LUND UNIVERSITY

University Board

Framework for the internal governance and control at Lund University

This decision replaces the risk assessment model for Lund University, adopted by the University Board on 26 September 2008, and the risk management policy for Lund University, adopted by the University Board on 5 May 2008. Amended 9 December 2016.

Objective of the work on internal governance and control

Internal governance and control refers to the process that is to ensure that the government authority, with reasonable certainty, fulfils the objectives of the organisation. In accordance with the Ordinance (2007:603) on Internal Governance and Control, the University is to identify, assess, adopt measures and follow up risks within the organisation that could affect whether the university is able to fulfil its objectives. Through this procedure, the University will achieve good internal control. Effective risk management is to permeate all activities and ensure that the risks are handled in a reasonable manner. To achieve its objectives, the University is not to avoid risks altogether, thus refraining from being able to take advantage of new opportunities. Risk management must therefore strive to increase the University's awareness and understanding of risks, and thereby support risk acceptance when relevant, but in a structured and controlled manner.
Because risk management is an integral part of all decision-making within the University, it is not only a responsibility of the University management but a responsibility for all management functions within the various parts of the University. Risk management will therefore be performed in different ways, depending on the unique needs of each organisation.

Responsibilities

The University Board has the overall responsibility for internal governance and control, and is thereby responsible for ensuring that the University has a risk management procedure that is fit for purpose. The University Board annually decides on the University's risk assessment and the acceptable level of risk (risk appetite, see definitions below).

The Risk Committee of the University Board is to participate in preparing the University Board's decisions on risk assessment, as well as the assessment of the internal governance and control.

Postal address Box 117, 221 00 Lund *Visiting address* Paradisgatan 5b *Telephone* +46 46 222 92 59, +46 46 222 00 00
Email magnus.ekblad@rektor.lu.se *Website* www.lu.se

The Audit Committee of the University Board follows up the observance of the University's framework for internal governance and control.

The vice-chancellor is to ensure that good internal governance and control permeate all activities at the University.

The vice-chancellor is responsible for making sure that appropriate support functions are available to ensure and follow up the work on internal governance and control, as well as provide support to the different levels of management.

The vice-chancellor is responsible for managing the University's overall risks (or equivalent). If the board has determined the acceptable level of risk, the vice-chancellor is also responsible for making sure that the University's overall risks (or equivalent) are managed accordingly.

The vice-chancellor is responsible for annually preparing the University Board's decision concerning risk assessments, the level of acceptable risk, and assessment of the internal governance and control, in connection with the annual report.

The university director, deans, heads of faculty office, heads of division, process owners and system owners and equivalent are responsible for the work on risk management within their respective areas of responsibility, such as line organisation, processes and systems.

The Internal Audit Office performs independent reviews of the risk management process. All levels within the organisation are to be involved in the risk management process.

Definitions
The following definitions apply for the risk management work at Lund University.

Risk management process: the risk management process is the process to ensure good internal governance and control through the following steps: formulation of objectives, risk identification, risk management, control measures and follow-up.

Objectives: the objectives for Lund University refer to:

- the requirements imposed by the Government and Parliament, primarily through the Government Agencies and Institutes Ordinance (2007:515), the Higher Education Act (1992:1434), the Higher Education Ordinance (1993:100) and public service agreements.
- the objectives of the strategic plan and other objectives determined by the University Board.
- other internal regulations, such as policies, guidelines and decisions on different levels.

Risk identification: identifying the events which may involve a risk that the objectives are not achieved.

Risk assessment: an assessment of the likelihood that a certain event will occur and how serious the impact of such an event could be. Risks in our activities are an assessment that cannot be calculated statistically.

Risk management: implementation of measures to manage a risk. The management can be based on the following assessments:

- Accepting the risk: accepting the risk means that no measures are taken, based on the assessment that the impact on the organisation is minor, that the risk is beyond the organisation's control, or that the measures are too costly to implement in relation to the expected benefit.
- Limiting the risk: limiting the risk means that measures are taken to reduce the likelihood and/or impact of an event.
- Sharing the risk: the management of risks can in some cases be shared within the Government, for instance through the Swedish Legal, Financial and Administrative Services Agency (Kammarkollegiet). Claims management is performed in accordance with the current ordinance.
- Eliminating the risk: a risk is eliminated by avoiding the activities or events that generate the risk.

Control measures: the measures taken to manage a risk and to ensure that the objectives are achieved.

- Detective measures: measures aiming to detect whether a risk has occurred.
- Directive measures: measures aiming to ensure that a particular outcome is achieved, for example, regulations and guidelines.
- Preventive measures: measures aiming to reduce the likelihood that an unwanted outcome will occur.
- Corrective measures: measures aiming to correct undesirable outcomes which have already occurred.

Follow-up: follow-up of the risk management process to ensure satisfactory internal governance and control, as well as risk assessment and control measures to assess whether the risk assessment is up-to-date and whether the measures are fit for purpose.

Risk: a risk is an event that constitutes a threat to the University's ability to achieve its objectives. Such an event could also involve a missed opportunity.

Risk assessment model: the model that the University uses to assess the likelihood of an event taking place and the impact it will have for the University if it occurs.

Risk appetite: can be used to describe the level of risk the organisation finds acceptable. The level may vary from one organisational unit to another. For example, within its core activities – education, research, innovation and external engagement – the University may take greater risks so as not to miss out on opportunities, while the same level of risk is not acceptable within support processes.

Assessment criteria with regard to likelihood		
Criteria for assessing likelihood		
Likelihood		**Examples**
Very common (5)	The risk can occur at any time or has already occurred	• We know that this will occur • The event could occur at any time
Common (4)	The risk is generally known to occur	• This type of event is generally known to occur • It is expected to occur within a 12-month period
Fairly common (3)	The risk has occurred a few times	• There are several known cases of when the event has occurred • May occur within 1–5 years
Fairly uncommon (2)	The risk has occurred on single occasions	• There are few known cases of when the event has occurred • May occur within a 5-year period
Unlikely (1)	The risk could only occur under exceptional circumstances	• The event has never previously occurred • Not expected to occur in the foreseeable future

Assessment criteria with regard to impact		
Criteria for assessing impact		
Impact		**Examples**
Devastating (5)	Lasting/permanent impact	• Major damage to the brand, research and the number of students • The current board and management are not managing the situation
Serious (4)	Long-term impact	• Significant damage to the brand and the number of students • Events and issues which require measures from the management team and other managers
Medium (3)	Short-term impact	• Short-term damage to the brand and the number of students • Events and issues which require measures from the management team and other managers
Minor (2)	Short-term limited impact	• Possible minor damage to the brand and the number of students • The impact can be handled within the scope of the regular activities; events and issues are handled by the respective managers
Insignificant (1)	No actual impact	• No damage to the brand and the number of students • Events and issued are handled by lower management and other employees

Likelihood	Very common	**5**	**R3**	**R3**	**R4**	**R5**	**R5**
	Common	**4**	**R2**	**R3**	**R4**	**R4**	**R5**
	Fairly common	**3**	**R2**	**R3**	**R3**	**R4**	**R4**
	Fairly uncommon	**2**	**R1**	**R2**	**R3**	**R3**	**R3**
	Unlikely	**1**	**R1**	**R1**	**R2**	**R2**	**R3**
			1	**2**	**3**	**4**	**5**
			Insignificant	Minor	Medium	Serious	Devastating
			Impact				

Classification of risk and prioritisation of measures		
	Classification of risk	**Need of measure**
R1	Low, insignificant risk	Measure not required
R2	Minor risk	Consider measure
R3	Medium, certain risk	Take reasonable measure
R4	Serious risk	Take measure as soon as possible
R5	High, very serious risk	Measures must be taken immediately