which reason risk and vulnerability analysis is essential.

5.2. Responsibility

Continuity can be divided into three parts:

- business continuity management (BCM)
- IT service continuity management (ITSCM)
- crisis plan

Stockholms universitet

The Director of Administration is responsible for the University's business continuity management (BCM) including all crisis planning.

The head of department is responsible for IT service continuity management (ITSCM) at departments with their own IT environment.

The head of IT Services is responsible for IT service continuity management (ITSCM) in the central IT environment and also for the communication of the process for IT service continuity management to those concerned, its appropriateness and the availability of instructions/procedures.

The head of the Technical Support Office coordinates the University's crisis plan and crisis organisation. As of 1 January 2017, the head of the Property Management Office is responsible for ensuring that this coordination takes place.

5.3. Continuity plan

A classification is to be made of which operations and services are most critical to operations. This can be done with the support of IT Services. Business continuity management is to identify and manage risks that can lead to serious disturbances or disruptions in the delivery of these operations and services. Operations and services are to be restored as soon as possible in order to minimise the impact on operations. Business continuity management is also to manage rapid changes in the need of resources and capacity in existing operations and services due to the repercussions of disruptions and disturbances.

Business continuity management is a continuous process that

encompasses: Planning

- analysing which operations and services are critical to operations
- identifying and analysing risks that might threaten or disrupt operations and services
- producing solutions in order to avoid disturbances or minimise their consequences

Implementing

- introducing solutions in order to avoid risks and associated consequences
- allocating responsibilities
- producing a continuity plan with procedures for managing disturbances
- informing and training
- testing and introducing the continuity plan

Following up

- following up how the plan functions

Stockholms universitet

- analysing disturbances and incidents that have occurred

Improving

- renewing the vulnerability analysis
- amending technical, administrative and organisational solutions and procedures
- improving the plan

5.4. Crisis plan

The purpose of a crisis plan at the University is to create preparedness through coherent and explicit central crisis management and to develop procedures for initiatives in the case of serious events.

The head of department must know how the crisis plan for the University functions in general and what is expected of the head in a crisis situation. This means that each department must draw up a plan of measures for managing different crisis situations that might arise.

It is of great importance that all staff are aware of the plan of measures and who is to be contacted in the event of a crisis.

The crisis plan is activated by the Director of Administration when a serious event befalls the University.

Stockholms universitet

Appendix 1: Detailed process for operations analysis incl. risk and vulnerability analysis

1. Identify information assets
    - Input data: Organisational information and potential information assets
    - Identify the most important information assets
    - Result: Asset map (e.g. research information, systems, educational material, personal data)

2. Identify owners of information assets
    - Input data: Asset map
    - Identify owners and responsibilities based on asset map
    - Result: Mapped ownership and responsibilities (Examples of owners are head of department, administrative manager, object owner)

3. Classify information assets
    - Input data: Asset map, ownership
    - Classify assets based on the properties *confidentiality*, *availability*, *integrity* and *traceability*
    - Result: Classified information assets

4. Identify risks to information assets
    - Input data: Asset map, ownership and classification
    - Identify and classify risks based on probability and consequences. Escalate risks with high probability and consequences as necessary to higher management
    - Result: Risk map (Examples of risk are unauthorised intrusion and destruction of research data)

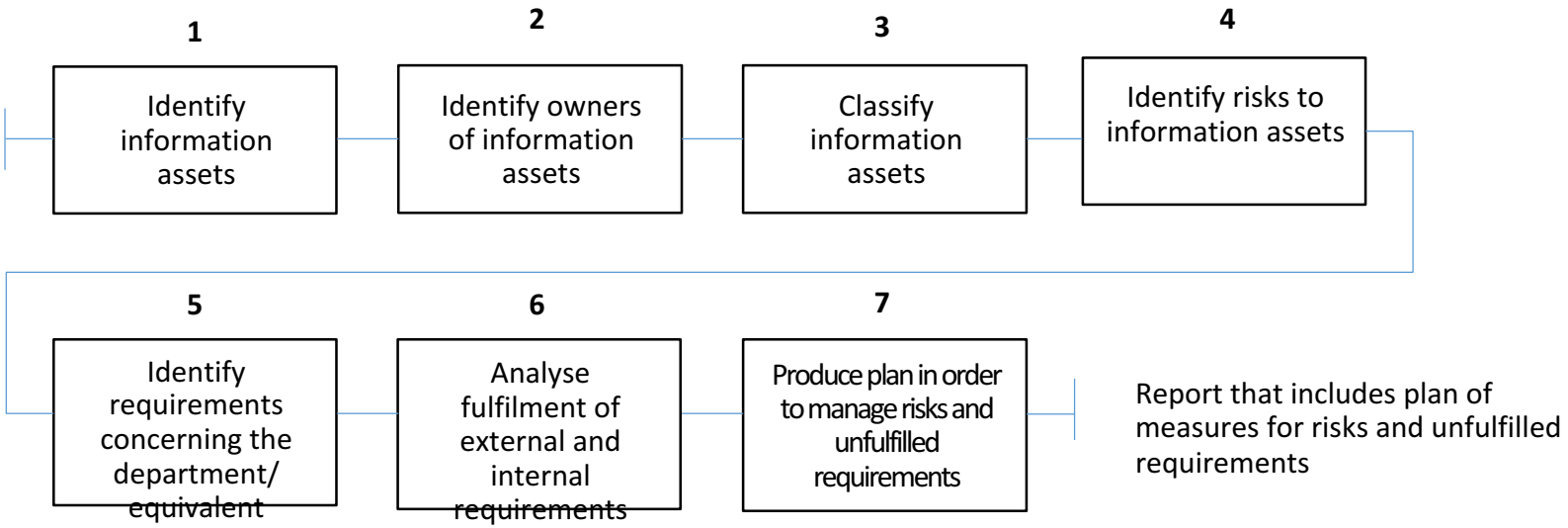
5. Identify requirements concerning the department's operations
    - Input data: External and internal requirements
    - Identify legal requirements
    - Result: Applicable external and internal requirements (Example of requirements is the Personal Data Act)

6. Analyse fulfilment of external and internal requirements
    - Input data: Applicable internal and external requirements. Asset map
    - Analyse based on measures for each security category in no. 3.1–3.5 according to Guidelines for Information Security
    - Analyse based on external requirements
    - Ensure that the information security function of IT Services is informed of the result
    - Result: Analysis of fulfilment of internal and external requirements

7. Produce plan of measures in order to manage risks and unfulfilled requirements
    - Input data: Risk map. Analysis of fulfilment of internal and external requirements
    - Produce plan of measures for identified risks in risk map
    - Prioritise measures and produce time schedule
    - Identify responsibilities and the person responsible for each activity
    - Result: Report that includes plan of measures for risks and unfulfilled requirements

Stockholms universitet

Process for the need to secure strategically important information assets



Stockholms universitet

Appendix 2: Security categories and associated security measures

Acquisition, development and maintenance of systems

Measure	**Responsible for fulfilment**
Analysis and specification of information security requirements: Documented procedures are to exist regarding requirements concerning information security for new information systems or improvements to an existing information system	Head of department/equivalent
Securing of program services on public networks: Documented procedures are to exist regarding use of public program services.	The asset owner
Protection of program services in transactions: Documented procedures are to exist regarding program services' transactions.	The asset owner
Rules for secure development: Documented procedures are to exist regarding development of programs and systems.	Head of department/equivalent
Procedures for the management of system changes: Documented procedures are to exist regarding system changes within the development cycle.	Head of department/equivalent
Technical review of applications following changes in operating environment: Documented procedures are to exist regarding changes in operating environment.	The asset owner
Restrictions for changes in program packages: Documented procedures are to exist regarding changes to program packages.	The asset owner
Secure development environment: Documented procedures are to exist regarding need of protection for development environment.	Head of department/equivalent

Stockholms universitet

Outsourced development: Documented procedures are to exist regarding monitoring and controlling of outsourced system development.	Head of department/equivalent
Test data: Documented procedures are to exist regarding management of test data.	The asset owner

Stockholms universitet

Access control

Measure	Responsible for fulfilment
Rules for control of access: Documented procedures are to exist regarding access to networks and network services for which users have been specifically granted permission. (regulation for use of the University's information and information managing resources found in the Rule Book).	Head of department/equivalent
Review of users' access rights: Documented procedures are to exist regarding current access rights.	The asset owner
Systems for password management: Documented procedures are to exist regarding allocation of passwords.	The asset owner
Use of privileged utility programs: Documented procedures are to exist regarding utility programs that might have the ability to circumvent security measures.	The asset owner
Access control for program source code: Documented procedures are to exist regarding access to source code.	The asset owner

Stockholms universitet

Operational reliability

Measure	Responsible for fulfilment
Operating procedures: Documented operating procedures are to exist regarding information processing and communications resources.	The asset owner
Change management: Documented procedures are to exist regarding changes in information processing resources and systems.	The asset owner
Capacity requirements: Documented procedures are to exist regarding present and future capacity requirements.	The asset owner
Separation of development, test and operating environments: Documented procedures are to exist regarding choice of separation between the environments.	The asset owner
Protection against malicious code: Documented procedures are to exist regarding detection, prevention and restoration.	The asset owner
Backup: Documented procedures are to exist regarding backup of information, programs and the mirroring of systems.	The asset owner
Logging and monitoring: Documented procedures are to exist regarding event logs.	Head of department/equivalent
Control of operating systems: Documented procedures are to exist regarding installation of programs on operating systems.	The asset owner
Management of technical vulnerabilities: Documented procedures are to exist regarding management of technical vulnerabilities in the information systems that are used.	The asset owner

Stockholms universitet

Restrictions for installation of programs: Documented procedures are to exist regarding program installations.	The asset owner

Stockholms universitet

Communications security

Measure	Responsible for fulfilment
Security measures for networks: Documented procedures are to exist regarding management and control of networks.	Head of department/equivalent
Security in network services: Documented procedures are to exist regarding which requirements should be included in agreements.	The asset owner
Separation of networks: Documented procedures are to exist regarding management of networks.	Head of department/equivalent
Information transfer: Documented procedures are to exist regarding transfer of information using means of communication.	Head of department/equivalent

Stockholms universitet

Supplier relations

Measure	**Responsible for fulfilment**
Information security rules for supplier relations: Documented procedures are to exist regarding the supplier's access to the organisation's information.	Head of department/equivalent
Management of security within supplier agreements: Documented procedures are to exist regarding which information security requirements should be included.	Head of department/equivalent
Management of the supplier's service delivery: Documented procedures are to exist regarding verification of agreed level.	Head of department/equivalent