

RULES

RISK¹ AND COMPLIANCE² MANAGEMENT

1. PURPOSE

The purpose with the set of rules is to ensure the establishment of a management environment conducive to the realisation of the policy statements included in the NWU Policy on Risk and Compliance Management (approved by Council on 19 March 2020).

The UMC has approved this set of institutional rules on 22 April 2021.

2. OBJECTIVES

At principled level, the NWU views risk and opportunity management as much more than the mere maintenance of its risk and compliance registers and the continuous update thereof. In accordance with the COSO ERM Framework (2017), risks and opportunities are linked to strategy-setting, the effective governance and management of the university, the measurement of performance and communication to all stakeholders.

Similarly, in accordance with King IV compliance management is viewed as much more than only an obligation resting on the NWU, but as a manner in which the university is afforded the opportunity to establish and strengthen its reputation as being ethical and a good corporate citizen.

Therefore, the objective with the institutional rules included below is to ensure synergy and focus in the organisational pursuit towards the integration of risk and compliance management into day-to-day organisational and decision-making and business processes so as to enable an optimal risk-management environment.

The NWU Rules on Risk and Compliance Management depart broadly from the principles laid down by the Committee of Sponsoring Organizations of the Treadway Commission (“COSO”) and references to COSO in this set of rules are from COSO 2013³, and COSO 2017⁴

¹ King IV (2017) definition of risk: “Risk as about the uncertainty of events; including the likelihood of such events occurring and their effect, both positive and negative on the achievement of the organisation’s objectives. Risk includes uncertain events with a positive effect on the organization (i.e. opportunities) not being captured or not materialising.”

² King IV (2017) description of compliance: “... compliance is understood not only as an obligation, but also as a source of rights and protection” ... needing “a holistic view on how applicable laws and non-binding rules, codes and standards relate to one another” ... “in a way that supports the organisation being ethical and a good corporate citizen”.

³ COSO 2013: Deloitte COSO 2013- An approach to internal control framework. (URL: [Downloads/ng-coso-an-approach-to-internal-control-framework.pdf](https://www.ciso.org/Downloads/ng-coso-an-approach-to-internal-control-framework.pdf)) [Accessed: 2021.04.11]

⁴ COSO 2017: Enterprise Risk Management: Integrating with Strategy and Performance, June. (URL: <https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>) [Accessed: 2021.04.11]

3. RULES

3.1. Establishment of a risk and compliance culture in the operational management environment

3.1.1. Responsibility matrix

1. All UMC members and their direct reports as well as operational managers, heads of departments, supervisors and section heads take the responsibility to ensure the establishment of an appropriate environment for the identification and management of risk and compliance in the relevant area.
2. Task allocation in regard to risk and compliance management takes place and is monitored officially during the annual performance management process.
3. Where appropriate, a line manager may identify a so-called risk and compliance champion in the relevant environment to act as point of liaison with the NWU Risk and Compliance Coordinator to optimise and align the administration of risk and compliance.

3.2. Enabling an environment for the optimal management of risk at business-process levels

3.2.1. Risk and opportunity identification and risk management

3.2.1.1 Maintenance of risk and opportunity register

1. A risk and opportunity register must be established and kept on record within each relevant line-management environment.
2. The risk and opportunity register is drafted in accordance with the NWU template for risk identification or as per the software implemented by the NWU and as determined by UMC.

3.2.1.2 Risk and opportunity identification

1. Annually, with the drafting of the NWU Annual Performance Plan ("APP"), the goals and the key performance indicators to accomplish these goals are subject to a risk and opportunity analysis to be ensured by the relevant UMC members.
The risk and opportunity analysis is to be included in the NWU APP and reported on during the mid-year and final performance cycles.
2. At the operational level, the relevant line manager or the person designated by the line manager ensures
 - 2.1 the ongoing identification of risks and opportunities that may affect a new/existing operational activity, process or project;
 - 2.2 the capturing thereof on the prescribed risk template; and
 - 2.3 the reporting thereto to the Compliance and Risk Coordinator in the Corporate Information and Governance Services Department ("CIGS").
3. The identification and evaluation of each risk and opportunity must include information on the following matters:
 - 3.1 A risk description indicated in a full sentence;
 - 3.2 The risk owner (i.e. the line manager who takes responsibility as per the annual performance agreement for the ongoing management of the relevant risk);
 - 3.3 Risk causes substantiating the risk description in a comprehensive manner;
 - 3.4 Existing controls;

- 3.5 Analysis of the probability⁵ of the risk and its impact⁶ risk as per the provided scale;
- 3.6 Identification of suitable planned controls and action plans to address the risk; and
- 3.7 Reporting of the risk to relevant line manager and the Risk and Compliance Coordinator (CIGS), and/or to the Combined Assurance Forum.
- 3.8 The Risk and Compliance Coordinator (CIGS) shall facilitate the capturing of the risk on the relevant platform of the NWU risk register (strategic/operational).

3.2.1.3 Risk management

1. The relevant risk owner must ensure that an appropriate risk-abatement strategy is developed (including practical responses, tasks and controls) to ensure the establishment of an appropriate environment as a response to the risk.
2. The abatement/plans to mitigate the risk must be accounted for in the performance management of the functionaries responsible for the mitigation and management of the relevant risk.
3. The risk owner is responsible for the implementation of sufficient internal controls⁷ and control activities⁸ to optimise these in an ongoing fashion to strengthen the ongoing monitoring⁹ of the mitigation process.

The risk owner needs to indicate and record instances where limitations exist in regard to internal controls, such as those events/conditions that would be regarded beyond the control of the relevant organisation.

⁵ The probability scale applied in the Exclaim! Software is utilised as point of departure.

⁶ The impact scale applied in the Exclaim! Software is utilised as point of departure.

⁷ The COSO 2013 Framework defines an *internal control* as “a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance” and defines *control environment* as “the set of standards, processes and structures that provide the basis for carrying out internal control across the organisation” in regard of which “... the board of directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct”. The following five principles guide an effective control environment: (i) Demonstrating commitment to integrity and ethical values; (ii) Responsible exercise of oversight responsibility; (iii) Established structure, authority and responsibility; (iv) Demonstrating commitment to competence; (v) Enforced accountability.

⁸ The COSO 2013 Framework defines *control activities* as follows: “Control activities are the actions established by the policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes and over the technology environment. These may be preventive or detective in nature and may encompass a range of activities such as authorizations, approvals, verifications, reconciliations and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.”

At a principled level, COSO 2013 indicates as follows in regard to control activities: (i) It is the prerogative of the organisation to select and develop controls appropriate to the mitigation of risks to acceptable levels; (ii) The organisation has the mandate to select and develop general control activities over technology to support the achievement of objectives; (iii) The organisation needs to deploy control activities through policies, rules and procedures.

COSO 2013 makes clear the importance to establish an appropriate communication environment to ensure the support and effectiveness of the internal control environment to internal and external stakeholders.

⁹ The COSO 2013 Framework defines monitoring activities as: “Ongoing evaluations, separate evaluations, or some combination of the two used to ascertain whether the ... components of the internal controls ... are present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management and to the board.”

COSO 2013 defines a management review control as both a control activity and a management activity, responding both to a control activities focusing on the detecting and correcting of errors in respect of a particular risk, and also focusing broader on general monitoring asking why errors exist and assigning responsibility to fixing errors.

Of importance, is the building-in of routine operations performed regularly on interval basis. Also ensuring separate evaluations executed periodically and checked by objective parties such as Internal Audit.

The underlying principles put forward by COSO 2013 regarding control activities: (i) The organisation has the mandate to select, develop and perform ongoing and/or separate evaluations to determine the appropriateness of the components of its internal controls; (ii) The organisation evaluates and communicates internal control deficiencies in a timely manner to the relevant parties in order to ensure that corrective action is taken.

3.2.1.4 Reporting

Reporting of the ongoing risk management venture takes place in accordance with 3.1.1(3), 3.2.1(2)(3) and 3.2.1.(3)(7) stated above.

3.2.2. Roles and responsibilities of assurance providers

1. The NWU Combined Assurance Model aims at coordinating a holistic and integrated understanding of the University's strategic risks and providing effective and efficient risk-management and internal-control processes, resulting in integrated and consistent risk-management and risk-assurance reporting to governance structures.
2. The University's risk-assurance strategy is linked to the 2015-2025 NWU Strategy in terms of the focus of the risk-assurance strategy on key risks and associated business processes that could prevent the University from achieving the strategy.
3. The NWU risk universe with its eight clusters that are linked to the realisation of the University strategic agenda form the basis of strategic and operational risk management and assurance provision.
4. In accordance with King IV the NWU Council as advised by the Audit, Risk and Compliance Committee assumes the responsibility to set the direction on assurance services and functions and overseeing optimal arrangements in regard to the following matters:
 - 4.1 Enabling an effective internal-control environment;
 - 4.2 Enabling an environment in which the integrity of information needed for decision-making by management and governance structures is ensured; and
 - 4.3 Enabling an environment that ensures the integrity of external reports.
5. The NWU Combined Assurance Forum ensures that the planning and the coordination of assurance activities towards optimal collaboration among assurance providers take place and is reported to the UMC and the Audit, Risk and Compliance Committee.
6. Assurance provisioning is organised in terms of King IV's six-level assurance model that distinguishes between assurance provided in the risk-ownership environment and independent assurance provisioning, and is explicated as indicated in Table 1:

Table 1: King IV assurance levels, the functions involved, and rules on the actions to be taken, as well as the roles and responsibilities in terms of combined assurance provisioning

Assurance level	Functions involved	Actions regarding assurance provisioning ¹⁰	Role clarification in the combined assurance provisioning process at internal level ¹¹
Assurance provisioning, level 1	The line functions that own and manage the risk and opportunity	<ul style="list-style-type: none"> · Risk identification, and risk management. · Design and implement controls · Develop policies, rules, procedures · Conducting risk- and control self-assessments 	1. Integrated processes: Information collected from assurance providers analysed to formulate a combined view on the risk management and control effectiveness.
Assurance provisioning, level 2	Specialist functions that facilitate and oversee risk and opportunity (such as Quality Enhancement, Legal Services Department, Risk and Compliance)	<ul style="list-style-type: none"> · Providing the framework and tools according to which risks are to be managed. · To inquire on the appropriateness of the risk management endeavour of line management. 	2. Integrated audits:

¹⁰ Mutevhe, Tabeth. 2019. Implementing combined assurance in organisations to enable boards to exercise risk oversight. Pretoria: Gordon Institute of Business Science, University of Pretoria. A research project in partial fulfilment of the requirements for the degree of Master of Business Administration.

(URL: https://repository.up.ac.za/bitstream/handle/2263/74030/Tayengwa_Implementing_2019.pdf?sequence=1&isAllowed=y)

[Accessed: 2021.04.11]

¹¹ In accordance to Mutevhe (2019:29-31)

		<ul style="list-style-type: none"> · Advising on the the institution's risk strategy, risk appetite, frameworks and processes for the identification, assessment and management of risks. · Assisting risk owners on appropriateness of internal controls. · Validating the monitoring done by risk owners. · Identifying areas of non-compliance. 	<p>Assurance providers work together on audits to perform assurance on a particular aspect of the risk-management process and control environment.</p> <p>3. Aligned assurance activities Alignment of activities and coordination thereof, supplemented with clear communication and agreement on further action.</p>
Assurance provisioning, level 3	Internal Assurance Provider (Internal Audit)	<ul style="list-style-type: none"> · Internal Audit (IA) working in accordance with professional standards in executing audits. · IA provides assurance on the effectiveness of governance, risk management, internal controls, including the effectiveness of the assurance provisioning at levels 1 and 2. 	
Assurance provisioning, level 4	External Assurance Provider (External Audit)	<ul style="list-style-type: none"> · In accordance with professional standards and the scope of the audit commission · External Audit usually relies on the work done by Internal Audit 	n.a.
Assurance provisioning level 5	Other external assurance providers such as sustainability and environmental auditors, external actuaries, external forensic fraud examiners.	<ul style="list-style-type: none"> · In accordance with professional standards and the scope of the audit commission · Normally conducting independent reviews of the assurance provided by assurance providers on levels 1, 2 and 3. 	n.a.
Assurance provisioning level 6	Regulatory inspectors	<ul style="list-style-type: none"> · In accordance with professional standards and the scope of the audit commission 	n.a.

3.3. Enabling an environment for the optimal management of compliance and the creation of awareness in regard to compliance at business-process levels

3.3.1. Founding of the NWU compliance management approach

In accordance with Principle 13 of King IV, the NWU founds its compliance management approach in the statement that the NWU is an ethical and good corporate citizen, therefore compliance is assured to applicable laws and rules, codes and standards applicable to the business of the University.

3.3.2. Long-term compliance management goals

1. Departing from the practices of principle 13 in King IV, taking a holistic view of how applicable laws and non-binding rules, codes and standards relate to each other and continual monitoring of the regulatory environment and appropriate responses to changes and developments inculcated in all business processes and supported and advised by CIGS.
2. Rolling out, at institutional, a compliance programme as approved by UMC, and rolled out to all relevant levels (levels of assurance, line management).
3. The establishment of a holistic compliance culture is achieved in the following ways:
 - Ongoing training in regard to compliance responsibilities and execution thereof in the particular line function.

- Establishment of a web environment that provides up-to-date information relevant to compliance to act owners and other stakeholders.
 - Separate campaigns are run, aimed at assisting management in promoting a compliance culture.
4. The provision of proactive advice in all compliance risk areas and legislative interpretation to ensure proper implementation by line functions.
 5. The implementation of an holistic compliance, risk and business continuity plan by means of a comprehensive integrated approach.

3.3.3 Three-year rolling planning cycles regarding the institution-wide compliance management process

1. Three-year rolling plans on compliance management as approved by UMC are implemented that focus on policy implementation, management of oversight in regard to compliance, assurance provisioning and appropriate reporting.
2. The following rules guide the implementation by CIGS:
 - 2.1 Continued identification of all legislation, sub-ordinate legislation, licences, permits and other legal requirements that could have a reputational, statutory or occupational health or safety impact on the university.
 - 2.2 Enabling a web-based compliance system to be operational in all departments with high risk rated legislation analysed into easy to understand checklists.
 - 2.3 Establishment of a control library that interlinks with the NWU risk registers and audit overview.
 - 2.4 Monitoring of all controls in place for high risk legislation.
 - 2.5 Interdisciplinary working relationship with Internal Audit in terms of self-assessments and monitoring, assisting in planned audits according to the Internal Audit plan.
 - 2.6 Conducting of compliance awareness, with the focus on the understanding of compliance not only for the obligations it creates, but also for the rights and protection it affords.
 - 2.7 Ensuring high-standard compliance reporting to governing bodies.
 - 2.8 Implementing and quality assuring the compliance programme/compliance charter and procedure manual for the NWU based on the Generally Accepted Compliance Principles (GACP) of the Compliance Institute of Southern Africa.

End