LUNDS UNIVERSITET

DECISION

Registration number
STYR 2022/587

Date
24 March 2022

Vice-Chancellor

Information Security Management System at Lund University

Approved by the Vice-Chancellor
24 March 2022

Postal address Box 117, 221 00 Lund, *Visiting address* Arkeologen Sandgatan 1 *Phone +46* 761 30 35 66, +46 46-222 00 00,
E-mail ingegerd.wirehed@rektor.lu.se

Contents

Postal address Box 117, 221 00 Lund, *Visiting address* Arkeologen Sandgatan 1 *Phone +46* 761 30 35 66, +46 46-222 00 00,
E-mail ingegerd.wirehed@rektor.lu.se

1. Introduction

Information is a necessary resource and a condition to enable Lund University to conduct high-quality education and research in collaboration with wider society and contribute to societal development. Increased digitalisation, use of technical aids, cyberthreats, legal requirements, regulations and ordinances as well as a rapid rate of change in the wider world makes systematic and risk-based information security management crucial to the University. The systematic approach described here takes the form of the University's Information Security Management System (ISMS) and aims to ensure the University's critical information assets are given adequate, relevant and continuous protection. See Appendix 1 Information Security Management System (ISMS).

The University's information security management is based on Swedish standard series ISO 27000, and is to fulfil the requirements in the Swedish Civil Contingencies Agency (MSB)'s *regulations on information security for public authorities*, MSBFS 2020:6[1] and MSBFS2020:7 and MSBFS 2020:8, as well as complying with the MSB's ISMS model.

Policy documents
The following policy documents are included in the University's Information Security Management System:

- *Information security policy*

  Expresses the intention and strategic goals of the University Board and the scope of the management system

- *Information Security Management System at Lund University*

  Establishes and describes how the University governs its information security

- *Guidelines – Risk-based information security management*

  Describes the risk process – information security

- *Instructions – Established information security measures*

  Describes security measures in information security

1.1 Definitions

Terminology and definitions for the area and for related areas at the University are to be found in the document entitled "Terminology for information security at Lund University" on the Staff Pages.

1.2 Scope

The management system covers and applies to all organisational units, employees, students and external collaboration partners at the University and thereby all information and data for which the University is the principal responsible on the basis of the University's corporate identity number 202100-3211.

[1] *MSBFS 2020:6*

Information security is to be conducted as efficiently as possible and as an integral part of everyday work, according to the University's existing annual cycle, budget procedure, operational planning and other relevant processes.

2. Management and governance

The University Management is to govern and follow up information security so as to continuously ensure its continued suitability, adequacy and effectiveness. Evaluation of information security performance takes the form of monitoring, measurement, analysis and evaluation, and revision.

The University's model for operational governance and risk management and the requirements in the MSB regulations MSBFS 2020:6 form the basis of how information security is governed.

Fundamental elements for functional and efficient information security management, including the field of IT security, are continuous follow-up and improvement, and the maintenance of an active dialogue between the University Management, faculty managements/equivalents and the University's CISO (Chief Information Security Officer). The MSB model describes all the cyclical stages in ISMS in Figure 1.

Figure 1, The MSB model for ISMS

Responsibilities and authority

In the University's Rules of Procedure, the University Board has established the allocation of responsibilities and authority within the University and also decides on the overarching *Information security policy*.

The Vice-Chancellor has the ultimate responsibility for activities at Lund University and is thereby also ultimately responsible for ensuring that information security management fulfils the requirements set by laws, ordinances and regulations. The Vice-Chancellor has also established the allocation of decision-making powers. The present document concretises the existing delegation and rules of procedure regulating the allocation of responsibilities and duties regarding information security and the conditions for delegation.

The Vice-Chancellor decides to delegate responsibilities and authority according to the allocation in:

- Appendix 3a Responsibilities and delegations
- Appendix 3b Responsibilities and delegations in the field of information security

2.1 Management Review

Reporting of information security work is done in the form of a Management Review and described in Appendix 2 Procedure for the Management Review of information security work. Here, management refers to the University Management.

Reporting is done by the CISO as part of the work to enable the Vice-Chancellor to assess the effectiveness of information security efforts and to decide on goals, action plans and priorities.

In addition to the above, ongoing status updates and reporting are carried out as necessary.

3. Risk process – information security

The University's process for risk-based information security work follows the MSB methodological support and comprises the following elements:

1. *Intelligence analysis*
2. *Organisational analysis*
3. *Risk analysis*
4. *Gap analysis*
5. *Information classification*
6. *Management of identified risks/choice of security measures*
7. *Action plan*

The process, also referred to as risk process – information security, is described in Appendix 4 Risk process – information security and in greater detail in the policy document *Guidelines –Risk-based information security management.*

It is to be implemented:

- annually at the faculties/equivalents and in the central administration
- as necessary, e.g. in case of major changes and projects.

The results are the entry values for decisions on action plans and the Management Review, and subsequently for the budget process and organisational planning.

The process stages are facilitated by the CISO (university-wide Chief Information Security Officer) who also compiles, documents and communicates results and follows up in collaboration with the relevant organisational unit. At each stage, relevant functions are to participate. Experts at the faculties and in the central administration are to be invited, participate and contribute to the process.

The final stage is the drafting of an action plan to address information security risks, meet the information security targets and take account of opportunities for the organisation.

4. Organisation and support

The organisation, responsibility and roles for information security work are regulated in the present policy document, in the University's Rules of Procedure, through decisions by the Vice-Chancellor, and by the Swedish Civil Contingencies Agency's regulations on information security for public authorities, MSBFS 2020:6.

An Information Security Council is to be established at the University level and tasked with preparing strategic issues, conducting risk assessments, e.g. ahead of decisions by the Vice-Chancellor, and acting as an advisory body to the CISO. The members should be representatives of information risk owners and selected representatives from faculty managements/equivalents, as well as the University Director.

Where necessary, local councils for information security can be established at the faculties, or the information security field can be handled in the faculty management group. At the faculty level, the faculty board decides on whether a local information security council should be established. In that case, the task of such a council could be to investigate and propose general and targeted measures to ensure that information security meets current requirements, and to provide support to the organisation on issues concerning information security.

Support to the organisation is also provided by the central CISO, among others. For example, the CISO produces and makes available university-wide policy documents, rules, guides, training courses and news. The CISO also provides support in the implementation of risk process – information security within the framework of the University's annual cycle and as needed.

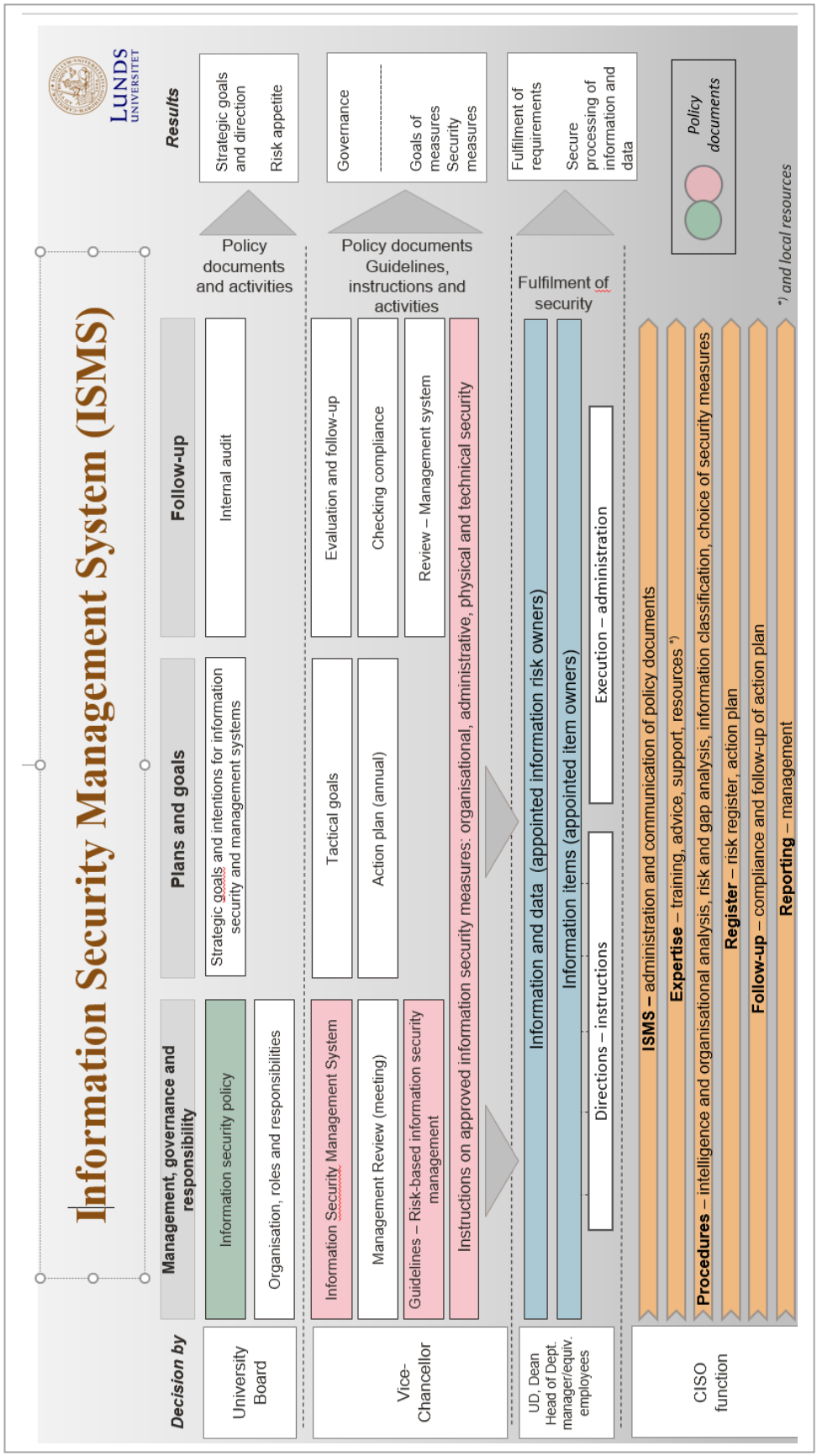
All faculties/equivalents and the central administration are to appoint local coordinators for information security. The CISO is responsible for the forum for local coordinators, which hosts dialogues and exchange of experiences on operational issues. Training courses will be offered for local coordinators.

Appendices 3a and 3b describe all functions, responsibilities and delegations.

Appendix 5 Organisation, reporting, responsibility and resources, describes the organisation, reporting, responsibility and resources.

Postal address Box 117, 221 00 Lund, *Visiting address* Arkeologen Sandgatan 1 *Phone +46* 761 30 35 66, +46 46-222 00 00,
E-mail ingegerd.wirehed@rektor.lu.se

Appendix 1 Information Security Management System (ISMS)



Postal address Box 117, 221 00 Lund, *Visiting address* Arkeologen Sandgatan 1 *Phone +46* 761 30 35 66, +46 46-222 00 00,
E-mail ingegerd.wirehed@rektor.lu.se

Appendix 2 Procedure for the Management Review of information security work

Aim and scope

The aim of this procedure is to describe how the Management Review of information security work is to be planned, implemented, documented and followed up, both on the university-wide level and, where applicable, at the faculties/equivalent organisations[2].

The aim of the Management Review is to create the conditions for the University to direct and conduct systematic, risk-based information security work which is preventive, continuously improved and complies with applicable legal requirements as well as external and internal rules. The Management Review is to include informing management, evaluating the effectiveness of information security work and ISMS, and presenting an action plan.

The university-wide level

Cases and reporting points are to be drawn up by the CISO in consultation with the University's Information Security Council.

The Management Review is conducted in the Vice-Chancellor's Management Council (RL).

The CISO is responsible for:

- preparing, compiling and making available the documentation for the Management Review

Implementation
The Management Review at the university-wide level is to be held in the Vice-Chancellor's Management Council at two regularly scheduled meetings, in April and November for example.
The Management Review should contain all the points on which MSB recommends the highest levels of management in public authorities stay informed, see *Agenda for the Management Review* below.
The decision on an action plan after the Management Review is taken by the Vice-Chancellor at the usual Vice-Chancellor's meeting (RS).

As necessary, specific questions concerning information security are to be raised with the Vice-Chancellor even between these regular occasions.

Agenda for the Management Review

[2] *Equivalent organisational units refers to the central administration, the University Library, the University Specialised Centres (USV), the University's cultural and public centres and the MAX IV Laboratory*

April

Follow-up

Previous meeting and follow-up of previously approved measures

Security awareness

Status regarding awareness of information security in the organisation. Risks regarding digitalisation and IT use.

Statement on applicability

Information assets

Status of the most critical and sensitive information assets in the organisation.

External requirements

Legal requirements and other external requirements on information security and status on compliance.

Risks

The most serious information security risks. Both specific to the organisation and for society as a whole.

Protection

Status of existing protection, serious shortcomings and vulnerabilities. Gap analyses against the requirements of the ISO27000 standards/MSB requirements.

Incidents

Summary and analysis of information security incidents since the previous report.

Action plan

Presentation of the action plan and targets for the following financial year. The action plan and targets are then approved by the Vice-Chancellor through the usual process for Vice-Chancellor's decisions and meetings (RS).

Other issues

November

Follow-up

Minutes from previous meeting, and follow-up according to the April meeting:

- Statement on applicability
- Incidents
- Action plan

The effectiveness of ISMS and information security work

Where applicable, decision on improvements

Revisions and reviews

Results from implemented information security-related revisions and reviews of compliance with the University's policy documents for information security.

Improvement measures

Measures taken regarding information security.

After the meeting

The meeting secretary for the Management Review writes up the minutes for the meeting and ensures that they are approved by the person appointed to the task and distributed to the Vice-Chancellor's Management Council, all heads of faculty offices, and all heads of division/equivalent in the central administration. The heads of faculty offices are responsible for communicating the information to their organisations.

All members of the Vice-Chancellor's Management Council and the CISO are responsible for informing their own organisations about the outcome of the meeting and any relevant assignments.

Faculty level/equivalent

Each faculty/equivalent is responsible for whether the Management Review of information security work is to be done at the faculty level. If implemented, it is appropriate to conduct the review according to the structure described above for the university level, annually and preferably in connection with the annual review of the risk process – information security with the faculty's management group or the local information security council if such a body has been established.

Postal address Box 117, 221 00 Lund, *Visiting address* Arkeologen Sandgatan 1 *Phone +46* 761 30 35 66, +46 46-222 00 00,
E-mail ingegerd.wirehed@rektor.lu.se

Appendix 3a Responsibilities and delegation

The Vice-Chancellor of Lund University:

- as head of the public authority, has overall responsibility for ensuring that the information security work meets the current legal requirements
- ensures that good information security permeates the organisation
- keeps abreast of information security work, risks, etc.
- takes decisions on action plans and management of information security risks at the University level
- ensures that the University's Information Security Management System is fit for purpose and that the work is conducted according to approved policy documents
- ensures that there is a university-wide CISO with the necessary resources and conditions.

The Vice-Chancellor delegates responsibilities and certain powers in the information security field as specified below.

All people active at LU

All people active at the University, such as employees, all students and external collaboration partners, have a responsibility and an obligation to protect the organisation's information when processing it and to report any deviations from the regulations or undesirable incidents that are discovered. Reporting is to be done promptly and without delay according to the instructions on the University's Staff Pages. Reported deviations and undesirable incidents are managed by the security officers concerned in accordance with approved procedures.

Operational managers

Organisational heads and operational managers are responsible for the work on risk management within their area of responsibility.

Operational managers at all levels are to ensure that their employees/equivalents receive adequate training and continuous information on approved security measures and to ensure that the requirements set for their organisation and on individuals are fulfilled.

Deans

The dean/equivalent is responsible for information security within their faculty/equivalent as part of their delegated organisational responsibility. The responsibility can be further delegated to heads of department or equivalent.

The dean/equivalent is responsible for:

- meeting the requirements for risk management and security measures set for their own organisation

Postal address Box 117, 221 00 Lund, *Visiting address* Arkeologen Sandgatan 1 *Phone +46* 761 30 35 66, +46 46-222 00 00,
E-mail ingegerd.wirehed@rektor.lu.se

- regular follow-up and reporting of deviations from information security requirements within their area of responsibility to the CISO or according to applicable processes on the University's Staff Pages
- ensuring the necessary time, resources and conditions for information security work within their own organisation
- ensuring the implementation of the risk process – information security according to the University's annual cycle and as necessary
- appointing a local coordinator for information security at the faculty/equivalent. Several departments/equivalents can choose to appoint a common coordinator. In cases where no contact person is appointed, the dean/equivalent is responsible for contacts and support concerning information security
- compliance follow-up and reports to be submitted to the CISO twice per year and as necessary.

University Director

Pursuant to delegation from the Vice-Chancellor, the University Director has overall responsibility for the University's organisation with regard to legal, financial and administrative matters.

The University Director is responsible for information security within the central administration as part of their delegated organisational responsibility. This responsibility can be delegated further to the heads of division/equivalents.

The University Director is responsible for:

- meeting the requirements for risk management and security measures set for their own organisation
- regular follow-up and reporting of deviations from information security requirements within their area of responsibility to the CISO or according to applicable processes on the University's Staff Pages
- ensuring the necessary time, resources and conditions for information security work within their own organisation
- ensuring the implementation of the risk process – information security according to the University's annual cycle and as necessary
- ensuring that continuity planning with regard to information security is done on an organisation-wide level
- ensuring the CISO is given the necessary resources to be able to implement approved assignments and tasks and provide adequate support to the organisational units.

System owners

System owners/equivalents:

- have superior responsibility for the administration, operation and overall information security regarding specific IT systems

Postal address Box 117, 221 00 Lund, *Visiting address* Arkeologen Sandgatan 1 *Phone +46* 761 30 35 66, +46 46-222 00 00,
E-mail ingegerd.wirehed@rektor.lu.se

- are responsible for meeting the requirements of the information risk owner for information security measures for the IT system/service operated within the University or by an external party, so that the information is adequately protected
- are responsible for defining and following up the technical protective measures for the IT system on the basis of the current action plan and within the framework of the University's system administration model and to ensure that IT security measures fulfil the requirements for information security.

These duties can be delegated according to the roles and responsibilities in the University's system administration model. Consult the University website.

In cases where no system owner has been appointed, the head of the organisation in which the system operates is responsible.

IT managers

IT managers/equivalents are responsible for:

- ensuring that the necessary resources, expertise, documented directions and instructions for IT are in place so that the required, approved technical IT security measures can be introduced and administrated based on the University's policy documents for information security
- ensuring compliance with regard to the information security requirements set for IT systems and infrastructures within their own area of responsibility.

Data Protection Officer / DPO

Pursuant to the General Data Protection Regulation (GDPR), the Data Protection Officer has the following information security tasks in relation to personal data:

- to inform, advise and train the University and its employees about their obligations pursuant to data protection legislation
- to oversee compliance with data protection legislation and with the University's strategy for the protection of personal data
- to provide advice on the impact assessment regarding data protection which is to be conducted pursuant to the data protection legislation
- to provide support in the management and reporting of personal data incidents
- to function as a contact point for the supervisory authority and the data subjects.

The officer should participate as an expert when information security risks are being assessed. The role and tasks are specified in more detail in a separate decision by the Vice-Chancellor.

Chief Security Officer

Pursuant to the Security Protection Act (2018:585), the Security Protection Ordinance (2018:658), the Swedish National Police Board's regulations on security protection and the Public Access to Information and Secrecy Act, the University is responsible for taking preventive measures to protect security-sensitive activities at the University against espionage, terrorism and other crimes which could threaten the organisation, as well as for protection in other cases of security-classified information.

In analyses of information assets in which this legislation may be applicable and any of the following may be required, the University's Chief Security Officer is to be contacted:

- security protection analysis
- background checks and security review appraisals
- security classification.

The role and tasks are specified in more detail in a separate decision by the Vice-Chancellor.

Postal address Box 117, 221 00 Lund, *Visiting address* Arkeologen Sandgatan 1 *Phone +46* 761 30 35 66, +46 46-222 00 00,
E-mail ingegerd.wirehed@rektor.lu.se

Appendix 3b Responsibilities and delegation in the field of information security

The Vice-Chancellor delegates responsibilities and authority in the field of information security as follows:

CISO (Chief Information Security Officer)

The remit and role of the CISO[3] is independent and reports to the Vice-Chancellor. The CISO is responsible for and has authority over:

- planning and coordinating the university-wide information security work in accordance with approved policy documents, processes, goals and frameworks from the management, and being responsible for university-wide procedures and tools
- reporting on the information security field and its status, and producing and recommending action plans to the Vice-Chancellor and the Vice-Chancellor's Management Council at the Management Review
- reporting to the management and assessing the appropriate handling of major information security-related incidents and crises
- representing the University in relation to other public authorities and organisations on information security issues such as incident reporting to the Swedish Civil Contingencies Agency (MSB). This does not apply to issues that are to be managed by the Data Protection Officer or the Chief Security Officer unless this has been agreed previously.

The role and tasks are specified in more detail in a separate decision by the Vice-Chancellor.

University-wide CISO function

The University's central administration has a CISO function for which the CISO has management and organisational responsibility. The tasks of this function are to:

- administrate LU's Information Security Management System and ensure that the associated documentation is kept current, up to date and communicated
- set requirements for the organisation regarding information security
- train and inform employees, students and external collaboration partners as needed
- participate in the assessment and management of major information security-related incidents and crises
- facilitate and support in the implementation of risk process – information security, by involving and collaborating with other support and expert functions at the faculties and the central administration such as the Data Protection Officer, the Security and Environment Division, IT security experts, HR, the Legal Division, LU Estates, and the Records Management and Archives Office.

Local information security coordinator

The duties of the coordinator are determined by the scope and nature of the organisational unit. This may entail being the contact person for information security and support for local management and staff in everyday work, taking part in the annual

[3] *MSBFS 2020:6 Section 5*

Postal address Box 117, 221 00 Lund, *Visiting address* Arkeologen Sandgatan 1 *Phone +46* 761 30 35 66, +46 46-222 00 00,
E-mail ingegerd.wirehed@rektor.lu.se

risk process work concerning the local organisational unit and being the contact person for the university-wide CISO function.

Information risk owner

The information risk owner [4] is linked to a type of information, identified during the risk analysis stage and responsible for

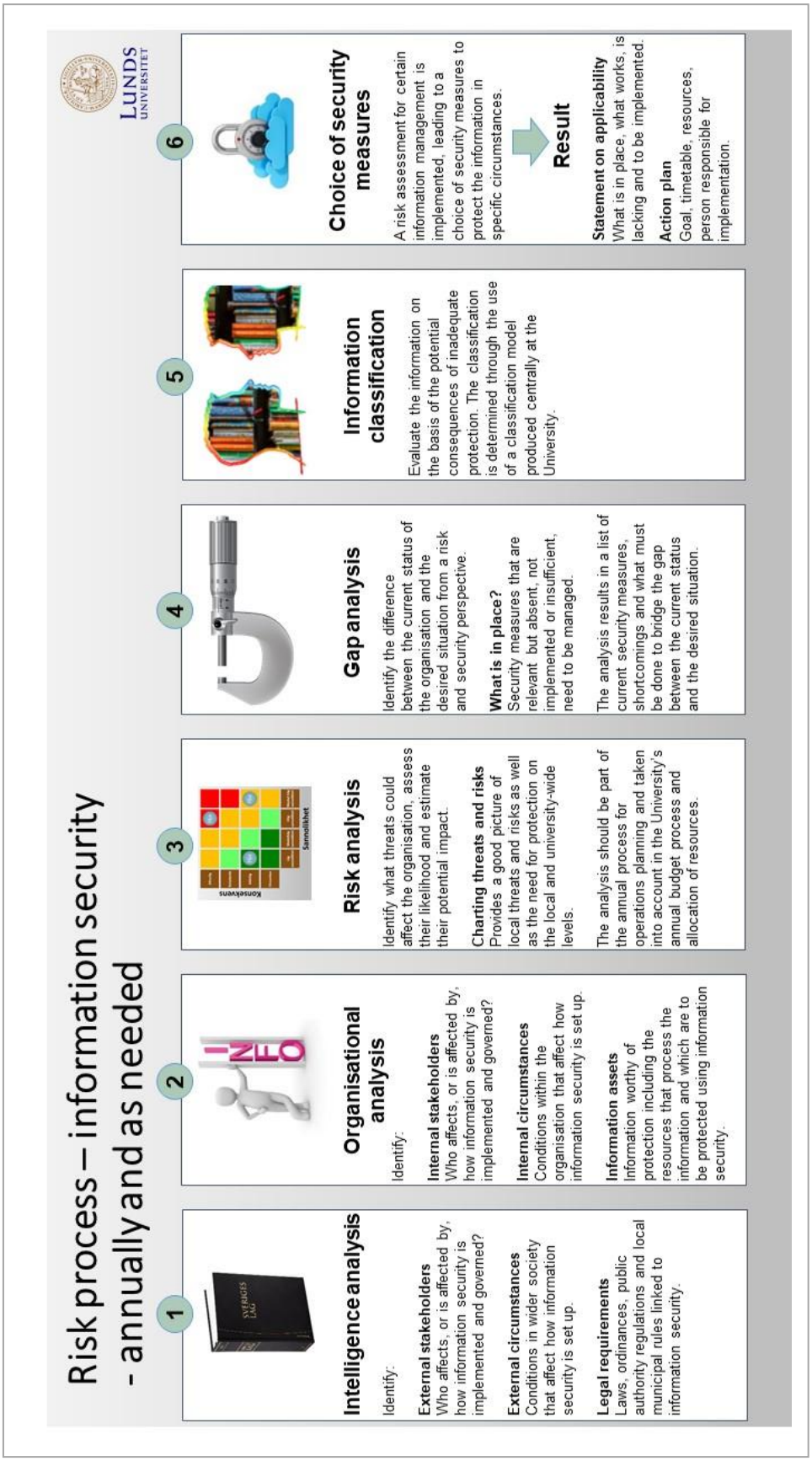
- ensuring information is managed in a way that maintains the appropriate level of confidentiality, correctness and reliability throughout its life cycle, e.g. in an IT system/service, by setting the formal requirements
- ensuring information is classified according to an approved and adequate process
- taking decisions on acceptance of any residual risks (risk acceptance) which exceed the University's risk appetite once an action plan has been approved.

Information risk ownership follows the regular organisational responsibility (line management structure) as long as the risk only involves the local organisational unit.

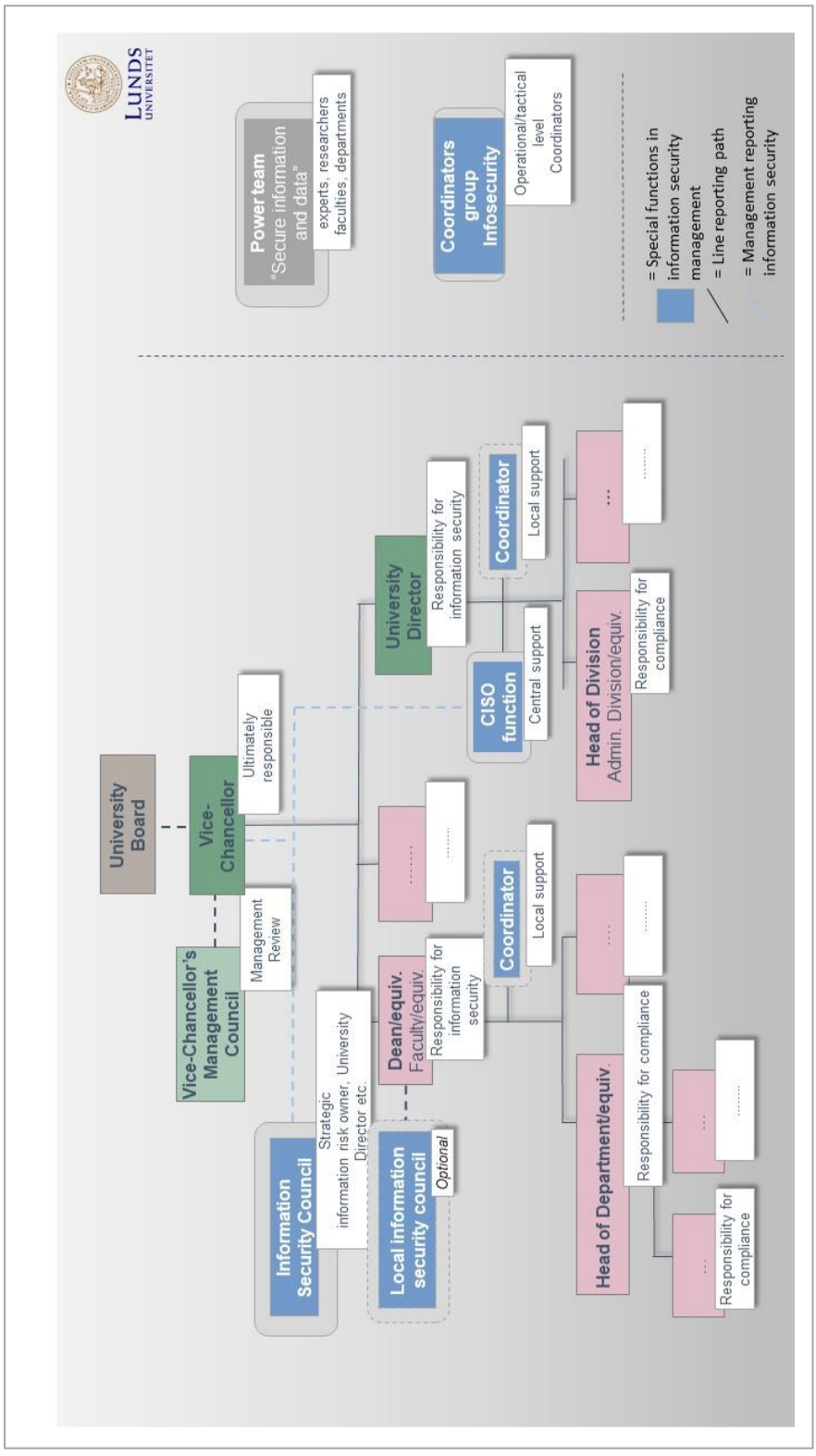
For university-wide types of information and university-wide risks, the information risk owner is determined by the Vice-Chancellor.

[4] *MSBFS 2020:6 Section 5*

Appendix 4 Risk process – information security



Appendix 5 Organisation, reporting, responsibilities and resources



Postal address Box 117, 221 00 Lund, *Visiting address* Arkeologen Sandgatan 1 *Phone +46* 761 30 35 66, +46 46-222 00 00,
E-mail ingegerd.wirehed@rektor.lu.se