UNIVERSITEIT STELLENBOSCH UNIVERSITY

Risk Management Policy

Type of Document:	Policy
Purpose:	To guide the management of risks at SU
Approved by:	SU Council
Date of Approval:	2015/11/30
Date of Implementation:	2016/01/01
Date of Next Revision:	As required
Date of Previous Revision(s):	None
Policy Owner[1]:	Chief Operating Officer
Policy Curator[2]:	Chief Director: Finance
Keywords:	Risk Management, Risks, Safety and Security
Validity:	In case of differences in interpretation the English version of this policy will be regarded as the valid version.

SU Policies are available at www.sun.ac.za/policies

[1] Policy Owner: Head(s) of Responsibility Centre(s) in which the policy functions.
[2] Policy Curator: Administrative head of the division responsible for the implementation and maintenance of the policy

STELLENBOSCH UNIVERSITY

RISK-MANAGEMENT POLICY

Reference number of this document	
HEMIS classification	0601 "Executive Management" 1601 "Strategic Planning" 1604 "Management Information Services "
Purpose	To guide the management of risks at SU
Type of document	Policy
Accessibility	Internal and external
Date of implementation	
Revision date/frequency	
Previous revisions	No previous revisions; new policy
Owner of the policy	Chief Operating Officer
Institutional functionary (curator) responsible for this policy	Director: Risk Management and Campus Security
Approval date	30 November 2015
Approved by	SU Council
Keywords	Risk management / Risk

1. Introduction

Stellenbosch University (SU) is, like any other organisation, exposed to various risks. These risks have the potential to disrupt the attainment of SU's strategic and operational goals as well as sustainability. SU aims to make more informed decisions based on a structured approach to risk management and with consideration of any advantages that risks taken may hold. In this way a proactive preventative, rather than a reactive, approach is followed, with higher expectations of SU attaining its goals.

2. Application of the policy

This policy is by default applicable to all staff members (permanent and part-time) in faculties, departments, centres, bureaus, institutes and the support services, as well as to all members of the statutory bodies of SU and the members of companies controlled by SU that are involved in the governance and management of risks. Student structures are also encouraged and supported to follow the principles. Risk management is applicable to all areas of SU's activities, including corporate governance, academic, commercialisation, sports, cultural and student activities.

3. Definitions

Definitions are provided in a separate glossary to, where necessary, provide room for a broader explanation of concepts and the creation of general risk-management definitions. The glossary is applicable to all documents on risk management, for example the policy and manual, and prevents duplication and contradictions. The glossary is adapted and updated from time to time as necessary. See **Appendix B**.

4. Purpose of the policy

The purpose of the policy is to:

- Commit SU formally to risk management modelled on SU's current vision, mission, core values, ethics and strategic as well as operational goals, and to support these;
- Commit SU to the implementation and maintenance of effective and transparent risk management supported by resources consisting of people, capital, physical facilities, equipment, policies, regulations, systems, processes and information systems; and
- Set guidelines for the take, governance and management of risks applicable to SU in the context of each staff member's role and work environment, as well as the broader university environment.

5. Aims of the policy

With the implementation of this policy, SU wants to attain the following aims:

a) To formalise the framework, methods and terminology of risk management of all SU's activities and to establish a reporting protocol;
b) To give guidance to persons responsible for the review, identification, assessment, monitoring, management and notification of risks;
c) To ensure that the policy and management documents are available to all interested parties;
d) To ensure that risks are continuously identified, documented and managed;
e) To ensure better coordination and identification/demarcation of roles and responsibilities regarding the review and management of risks;
f) To ensure that SU manages risks appropriately and thereby ensure that potential opportunities are maximised and the detrimental effect of risks are minimalised, not necessarily with the aim of totally eliminating risk from all activities; and
g) Effective reporting to the Audit and Risk Committee of Council (ARC(C)).

The overarching aim of this policy is to ensure that SU applies the identification, measurement, governance, monitoring and notification of risks consistently at all levels and in all SU's activities.

6. Policy principles

The risk-management policy and the application thereof must, considering all relevant legislation:

a) Be aligned with SU's current Institutional Intent and Strategy;
b) Be in line with regulatory requirements, such as the Regulations for Reporting by Higher Education Institutions and leading risk-management practices, for example the recommendations regarding corporate governance, the applicable guidelines on risk management, as contained in the King Code and Report, the COSO and ISO 31 000 risk-management frameworks, and monitor changes and compliance continuously;
c) Be supported by a risk-management structure relevant to SU given the external context, nature and complexity of SU's activities and current business model;
d) Be embedded in SU's core activities, systems and processes, yet also be dynamic enough to adapt to changing circumstances;
e) Evaluate all types of risks applicable to SU;

f) Clearly establish the accountability, ownership, responsibilities, expectations, as well as the required conduct and mindset with regard to the risk-management responsibilities of Council, Management and staff members; and
g) Establish and develop the required risk-management culture.

7. Policy provisions

a) SU should continuously strive for an effective institutional risk-management maturity level through the establishment and continuous refinement of risk management, as contained in the applicable policy, framework, strategy, plan and manual.
b) Council delegates the responsibility for designing, implementing and monitoring SU's risk strategy to the Rector. The Rector and the Rectors' Management Team (RMT) are accountable to Council and responsible for integrating risk management into the operational activities of SU.
c) SU's risk-management framework consists of a system of risk review, risk management and internal controls designed to identify, assess, monitor, communicate and manage risks.
d) Management should:
    (i) regularly review the relationship between strategic goals and risks to ensure that emphasis is placed on activities with the highest priority; and
    (ii) determine the acceptable levels of risk for SU by establishing an overhead risk tolerance and acceptable levels of deviation.
e) Risks must be identified on both institutional and environment levels and managed within SU's risk tolerance. This approach acknowledges that risks are often related and have a mutual influence, which may increase the impact of risks, and that not all risks can be avoided.
f) Members of the RMT, deans and faculty managers as well as environment heads and their subordinate management team members are compelled to capture their environment's risks in the SU risk register for review and notification purposes. They should also implement specific limits of risk-tolerance levels aligned with the overarching limits approved by Council.
g) The level on which a risk is managed is determined in the risk-management plan by escalating risks upwards to the relevant level for the effective management of the risk and related interventions.
h) The risks that are documented in SU's risk register serve as account of risk events to which SU is potentially or historically exposed. Each risk is classified in terms of one primary risk classification. The primary classifications are (1) Strategic, (2) Operational, (3) Finance, (4) Research, (5) Teaching and learning, (6) Reputation, (7) People, (8) Facilities, (9) Technical and IT, (10) Safety and security, (11) Sustainability and (12) Compliance. An Institutional Classification Owner is appointed to oversee and report on each classification. The classifications and typical risks specific to each classification eventually form a risk universe map specific to universities. The secretariat of the Risk Management Committee (RMC) will keep and update a risk universe map to serve as risk-identification aid as well as review document.
i) Risk management is embedded in the establishment of strategy, planning, performance management and operational processes.
j) Risk management should also be used to obtain the correct balance between the risk associated with an activity or initiative and the benefits thereof.

k) Council must ensure that Management and all staff members are provided with the applicable and sufficient guidance and training on various levels in terms of the principles of risk management to enhance awareness and establish responsibilities.
l) Risk management must provide for extraordinary events.
m) Risk intervention, reporting systems and processes must ensure that the management and notification of such exceptional and critical events and other high risks are expedited and escalated to the relevant level.
n) Council should receive reassurance on the extent and efficiency of the risk-management system and process. Council receives its reassurance through the reporting of the ARC(C), Management and internal audits.

8. Conflict resolution

Conflict arising from this policy should firstly be referred to the Chief Operating Officer for consideration and resolution. Should the conflict not be resolved in this manner, it should be escalated to the RMT.

The Rector has the final authority to resolve conflict arising from the application of this policy.

9. Policy governance

9.1 Governance structure

The policy is enacted by SU Council. The Rector, as chief risk manager, is responsible for the execution of this policy. The Rector delegates the overhead responsibility to the relevant member of the RMT, namely the Chief Operating Officer. **Appendix A** gives a schematic representation of SU's levels of safety and risk management.

The Chief Operating Officer is the owner of the risk-management policy.

9.2 Roles and responsibilities

Roles and responsibilities arising from this policy are allocated in terms of SU's delegation policy and system.

9.2.1 *SU Council* has the overhead responsibility for direction in terms of, and supervision of, the management of risks and the internal control environment in the University and is the final authority responsible for risk management.

Council is further responsible to report via the annual report on risk management and how the institution dealt with institutional risks, as prescribed in the Regulations for Reporting by Higher Education Institutions.

Council is responsible for ensuring that effective risk-based internal audits and reporting take place, and also reports on the efficiency of the system of risk management and internal controls.

9.2.2 *The ARC(C)* is the Council committee with a direct review responsibility for risk management. The committee should as far as possible consist of independent, external persons with the required risk-management skills and experience.

9.2.3 *The Rector and Vice-Chancellor* is responsible to Council for risk management at SU. The Rector's responsibilities include the high-level review of management and administration, risk

management, review of information technology management, a risk-based internal audit system and integrated reporting.

9.2.4 *SU's Chief Operating Officer* is the Rector's delegate who, as the RMC chair, takes the lead in and supervises the risk-management and combined assurance processes at SU and takes responsibility for reporting on these to the RMT and then to the ARC(C).

9.2.5 *The heads of responsibility centres (RCs)* have the overhead responsibility for the identification and management of risks in their respective RCs, as well as guiding and supervising the management of operational risks on all operational levels in RCs.

9.2.6 *The RMC* makes recommendations to the RMT and the ARC(C) on suitable risk appetites in support of meeting institutional goals and operational requirements. The RMC also makes recommendations to the RMT and risk owners on the suitable risk-tolerance level as well as the acceptance of residual risks. The RMC is also responsible for receiving and considering recommendation reports from functional structures, such as the SU Security Forum and the Information Technology Management Committee, and compliance reports from the respective environments and *ad hoc* task groups that are appointed to monitor issues such as new legislation or best practices in risk management.

The purpose, functions, composition, work method and powers of the RMC are fully defined in the regulations of the RMC.

9.2.7 *Line heads* are responsible in terms of SU's risk-management model for the identification, management and communication of risks in their environment.

9.2.8 *The Director: Risk Management and Campus Security* has a threefold responsibility regarding risk management, namely to

- *As RMC secretariat, manage the secretary function*;
- *As policy curator*, take the lead in representation on formulation, approval processes, revision, communication and making this policy and supporting management documents available to establish common risk terminology, aligned processes and minimum standards; and
- *As Director: Risk Management and Campus Security,* offer institutional risk-management support services to line heads as well as functional support of SU's risk-management systems.

9.2.9 *External role players.* The RMC is functionally supported by SU's internal and forensic auditors, insurance brokers and other specialist experts who are contracted in as and when necessary. The internal auditors have a seat on RMC meetings and are invited to the ARC(C).

9.3 Implementation

The implementation of the policy will take place under supervision and guidance of the Chief Operating Officer.

9.4 Monitoring

The RMC monitors the application of this policy be setting and controlling strategic and operational risk-management goals.

9.5 Reporting and notification

Reporting takes place on each of the various levels of risk management as contained in the risk-management framework (**Appendix A**). Accordingly, guidelines and instructions by Council and/or the ARC(C) (level 1) are delegated to the Rector and RMT (level 2), to the RMC (level 3), to the four RCs (level 4), and to the faculties and support service environments (level 5). Notification takes place via the opposite route. Reporting should comply with applicable regulatory requirements.

9.6 Disclosure

The risk-management policy is an internal management document available to managers and all staff members on the intranet. The policy may, with permission from the curator of the policy, be made available externally.

9.7 Revision

This policy serves as the current foundation for SU's risk-management system and process and will be revised biennially or according to circumstances.

9.8 Action in case of non-compliance

Management intervention on an applicable level and in a relevant manner

10. Supporting and related documents

The architecture of SU's risk-management policy consists of the policy itself as well as supporting and related documentation. Supporting documentation gives effect to and offers guidelines for the policy. Related documentation establishes the requirements and context.

The appendices to the policy are supplementary to the policy and must be read in conjunction with it, but do not form part of the policy. The appendices may be revised and amended by Management from time to time.

Supporting documentation

Item no.	Name of document	Status
1.	SU Institutional Intent and Strategy as approved in 2013	
2.	Regulations of the Risk Management Committee as approved on 8 September 2011	
3.	SU risk-management framework and strategy	
4.	SU risk-management manual	
5.	SU research ethics policy	
6.	Risk-management plan	
7.	Appendices to the policy:	
	Appendix A – Levels of safety and risk management at SU	
	Appendix B – Glossary	

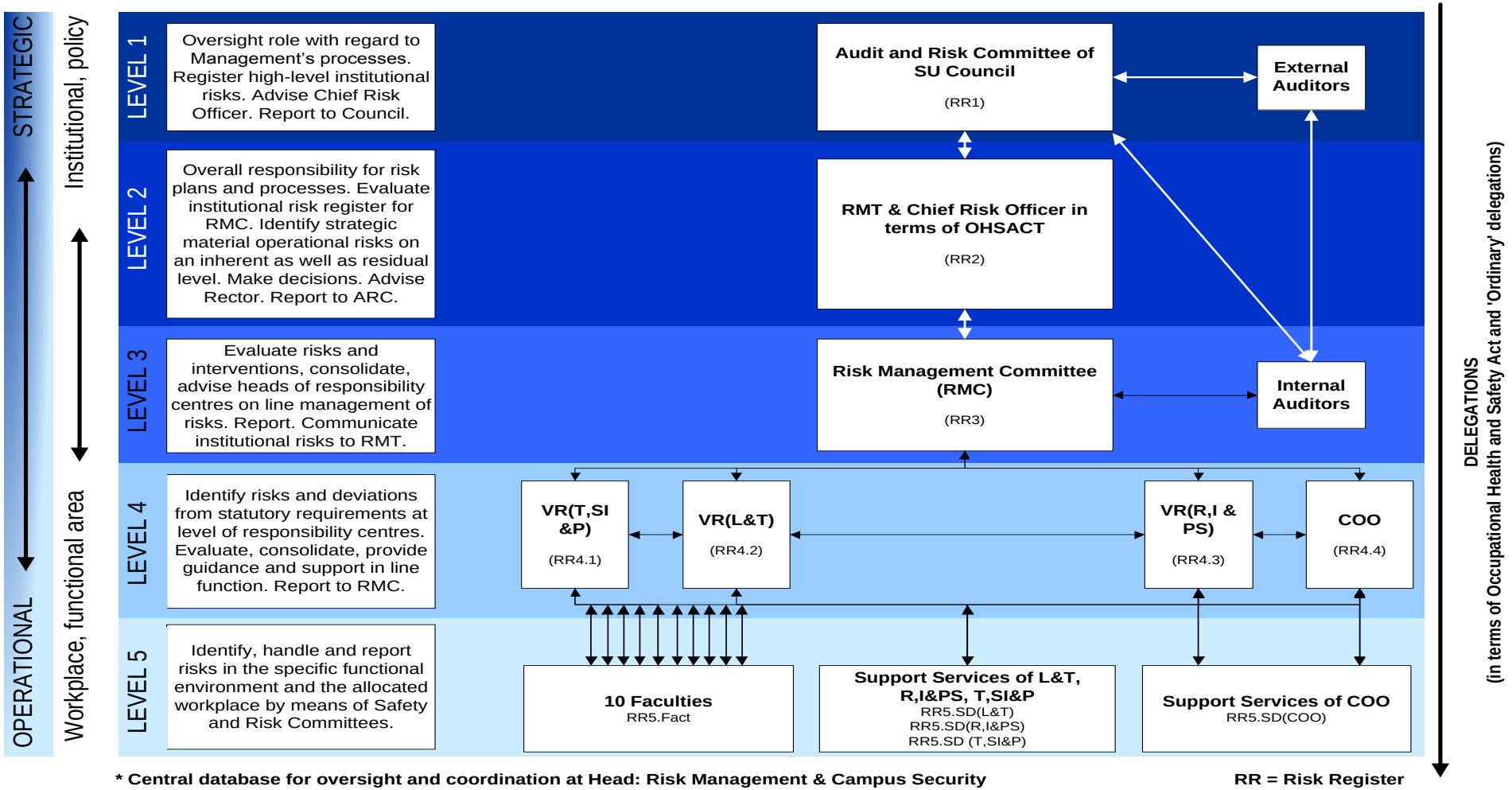
Related documents

Item no.	Name of document	Status
1.	King III Report on Corporate Governance	
2.	Occupational Health and Safety Act, No. 85 of 1993	
3.	Regulation 464 of the Higher Education Act (No. 101 of 1997): Regulations for Reporting by Higher Education Institutions signed on 9 June 2014	
4.	Policy on conflict of interests	
5.	SU delegation policy and procedures	

Appendix A

Levels of safety and risk management at SU

Embedded in existing structures for systemic safety and risk evaluation and integrated management



*** Central database for oversight and coordination at Head: Risk Management & Campus Security**

RR = Risk Register

Appendix B

GLOSSARY

ARC(C)	Audit and Risk Committee of Council
Corporate governance	In the context of this policy it refers to both control and supervision
Embedded risk-management model	The management model for risk management embedded in the organisational structure of the institution. Line heads manage their environments' risks and supervise the management of the risks of subordinate environments.
Environment	A faculty, or support service environment, subsidiary, other related companies or activities resorting under an RC and of which the head, whether dean, chief director or senior director, reports to a vice-rector or the Chief Operating Officer.
Environment-wide risk management	A continuous process of coordinated management activities by Council, Management and staff members applied during the establishment of strategy and on all levels at SU to identify and assess potential events that may influence SU and to allocate and manage responsibility within SU's risk appetite and tolerance to give reasonable assurance in terms of SU's attainment of its objectives Establishment of risk and governance ownership on all levels and within each role where risks must be managed
Extraordinary event	An event that takes place without expectation. Also known as a black swan event.
Impact	The effect that the risk will have on the environment or institution as a whole should the event occur
Inherent risk exposure	The exposure inherent to the potential risk event in the absence of interventions aimed at decreasing exposure; in short, the exposure before actions to decrease it
Management	Members of the RMT, deans and faculty managers as well as environment heads and their subordinate management team members up to director level, RC heads and line heads
Operational controls	Refers to operational processes, human resources, information and systems
Operational risks	Exposure to an event, resulting from unsuccessful operational controls, operational activities or incidents that could lead to loss, damage or injury
Probability	The chance that an event will take place. In the context of inherent risk it refers to, and is influenced by, factors such as the macro-economic environment and geographic representation. In the context of residual risk it is influenced by the efficiency of controls such as human resources, processes and systems.
RC	Responsibility Centre
RC head	The vice-rector or other senior manager that heads an RC
Reporting	A combination of activities that vary from the risk register that serves at the risk-management and operations meeting, to the overhead risk report and the risk register sent annually to the Department of Higher Education in compliance with the Regulations for Reporting by Higher Education Institutions

Residual risk	The residual or remaining exposure to a potential risk event after actions have been implemented to decrease the probability and impact (also called net risk)
Risk	The effect of uncertainty on goals. 'Effect' is a positive or negative deviation from the expected. Risk is also often defined as an event, a change in circumstances or a consequence, but this new definition of risk identifies risks in the context of the organisations' own goals and not only risks in general. 'Risk' is therefore distinguished from a risk event that has already taken place and about which there is therefore no uncertainty. Risk is evaluated in terms of impact and probability. *(ISO Guide 73: Risk is the effect of uncertainty on objectives.)*
Risk analysis	The process used to understand the nature, sources and causes of identified risks and to determine the level of risk. It is also used to evaluate the impact, consequences and controls currently in existence. *(ISO 31 000)*
Risk appetite	The amount of risk Council is willing to take in the pursuit of the attainment of goals
Risk assessment	The process consisting of risk identification, risk analysis and risk evaluation on the basis of impact and probability. Risks are assessed on an inherent and residual basis.
Risk context	External and internal considerations that must be taken into account in the management of all risks applicable to the institution
Risk description	A structured paragraph or statement defining the source of a risk, potential events to which it may lead and causes and possible consequences thereof
Risk evaluation	Application of techniques to evaluate the exposure of one risk against another in order to prioritise risks
Risk event	As risk event can be one or various events, or even a non-event (when something that should have happened did not happen). It can also be described as incidents or accidents. Events always have a cause and usually have consequences. Events without consequences are sometimes referred to as near-misses, near-hits or close calls.
Risk event database	A database into which all risk events and near-misses are entered. Such database can be used to identify and analyse risks in terms of probability and impact. Is distinguished from risk register (see later).
Risk identification	Application of various methods to find, recognise and describe, inclusive of the main causes, risks that may influence the attainment of goals
Risk management	An extensive description of the interventions taken to downmanage the exposure and/or impact, with distinction between actions already completed and actions in process, with the disposal target date. Risk response can be divided into actions that: (i) Tolerate risks – the risk where exposure is as low as possible (ii) Treat, decrease or mitigate risks – through improvements to the internal control environment (iii) Transfer risks – usually to a third party such as insurance or outsourcing

	(iv) Avoid/terminate risks – the activity that leads to the unacceptable risk • Exploitation of the risk where the risk exposure represents disregard of a potential event
Risk-management framework	The **fundamental** and **organisational** components that support and maintain risk management in an institution. The fundamental component includes the risk-management policy, goals and mandates and commitment to these. The organisational component includes the plans, relationships, accountabilities, resources, processes and activities used to manage the institution's risks.
Risk-management plan	Schema in which the approach and actions in terms of risk management as well as the relevant components are applied in an integrated way to attain risk-management priorities and goals. As risk-management plan is not a generic document, but should rather ensure that specific information is provided to participants in an activity or project. The plan stipulates how risk should be handled.
Risk-management policy	A declaration of the targets, direction and tempo to which an institution strives in the area of risk management
Risk-management process	The systematic application of policy, procedures and practices and application of communication and consultation activities to establish the context, identify, evaluate and manage risks and continuously revise the process and outcomes
Risk-management secretariat	The office, environment and functionary that assists the RMC chair with secretariat functions, such as keeping the risk register, institutional risk-management documents, agendas and minutes and convening meetings
Risk monitoring	Refers to ongoing activities that include the following: (i) Measurement of risk management based on risk indicators (ii) Periodical evaluation of progress of and deviations from the risk-management plan (iii) Changes in the external and internal operational environment and the impact thereof on the strategic risk profile of SU (iv) Assurance of the effective design and functioning of risk responses (v) Following up of implementation of risk responses (vi) Analysis and increased understanding based on changes, trends, successes, failures and risk events (including near-misses) (vii) Identification of emerging risks.
Risk owner	A person, incumbent or entity responsible and accountable for risk management
Risk register	The register of risks applicable to a specific organisation, area, and so forth. The risk register contains: (i) A description of risks with regard to impact and probability (ii) Evaluation of the inherent and residual risk per risk (iii) Evaluation of the efficiency of the relevant controls (iv) Action plans to implement additional controls needed to manage risks to an acceptable level (v) The status of risk-mitigation actions Risk registers contain risk information within each area and are primarily used to monitor risks.

	The various areas' risk registers are, depending on the level of risk, escalated to the next level up to SU's overhead risk register (if the risk is high enough).
Risk tolerance	The acceptable level of deviation with regard to goals, often expressed in numerical terms relating to the specific goal
Strategic risks	Risks that threaten the realisation of SU's institutional intent, strategy and goals, as defined in SU's Institutional Intent and Strategy or any part thereof
Strategy	The long-term goals of SU. The strategic-planning horizon for an institution is typically three, five or more years.
Uncertainty	A condition that refers to the inadequacy of information and that leads to insufficient or incomplete knowledge or understanding. In the context of risk management uncertainty exists when knowledge or understanding of an event, consequence or probability is insufficient or incomplete.