ICT Services

Risk Management Committee

Terms of Reference

Document Number	ICT-RMC-2.1
Document Owner	Kate Smit
Version	V2.1
ICT ManCo Approval Status	Approved
First Approval Date	13 March 2015
Last Approval Date	23 August 2017
Associated Documents	

Contents

1. Abbreviations

CoM……Committee(s) of ManCo

COBIT……Control Objectives for Information and Related Technology

ICT Services……Information and Communication Technology Services at the University of the Free State

ICT……Information and Communication Technology

ManCo…… ICT Services Management Committee

RMC……Risk Management Committee

UFS……University of the Free State

2. Definitions

Risk Management: This term refers to the practice of identifying, analysing, assessing and controlling threats that may have an adverse impact on the achievement of objectives.

3. Objectives

The Risk Management Committee (RMC) handles, among other things, the risk management and control responsibilities of ICT Services in accordance with prescribed legislation and corporate governance principles. The purpose of the RMC is to identify potential problems before they occur so that risk-handling activities can be planned and invoked as needed across the life of a process or project to mitigate a possible adverse impact on the achievement of objectives. A continuous risk management approach is applied to effectively anticipate and mitigate risks that form an important part of the business and technical management processes. Effective risk management includes early and aggressive risk identification through the collaboration and involvement of relevant stakeholders. Early detection of risks is important because it is typically easier, less costly, and less disruptive to take corrective measures as soon as possible. Strong leadership from all relevant stakeholders is needed to establish an environment conducive to the free and open disclosure and management of risks.

4. Mandate

The RMC was created under a directive of the ICT ManCo to serve as a supporting structure for the ICT ManCo to manage risks. The RMC is responsible to the ICT ManCo and has to make informed, responsible decisions in order to balance effectiveness against risk for the UFS student, support and academic communities.

5. Scope

The RMC must manage all risks that have a direct or indirect impact on the achievement of ICT Services objectives.

6. Membership

The RMC is a committee consisting of ICT Services staff members and does not include any members from the UFS business community or the UFS academic community. The RMC is comprised of the following members:

- The heads of the customer-facing delivery divisions
- The heads/leads managing each of the internal service divisions
- The chairpersons of each of the CoMs (if not yet represented in the foregoing groups)
- The secretariat
- Advisory members (based on the special needs of the RMC)

7. Roles and Responsibilities

7.1 Committee

It is the responsibility of the committee to:

- Create a culture of risk awareness at ICT Services to ensure that risk management forms an integral part of daily operations and that risk management is applied as an ongoing process.
- Assess and rank the impact and likelihood of identified risks.
- Review and evaluate the effectiveness of internal controls and mitigation strategies.
- Decide on the best mitigation strategy to manage risks to an acceptable level.
- Ensure that the ICT Services management considers appropriate risk responses and implements them.
- Monitor the mitigation plans to ensure fulfilment of the plans before the due dates.
- Update the UFS risk register and the ICT Services risk profile to ensure proper and timely reporting to the Support Services Risk Management Committee.
- Make recommendations to ManCo and the committees of ManCo to mitigate risks to an acceptable level.
- Review any material findings and recommendations by assurance providers (e.g. Internal Audit and external auditors) and ensure that appropriate action is instituted to address the identified control weakness.
- Conduct other risk-related activities as requested by ManCo or the Support Services Risk Management Committee.

7.2 RMC Manager

The RMC Manager is the chairperson of the RMC and oversees the management of risks through the RMC. All governance pertaining to the RMC is created and maintained by the RMC Manager. The RMC Manager must ensure that committee members are informed about policies, procedures, standards and guidelines as stipulated by the Support Services Risk Management Committee. The RMC Manager does not have a vote in the RMC, but does have the right to escalate a decision to the ICT ManCo and/or refer the risk to another CoM. Referral or escalation happens in accordance with the engagement model as described in Section 14.

7.3 Permanent Members

The permanent members are the heads of the customer-facing and internal service divisions (excluding the RMC Manager). Permanent members must manage and report on all ICT Services risks. Permanent members are responsible for drawing attention to all newly identified risks at RMC meetings and to create a culture conducive to risk disclosure and awareness in their units. Permanent members have voting rights.

A permanent member must, in writing, delegate a proxy to act on his/her behalf when he/she is not available for a meeting. Proxy members may not vote.

7.4 Secretariat

The secretariat is responsible for arranging meetings, preparing minutes, delivering a complete agenda, and distributing relevant documentation in a timely and professional manner and in accordance with the Committee's requirements. The secretariat does not have any voting rights.

7.5 Advisory Members

The RMC can invite internal or external advisors to the RMC to share their expert knowledge on applicable risk-related matters. Advisory members do not have any voting rights.

8. Meeting Types and Schedules

The RMC convenes the following types of meetings:

- **General RMC meeting** – A general RMC meeting considers risks as identified by permanent members and the other CoMs. This type of meeting takes place as often as necessary to ensure it manages identified risks in a timely manner to assist ICT Services in achieving its objectives.
- **Review RMC meeting** – A review RMC meeting only considers and evaluates risks on the UFS risk register, ICT risk profile and UFS compliance register. This type of meeting takes place as often as necessary, but at least three times a year to ensure it fulfils its responsibility to provide feedback to the UFS Support Services Risk Management Committee.
- **Emergency RMC meeting** – An emergency RMC meeting considers single risks that need urgent attention to ensure a stable, safe and secure operating environment. This type of meeting takes place as soon as possible after an emergency risk has been identified.

9. Agenda

The RMC must see to it that an agenda is prepared for every meeting and that minutes are kept of all meetings. Members can add items to the agenda before or at the start of a meeting.

10. Decision Register

All decisions must be noted in the meeting minutes.

11.Action List

All actions to be taken by members must be noted in the meeting minutes.

12.Communication

All RMC communication is conducted through two channels. If the communication is of a formal nature, it is done through the official communication function of ICT Services. General communication, however, is performed by individual RMC members, who communicate with their individual constituencies.

13.Governance

13.1 Principles

- The RMC operates as part of an ICT Services governance structure referred to as the ICT Services CoM.
- The RMC must manage all risks that have a direct or indirect impact on the achievement of ICT Services objectives.
- A quorum of two-thirds is required to mandate meetings.
- Democratic decision-making applies. Although all opinions are heard and considered, the formal decision must be supported by all, irrespective of individual opinion.
- Decisions require a two-thirds majority of the total voting membership.
- The decision of the RMC is final and can only be overruled by ManCo.
- ManCo must ratify RMC minutes and submissions.
- The roles and responsibilities described in Section 7 must be adhered to.
- Contravention of the rules and regulations of the RMC is a corporate offence and may be dealt with through the normal HR disciplinary process.

13.2 Policy

All the principles, rules and regulations stipulated in this document must be adhered to.

13.3 Procedures

All procedures related to the governance of the RMC are defined, revised and approved by the RMC and ratified by ManCo. These procedures are added as Appendixes to this document.

13.4 Standards and Guidelines

The RMC uses the COBIT framework as a risk management guideline.

14.Engagement Model

The figure below illustrates the relationship between the RMC and the other committees of ManCo: