Risk Management Framework

Managing Risk at the University

Risk and Compliance Office
Effective from 07-10-2014

Contents

Figures

Please note that the BWise risk and compliance management software will be live shortly. Whilst transition from current systems to the software occurs, the principles and processes of risk management written in this framework will still apply. For any queries regarding the transition to BWise, please contact the Risk and Compliance Office.

1 Risk Management Framework

A robust risk management framework is essential to ensure the University makes well informed decisions and achieves the strategic objectives outlined in *LIVE the Future 2020*. Risk management enables key stakeholders to understand and respond to the risks that may affect business objectives' effectiveness and efficiency.

The University's Risk Management Framework is aligned to Standards Australia and Standards New Zealand *AS/NZS ISO 31000: 2009 Australian/New Zealand Standard: Risk management – Principles and guidelines*.

Risk management provides current information of the strengths and weaknesses within the University in managing the risks it faces. Through understanding the impact of the University's risks and how effectively they are being managed the University is able to make key business decisions with confidence, knowing that the outcomes of the decisions made are manageable and within the University's capability and capacity.

Risk management engages the organisation in the identification, treatment, monitoring and reporting of business risks and ensure appropriate strategies are in place to mitigate risk and maximise opportunities to an acceptable level (refer to the risk tolerance below). By understanding the risks to the University and ensuring that they are kept within the University's risk tolerance, it is able to operate efficiently and maximise the benefits gained from its resources and systems.

In a modern business environment, risk can never be completely eliminated; having a framework that assists the business to assess and manage risks in a proportional and consistent manner is important.

The University's Risk Management program includes the totality of structures, including methodology, training, procedures and *website* that provide the foundation for the University's implementation, review and improvement of risk management. Corporate Governance, Risk and Compliance Services (CGRCS) coordinates the Risk Management Program and provides support and guidance to members of the University in relation to risk management and reports to the Executive and Audit and Risk Committee of the University Council in relation to risks and the overall risk management program.

1.1 Purpose of the Risk Management Framework

A risk management framework provides the tools and guidance for risk management to be performed in a consistent, proportional and prioritised manner. It outlines the different processes related to the University's risk management, so that it is accessible University wide, thus instilling a risk conscious culture. The processes outlined in the Risk Management Framework ('the Framework') are designed to make staff understand risk management and the components and processes involved and assist staff in fulfilling their risk management duties.

The key accountabilities and responsibilities are also detailed within the Framework, to ensure clarity to all areas of the University where accountabilities and responsibilities for risk management are assigned.

In understanding risk exposures and opportunities, and linking these to strategic and operational planning the University will:

- fulfil the University's objectives whilst minimising the effect of major risks;
- ensure its operations improve its reputation;
- operate in an ethical and responsible manner, ensuring that staff, students and the broader community are protected and that physical property is protected from loss or damage;
- improve efficiency of its operations and maximise its resources
- explore beneficial business opportunities;

- improve the University's resilience and ability to succeed with any changes to its operating environment

1.2 What is risk?

Risk is 'the effect of uncertainty on objectives' (the likelihood and consequence of an event occurring that will impact the objectives of the organisation) as defined by Standards Australia and Standards New Zealand (*AS/NZS ISO 31000: 2009 Australian/New Zealand Standard: Risk management – Principles and guidelines*.*)* As such, risks can be both positive (e.g. assessing whether to maximise an opportunity) and negative (e.g. failing to comply with requirements) in nature.

Risk may arise from both external factors (change in student demographics, government policy etc.) and internal factors (new projects, restructures, infrastructure etc.).

1.3 Why is risk management important?

Risk influences every aspect of the University's operations, it is therefore critical that risks are understood and managed appropriately. It is through understanding those risks that the University can make informed decisions regarding operating a successful business in terms of strategic achievement, student satisfaction, financial viability and the overall ability to manage changes effectively. Managing risks is important as it prepares the University for potentially adverse business outcomes. Through risk management preparation, the University is able to not only reduce the impact of the consequences of the risk, but also improve operational efficiency.

1.4 Accountabilities and responsibilities

Every University staff member has an active role to perform in establishing and maintaining a robust risk management culture and process. Notable responsibilities include the Executive and the University Council, who hold ultimate responsibility for risk management, which includes approval of the University's risk tolerance and risk management framework, and the Risk and Compliance Office who are responsible for oversight, guidance and advice on risk management.

Key responsibilities are outlined in Appendix B: *Responsibility and Accountability for Risk and Compliance Management*.

1.5 Risk tolerance

Not all risk can be avoided or mitigated — it would not be practical to do so. All organisations have to accept some level of residual risk. In order to understand the amount of risk the University is prepared to accept in order to meet strategic objectives, risk tolerance must be determined. The risk tolerance is the amount of risk that the University is willing to accept.

The University's risk tolerance is determined by the Executive, considered by the Audit and Risk Committee and approved by the University Council. The University's risk tolerance will change with circumstances in the internal and external environment. Therefore it is necessary to review the risk tolerance at least annually, or more frequently if required.

Currently the University's risk tolerance is reflected in the Risk Assessment Matrix in Schedule A: Risk Assessment Matrix in the Risk and Compliance Policy. Using this matrix, tolerable risk ratings are able to be assigned for all risks which indicate the level of risk Deakin is willing to accept for that particular risk. Tolerable risk ratings are aligned with the University's overall risk tolerance, enabling it to fulfil its objectives and make more informed decisions.

1.6 Risk registers

Risk registers document the results of the risk assessment and management process, as they document the identified risks, any contributing factors impacting the risks, the current controls to mitigate those risks and any action plans to further mitigate the risks, along with an assessment of the consequence and likelihood of these risks occurring from an inherent, residual and tolerable perspective. Risk registers are stored in the BWise software system. BWise is the software used to store risk registers and treatment plans. For more information please refer to section 5 risk software (BWise) and the *Risk and Compliance Office website.* There are currently two tiers of risk registers: strategic (L0 in BWise) and operational (L1 in BWise).

The strategic University risk register is owned by the Executive and contains critical organisational wide risks, which link directly to the strategic objectives outlined in the University's strategic plan — *LIVE the future: Agenda 2020*. Operational risk registers are maintained by the relevant Faculties Institutes and other areas (FIOAs) of the University and document specific localised operational risks. By recording risks in this way, it allows for operational risks to be appropriately aligned with strategic risks and enable a holistic approach to managing all University risks, showing the objectives that have sound mitigation strategies and management of any threats and those that require improvement, while also maintaining appropriate accountability.

Risk registers are continually reviewed and updated by FIOAs to ensure that appropriate and current risks are recorded along with the relevant key controls, as well as the progress of action plans. This continual review is also a chance to identify any new and emerging risks which should also be monitored.

1.7 Project risk

Project risks are first identified in business cases that are submitted to the Deakin Portfolio Office (DPO). These business cases are also reviewed by the Risk and Compliance Office to provide risk advice to ensure that all known risks have been identified and the proposed controls are effective in mitigating those risks. The Director, CGRCS is the validator for the risk section for every business case. At this stage the Risk and Compliance Office can recommend that relevant project risks are added to the FIOA's operational risk register or strategic risk register if appropriate.

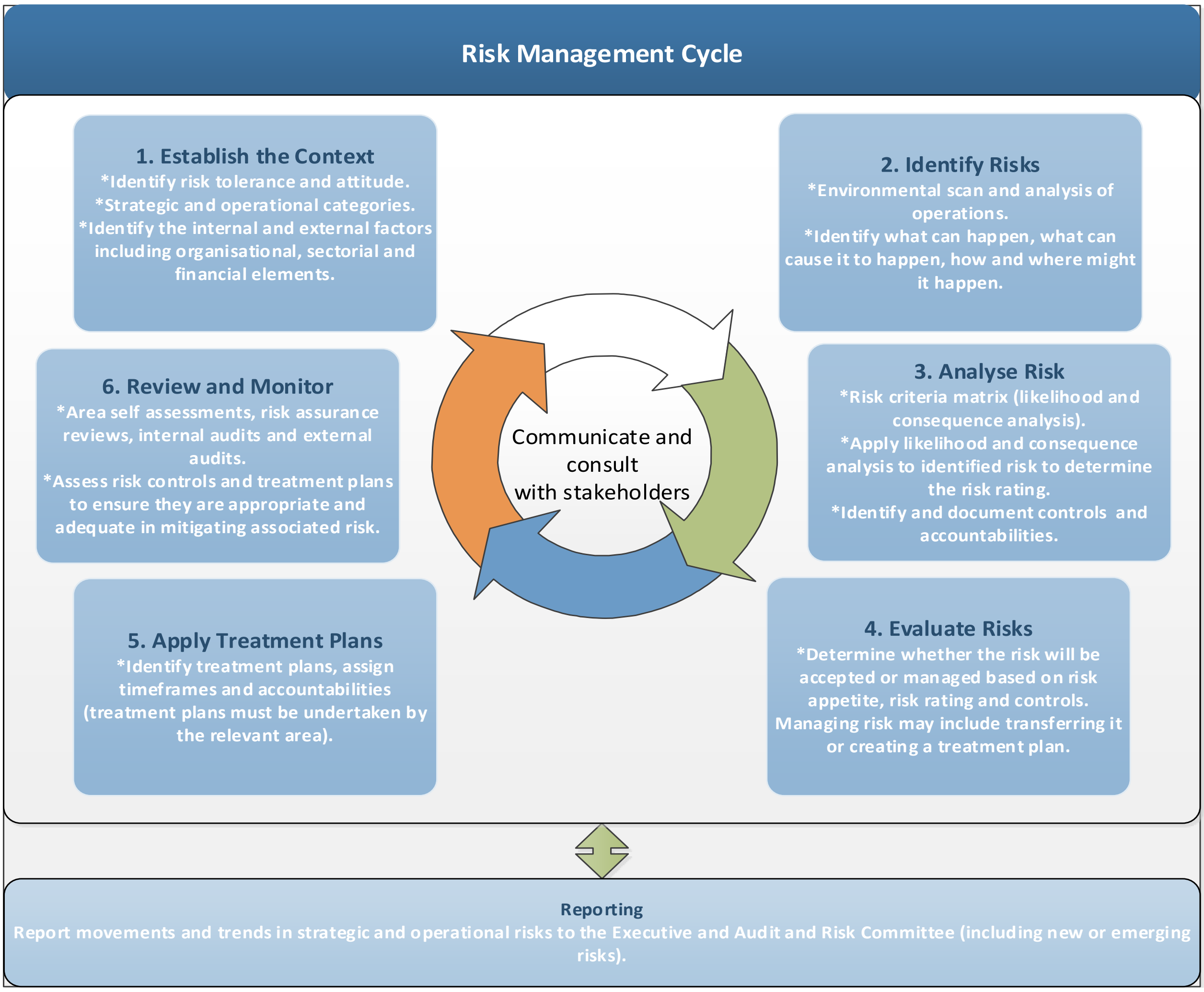
This step will only be taken for projects that the DPO deems as major and/or have the potential to negatively impact the strategic objectives of the University. Monthly reports will be received by the Risk and Compliance Office on these projects. If appropriate the Risk and Compliance Office may escalate risks to the Audit and Risk Committee.

The DPO is responsible for the monitoring and reporting of all project risks to the Deakin Portfolio Board and Project Managers are responsible for managing project risks.

2 Risk management methodology

There is a standardised approach to how the University identifies, assesses and manages potential risks as documented in the risk management framework. This process is aligned and compliant with the *AS/NZS ISO 31000: 2009 Australian/New Zealand Standard: Risk management – Principles and guidelines* and illustrated in the diagram below:

*Figure 1: Based on the Standards Australia and Standards New Zealand (*AS/NZS ISO 31000: 2009 Australian/New Zealand Standard: Risk management – Principles and guidelines*)*



Risk Management Cycle

1. Establish the Context
*Identify risk tolerance and attitude.
*Strategic and operational categories.
*Identify the internal and external factors including organisational, sectorial and financial elements.

2. Identify Risks
*Environmental scan and analysis of operations.
*Identify what can happen, what can cause it to happen, how and where might it happen.

3. Analyse Risk
*Risk criteria matrix (likelihood and consequence analysis).
*Apply likelihood and consequence analysis to identified risk to determine the risk rating.
*Identify and document controls and accountabilities.

4. Evaluate Risks
*Determine whether the risk will be accepted or managed based on risk appetite, risk rating and controls. Managing risk may include transferring it or creating a treatment plan.

5. Apply Treatment Plans
*Identify treatment plans, assign timeframes and accountabilities (treatment plans must be undertaken by the relevant area).

6. Review and Monitor
*Area self assessments, risk assurance reviews, internal audits and external audits.
*Assess risk controls and treatment plans to ensure they are appropriate and adequate in mitigating associated risk.

Reporting
Report movements and trends in strategic and operational risks to the Executive and Audit and Risk Committee (including new or emerging risks).

2.1 Establish the context

Understanding the context of the risk is an important preparatory step to the risk management process. Through understanding the context and the factors that affect the University, the University is able to better understand the risks to its operations and make a more informed and appropriate decision on the treatment of risks.

The strategic context refers to potential impacts on the ability for the University to realise strategic objectives, and have the potential to impact the entire University. Strategic risks can come with very high risk and also very high return, and should be managed at the Executive level. For the University, this refers to risks of not fulfilling the objectives of the *LIVE the future: Agenda 2020*. These risks may result from changes within the University's operating environment, including regulatory, sectorial, political and global & domestic economies that impact on the operation of the entire University.

Operational context is related to the changes that impact the ability of a specific area to achieve normal business operations, and may only impact one specific area of the University. Operational risks can affect the day to day running of a particular area of the business and should be managed and mitigated by internal controls. Often operational risks will align/contribute to the strategic risk context (e.g. level of strategic health and safety risk will be derived through operational risks in this area). These risks may result from operational context changes in the area such as changes in the area's systems, objectives, and structure or stakeholder requirements.

2.2 Identify the risk

The first step of the risk management process is to identify risks relating to both the strategic and operational context.

Risks can be internal or external to the organisation, and the causes and implications of the risk could involve other entities with connections to the University that are abroad, as well as the wider community.

Risks are typically identified through an examination of the University strategy and/or FIOA operations, and discussing potential events (or risks) which could impact upon the successful performance of the strategy or operations.

Risks are also identified through a number of other methods, including:

- risk identification workshops
- scenario analysis
- identifying and understanding the external environment (e.g. changes to government policy, legislative changes etc.)
- flowcharts, inspections and checklists to analyse work procedures (systems analysis)
- surveys
- lessons learned
- market and sector research
- specialist knowledge

Capturing the nature of the risk in the risk title is important for clarity and to avoid misunderstanding. The risk name should read like an event and not be a contributing factor, cause or consequence of a risk. It is essential that the BWise naming convention is applied (please refer to BWise training manual available on the *Risk and Compliance website* for further information).

Strategic risks have been grouped into the four categories outlined in *LIVE the future: Agenda 2020* (learning, innovation, value, experience).

A number of sub categories have been developed to enable grouping of like risks. These include:

- quality teaching and learning
- quality research
- financial viability
- resources and infrastructure
- community engagement
- communication and positioning
- students and staff

Once risks have been identified, a responsible risk owner must be assigned. For strategic risks, ownership and also approval of changes and treatment plans must sit at the Executive level. Whilst operational risks will still be owned by the member of the Executive for the area, approval of changes to risks and treatment plans may be delegated to a person that is at manager level or above. The risk owner is to ensure that the information regarding the risk is accurate and that all actions required to mitigate the risk are implemented to reduce the risk to its tolerable rating. Please also refer to *Appendix B: Responsibility and Accountability for Risk and Compliance Management*.

When the risk name, context and owner have been determined and recorded, the causes and consequences need to be recorded in the risk software BWise. This step is particularly important and needs to be accurate as this will inform the risk analysis and also help determine any mitigation steps that may need to occur.

Ensure all the information regarding the contributing factors of the risk and also the risk itself has been accurately documented in the risk software BWise, to ensure the next step, the analysis is undertaken with the correct information.

2.3 Analyse and evaluate the risk

Analysing the identified risk requires an assessment of impact and likelihood outcomes if the risk were to eventuate. This enables each of the identified risks to be consistently rated across the University, so that the risks can be appropriately compared and any required action can be prioritised.

OHS (Occupational Health & Safety)	How the consequences of the risk affect the health and safety of staff, students, contractors, visitors and the Deakin community, including physical and psychological well-being and ensuring facilities provide a safe environment for all.
Financial	The impact of the risk on Deakin's financial status and budgets in the long and short term and what affect it will have on Deakin's operations.
Environmental	How the risk will affect the environment including contamination and damage to the land, animals and plant life.
Reputation, Outrage & Media	The impact of the risk outcomes on Deakin's reputation and portrayal in the media. Consider how widely reported the risk outcomes would be and also to what extent the Deakin brand would be damaged and whether it would only be partially damaged regarding a specific area/Faculty or generally as a whole. Also consider the severity of the negative reactions of the Deakin community and the public and the repercussions of these reactions.

University Performance	How the risk outcomes affect Deakin's ability to achieve its strategic objectives as per the Live the Future 2020 plan. Will it affect its ability to perform as a University and fulfil its main objectives regarding areas such as research and conducting courses for students? Also consider how the risk outcomes may prevent Deakin in operating in its day to day environment.
Regulatory	Looks at the impact of the risk from a compliance perspective, such as potential breaches of legislation and University policy and procedure. It also looks at the impact of the risk consequences on the University's various licences and ability to be registered as a University.

The University's Risk Assessment Matrix outlines six impact and likelihood ratings to perform this assessment. The above impact categories have been explained so as to provide the context and criteria to which the risk are to be assessed and managed. This criteria is to be applied to all risk assessments, however not all the categories will always be applicable, if this is the case this is to be indicated in the risk assessment.

The University's risk framework identifies three types of risks in performing an effective analysis and evaluation of its risks:

a) Inherent risk rating (considering the potential risk without any controls or actions)
b) Residual risk rating (the level of risk after the current controls in place to manage the risk have been identified and assessed)
c) Tolerable risk rating (the level of risk the University is willing to accept, in line with the University's risk tolerance).

The first risk assessment is undertaken without taking into consideration current controls or actions (the inherent risk rating).

The impact rating must be determined against one or more of the six impact categories (e.g. financial, reputational etc.). When multiple impact categories have been selected for the inherent rating, select the highest rated impact rating and use this as the overall impact rating for the risk.

Once the impact rating has been established, a likelihood rating has to be selected for each impact rating. Select the highest likelihood rating and record this against the risk. When the overall impact and likelihood ratings have been determined, using the Risk Assessment Matrix the overall inherent risk rating can be determined (based on the impact rating against likelihood rating). This is recorded against the risk in BWise.

Controls are then required to be assessed and rated for their overall effectiveness in mitigating the risk using the Risk Assessment Matrix. Controls are defined as any action currently in place to manage a risk, usually to lower it. Examples of controls could be to establish a procedure or a policy or establish quality checks and reporting, which all may be useful, for example, for a risk related to incorrect payments being made. The controls should address the causes of the risk.

There are different types of controls that can be used. Using a range of types of controls is recommended so as to reduce the risk more effectively and efficiently. Please see below explanation of the different categories of controls:

Directive Controls

Controls designed to encourage desired behaviours and outcomes – as such, they can reduce both the likelihood and impact of the risk:

- Training and supervision
- Policy and procedure documents, guidelines and other manuals
- Position Descriptions

Preventative Controls

Designed to limit the possibility of an undesirable event from happening – as such, they reduce the likelihood of the risk**:**

E.g. –access controls (either physical or system access), authorisation procedures, separation of duties

Detective Controls

Controls that detect the occurrence of an undesirable event – as such, they also reduce the likelihood of the risk:

- Checking / monitoring of exception / error reports
- Quality Assurance checks e.g.: checking for consistency in assessments
- Reconciliations (e.g. bank reconciliation)

Corrective Controls

Controls designed to restore normality after the occurrence of an undesirable event – as such, these controls can reduce the impact of the risk:

- Complaint procedures
- Incident management procedures
- Business Continuity Plans

Based on the information received on the strength and effectiveness of the controls in mitigating the risk and the overall rating of the controls, the impact ratings used to form the inherent risk rating and the likelihood rating are re-rated. Take the highest impact rating and the likelihood rating and use the Risk Assessment Matrix to generate the residual risk rating.

A tolerable risk rating is developed based on the understanding of the University's risk tolerance.

2.4 Evaluate and treat the risk

Using the residual and tolerable risk ratings, it then needs to be determined how the risk will be managed and the type of risk treatment that is required. Risk treatment enables an evaluation of how the identified risks will be treated (if necessary).

An assessment needs to be made as to whether any further actions are required to manage the risk. This is performed by comparing the residual risk rating (i.e. the current risk level) against the tolerable risk rating (i.e. the desired level).

If the residual risk rating is the same as the tolerable risk rating then no further action is necessary as the risk is already at an acceptable level. If the residual risk rating is higher than the tolerable risk rating, then action is required and treatment plans must be put in place to mitigate the risk further, and reduce the residual risk rating to the tolerable level within a reasonable time period. If the residual risk rating is lower than the tolerable risk rating, then an analysis of the current controls is to occur as there may be too many controls to mitigate the risk. There might be controls that can be removed due to the high efficiency or effectiveness of other controls. The effectiveness of the controls in reducing the likelihood and or impact of the risk needs to be assessed, is the key criteria in establishing which controls and/or treatment plan are to be implemented

Selecting the most appropriate risk treatment involves balancing the costs and efforts of implementation against the benefits derived, i.e. the level by which the likelihood and impact are reduced. The treatment would also need to be assessed to ensure that it is workable within the wider operations of the University and does not create issues or duplication with other areas. When selecting a treatment plan it is also important to observe legislative requirements.

The strategies to manage risk can typically include transferring the risk to another party (e.g. insurance), avoiding the risk (e.g. this is achieved through multiple methods including discontinuation of activities that cause the risk), establishing measures that may minimise the consequences of the risk and/or the chance of the risk occurring, or prepare to accept the outcome if the risk were to occur.   To reduce risk, treatment plans are used and recorded against the risk. The treatment plans to manage the risk may comprise a combination of the above strategies (e.g. transfer part of the risk through insurance and reduce the likelihood through implementing additional controls).

Every treatment plan requires a person who is responsible for implementing the plan and an approver who ensures that the plan has fulfilled its objectives and is working efficiently to mitigate the risk. Included in the treatment plan should a schedule of the steps that are to be implemented. The schedule of the treatment plan should take into consideration the timeframe in which the risk is to be mitigated as per the description of the residual risk rating in the Risk Assessment Matrix, for example a high risk is only acceptable in the short term whilst the treatment plan is being completed, therefore it would need to be mitigated immediately.

A timeframe for the implementation of the treatment plan must also be assigned, and should align with the relative priority for mitigating the risk (e.g. if there is a high residual risk with a low tolerable risk, it would be expected that some treatment plans would be implemented in the short term to reduce the residual risk rating).

For high and very high inherent risks, the University will expect active management, regular monitoring by the Risk Owner and reporting to the Executive and Audit and Risk Committee by the Risk and Compliance Office.

Medium and low risks are more tolerable, with the University expecting regular monitoring by the Risk Owner.

Once treatment plans have been fully implemented, adjustments will need to be made to the risk register to appropriately reflect this, for example there may be a new control as a result of the treatment plan which may reduce the residual risk and therefore needs to be recorded against the risk in the risk register.

2.5 Monitor and review

The University's environment is constantly changing and hence the University needs to continually monitor and review its risks and the effectiveness of its risk management (including controls and treatment plans).

Ongoing reviews of strategic and operational risk registers will be facilitated by the Risk and Compliance Office, as well as an annual detailed review for all risk registers (both strategic and operational) to ensure risks and controls are still current and to ensure new or emerging risks have been identified. More frequent reviews of all strategic risks and very high and high operational risks will occur, with a particular focus on progress of treatment plans.

All strategic risks are reviewed by the Audit and Risk Committee five times a year while operational risks are reviewed by the Audit and Risk Committee on an annual basis.

The University Council reviews the University's risk profile annually, and receives reports from the Audit & Risk Committee in relation to risk management as necessary.

The risk assurance undertaken by the University as detailed below also forms part of the monitor and review process.

Risks with a very high residual risk rating are to be escalated to both the Vice Chancellor and to the responsible Executive member and risks with a high residual risk rating are to be escalated to the responsible Executive member. Medium rated residual risks are to be escalated to the responsible Director or Faculty General Manager for evaluation and action.

Should a stakeholder disagree with the contents in their risk register, risk reports or assurance review reports, then they can escalate their concerns to the Manager, Risk and Compliance in the first instance and then if appropriate to the Director, CRGCS.

3 Risk assurance

The Risk and Compliance Office understands that risks are managed on a daily basis by management and employees (through implementation of internal controls as a normal part of business operations). However, some risks that pose a greater threat to the University require additional support to ensure efficient and effective management.

There are three levels of 'assurance' that will be undertaken at the University:

- Self-assessments undertaken by the responsible risk owner (this includes checking that the controls for the risk are still relevant and achieving their objective in mitigating the risk and are cost effective. The risk owner should ensure also that controls are used in practice in a consistent manner. They should ensure all the risks and associated controls are captured in the risk register.)
- Risk assurance reviews conducted by the Risk and Compliance Office.
- Internal audit reviews and external audits (e.g. ISO certification).

For low and very low inherent operational risks, a heavy reliance will be placed on self-assessments. For medium, high and very high operational risks and all strategic risks, an appropriate combination of all three assurance approaches, in a coordinated fashion, will be taken to ensure an effective and efficient approach to managing these risks and that the required risk treatment is being undertaken.

An assurance map will be developed with a review occurring annually, to ensure that an appropriate level of assurance is provided for strategic and key operational risks. The assurance map will detail the kind of assurance, for example an internal audit, or assurance review that is to occur on the University's risks. This will ensure that there is adequate assurance of risks and reduce duplication.

As stated above, the frequency of risk assurance reviews will be determined by the inherent risk rating, with higher rated risks and associated controls/risk treatment plans being reviewed more frequently than low and very low risks. The inherent risk rating is used to prioritise risks, as they are the risks that could potentially cause the most damage to the University if not adequately controlled.

Risk assurance reviews will include:

- ensuring risks appropriately reflect the reality of the University's strategic and operating environment and risk tolerance levels
- review of risk ratings (likelihood and impact)

- review and validation of the adequacy and effectiveness of existing risk controls / treatment plans and recommend changes to treatment priorities & timeframes. Recommended changes may include methods to strengthen controls and/or the creation of new controls.
- identify new or emerging risks
- include consideration of the appropriate "responsible person(s)" for ongoing monitoring and review of risks within the University's risk register / risk management system.

An annual assurance plan is created using the stated method of prioritisation and in conjunction with the Internal Audit Annual Plan, to avoid duplication and concentration in the same areas. The plan is then presented and approved by the Executive and the Audit and Risk Committee.

4 Reporting

Governance Level

Audit and Risk Committee

The Audit and Risk Committee exercises a governance role on behalf of Council to ensure risk accountability is being properly exercised. The University's strategic risks (including any associated controls, treatment plans and status updates) are reported to the Audit and Risk Committee at every meeting. Any identified new or emerging risks, along with status updates on very high and high operational risks are also regularly reported to the Audit and Risk Committee. The strategic risks owned by the Executive and reviewed by the Audit and Risk Committee make up the University risk profile provided to and reviewed by Council annually. The operational risks are reviewed during the annual Audit and Risk Planning Day, and are considered in relation to the assurance program and internal audit plan for the coming year.

Management Level

All strategic and operational risks are monitored by FIOAs and the Executive and coordinated by the Risk and Compliance Office.

The Executive

The Executive receives regular reports from the Risk and Compliance Office, which are endorsed prior to each Audit and Risk Committee meeting. These reports include information on:

- University strategic risk register
- New and emerging strategic risks
- Changes to strategic risks

Senior Management/FIOA Directors

Each senior manager/director of all FIOAs will receive regular updates on the operational risks relevant to their area and the progress made (including outstanding treatment plans, etc.)

Internal Audit

The risk registers form part of the assessment and planning undertaken by Internal Audit in preparing the Internal Audit annual plan, as well as prior to each individual audit being performed. Internal Audit also performs an assessment of risk management practices for each audit they perform, with the results being reported back to the Risk and Compliance Office for information and appropriate action.

Report and Review Schedule

Please refer to the Risk and Compliance Office website for more details.

5 Risk software (BWise)

BWise is the risk software used to house all risks and treatment plans across the whole University. Please note that access to BWise will only be given to the designated Risk Administrator and Owner and persons assigned to implement treatment plans. For user guides and any further information on BWise, please refer to the Risk and Compliance Office website or contact the Risk and Compliance Office.

6 Training

The Risk and Compliance Office will be responsible for providing training and advice to all required areas of the University. Training will be tailored to the needs of each area and be based around the risk management framework and methodology. For more information on training please contact the Risk and Compliance Office.

7 Advice and support

Please contact the Risk and Compliance Office for any advice and support in relation to risk management.

Risk and Compliance Office contact details:

Website: *https://wiki.deakin.edu.au/display/staff/Risk+and+Compliance*

Email: *riskandcompliance@deakin.edu.au*

Appendix A – Glossary of terms

Assurance: Assurance is the monitoring and review of risk management, both by internal and external parties. Assurance activities, such as periodical reviews and audits, ensure that the established controls are implemented effectively, that areas requiring improvement are identified and further developed and find any potential unidentified risks.

Control: a measure, which could be one of or a combination of process, policy, device, barrier, practice, or other actions established to alter the level of likelihood and/or consequence of the risk event.

Control Rating: a rating that reflects the overall quality of the controls in place and their performance in changing (usually lowering) the inherent risk rating

Impact rating: a rating showing the magnitude of the impact the risk would generate on the impact category

Inherent risk rating: the level of the risk without any controls in place

Likelihood rating: a rating indicating the probability of the risk occurring

Operational risk: a risk that affects the ability for a sector of the University to complete its routine duties

Project risk: a risk that is associated with a specific project to be completed by the University

Regulatory authority: any government body or other organisation responsible for regulating or enforcing compliance with legislative and other requirements (e.g.: Tertiary Education Quality and Standards Agency, TEQSA).

Residual risk rating: The level of risk once controls have been established to alter the risk's likelihood or consequence.

Risk: is the 'effect of uncertainty on objectives', as defined by Standards Australia and Standards New Zealand (*AS/NZS ISO 31000: 2009 Australian/New Zealand Standard: Risk management – Principles and guidelines*.). Risk is typically characterised by reference to potential events, and measured in terms of a combination of the likelihood of the event occurring and the consequence if it was to occur.

Risk assessment: Overall process of risk identification, risk analysis and risk evaluation.

Risk Assessment Matrix: a matrix that facilitates the consistent assessment and measurement of risk across the University. It allows for the prioritisation of assessed risks and the determination of appropriate risk control measures and their importance in managing the risks.

Risk management: coordinated activities, processes, and structures in place and undertaken to direct and control risk across the university. The risk management process involves the systematic application of management policies, procedures, and practices relating to the risk management activities of communicating, consulting, establishing context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk management framework: A document outlining all the relevant components and processes for risk management across the University to ensure consistency of risk management application.

Risk management program: the totality of structures, including methodology, training, procedures and website that provide the foundation for the University's implementation, review and improvement of risk management.

Risk owner is accountable for:

a) New and current risks and compliance issues being managed with the appropriate controls and treatment plans
b) Ensuring controls to manage risks and compliance obligations are operating as expected, including performance of self-assessment reviews
c) Actioning breaches reported to them by their staff from a risk perspective – identifying root cause and implementing appropriate corrective action (in consultation with the Risk and Compliance Office)
d) Ensuring that recorded information regarding risk and compliance is completed and accurate.
e) Approve all changes made to risk registers, ensuring that the information is accurate. Please note that the risk owner and the 'approver' in the risk and compliance software are two separate roles. The 'approver' function may be delegated to another senior member of staff by the risk owner for operational risks.
f) Risk or Compliance Owners are to approve treatment plans, ensuring that they are implemented correctly, in a timely manner and any changes made to them have been appropriately explained.

Risk profile: description of a set of risks that can relate to the whole university, part of the university, or as otherwise specified. It will typically include some representation of the level/magnitude of the risks involved, expressed as a combination of likelihood and impact ratings.

Risk tolerance: the amount of risk the University is willing to accept in pursuit of its strategic objectives in accordance with the University risk tolerance levels.

Strategic risk: risks that affect the University's ability to realise its strategic objectives and have an impact on all the University

Tolerable risk rating: A risk rating indicating the maximum level of risk the University will accept for the associated risk, in line with the University's risk tolerance.

Treatment Plans: Treatment plans require actions that will reduce/mitigate the risk. It can involve avoiding activities that cause the risk, removing the source of the risk, changing factors driving either the likelihood and/or consequence, sharing or transferring the risk.

Appendix B — Responsibilities and Accountabilities for Risk and Compliance Management

Role	Responsibility / Accountability
Staff at all levels	Staff at all levels are responsible for: a) Developing an understanding of and applying sound risk management and compliance principals in their areas of work and embedding the University's risk management and compliance practices within general decision-making, operations, policies and procedures. b) Promptly reporting any risk related issues, concerns, or incidents/events and compliance breaches to their supervisors / managers, who will escalate them to the Risk and Compliance Office as appropriate. c) Being aware of common areas of legislation, University policy and procedure and appropriate professional standards that affect their day to day work and working relationships. Staff should also raise any concerns regarding issues and gaps as this will inform a robust risk and compliance training program. d) Ensuring that their activities on behalf of the University comply with the applicable laws and related University policies.
Compliance Implementation Officer	Compliance Implementation Officers are responsible for: a) Reviewing and making approved changes to the compliance obligations register on a regular basis. b) Ensuring all compliance issues are identified and included in their compliance obligations registers. c) The Compliance Implementation Officer is to be the main contact person for their area for all queries regarding compliance and are to escalate these as appropriate to the Risk and Compliance Office. d) Act on any compliance breaches identified by, or notified to, them in accordance with this framework, and participate in any breach investigation activity as required e) Co-ordinating the treatment plan and is also required to provide an explanation for any changes or delays to the treatment plan. Please note that for treatment plans, in the risk and compliance software BWise, the Compliance Implementation Officer is called 'Action Responsible'.
Risk Administrator	Risk Administrators are responsible for: a) Reviewing and making approved changes to the risk registers through the BWise software on a regular basis. b) Ensuring all risk issues are identified and included in their risk registers. c) Being the main contact person for their area for all queries regarding risk management and are to escalate these as appropriate to the Risk and Compliance Office. d) Co-ordinates the treatment plans including identification of the treatment plan and the appropriate stakeholders required, and the completion and monitoring all required tasks for the treatment plan. The Risk Administrator is also to provide an explanation for any changes or delays to the treatment plan. Please note that for treatment plans, in the risk and compliance software BWise, the Risk Administrator is called 'Action Responsible'.
Risk Owner and the Compliance Obligation Owner	Risk Owners and Compliance Obligation Owners are responsible for: a) New, emerging and current risks and compliance issues being managed with the appropriate controls and treatment plans.

	b) Ensuring controls to manage risks and compliance obligations are in place and operating as expected, including performance of self-assessment reviews and/or monitoring procedures c) Actioning compliance breaches reported to them by their staff – identifying root cause and implementing appropriate corrective action (in consultation with the Risk and Compliance Office) d) Ensuring that recorded information regarding risk and compliance is completed and accurate. e) Approve all changes made to risk and compliance registers, ensuring that the information is accurate. Please note that the risk "owner" and the "approver" are two separate roles in the risk and compliance software. The 'approver' function may be delegated to another senior member of staff by the risk owner for operational risks. f) Risk or Compliance Owners are to approve treatment plans, ensuring that they are implemented correctly and any changes made to them have been explained. g) Developing and delivering targeted risk and compliance training to relevant areas of the University as required.
Project Managers	Project Managers are responsible for managing project risks and reporting on them to Deakin Portfolio Office
Director, Corporate Governance, Risk and Compliance Services	The Director Corporate Governance, Risk and Compliance Services is responsible for/has the oversight of: a) Developing and maintaining the University's risk management and compliance management framework and standards (including breach reporting), providing technical risk management and compliance support and training and associated tools and practices. b) Reporting to the ARC on all aspects of both the risk and compliance framework, including academic risk and compliance issues. c) Compiling a University wide risk and compliance profile, including strategic and operational risks and compliance obligations for Executive and ARC reporting. d) Providing other relevant risk and compliance information to the Audit and Risk Committee and/or Executive (e.g. breach reporting trends, incidents etc.). e) Coordinating and supporting the establishment, ongoing maintenance and update of risks and compliance obligations for all areas of the University. f) Developing, implementing and maintaining a Risk and Compliance Assurance (control testing) Program (based on industry best practice), covering all risk and compliance obligations across all Faculties Institutes and other areas of the University. g) Coordinating the attestation process, breach reporting and any associated actions. Assisting areas to address issues in relation to breaches for rectification and continuous improvement. h) The Risk and Compliance Office receives advice regarding compliance obligation changes then we will ensure the relevant area is notified accordingly. i) In conjunction with the University Solicitor's Office, identify new and amended compliance obligations and consult with relevant areas on their applicability. j) In conjunction with the University Solicitor's Office, ensure that the University's compliance profile is reviewed annually. k) Reviewing all business cases, contracts over $400,000 and insurance waiver requests from a risk perspective. l) That all wholly owned entities are risk assessed bi-annually.
Deakin Portfolio Office	The Deakin Portfolio Office is responsible for the monitoring and reporting of all project risks to the Deakin Portfolio Board

University Solicitor	The University Solicitor is responsible for: a) Working with the Risk and Compliance Office to identify new and amended legislative compliance requirements. b) Providing advice to the Risk and Compliance Office in relation to legislative compliance matters when requested.
Vice Chancellor and Executive	The Vice Chancellor and the Executive are responsible for: a) Providing leadership and demonstrating commitment to the University's Risk and Compliance Management Frameworks. b) Ensuring that risk management is incorporated in the University annual planning cycle. c) Maintain an active oversight of the University's risk and compliance profiles (including ownership of strategic risks). d) Reviewing the Risk Assessment Matrix annually. e) Ensuring risk assessments are undertaken in relation to all material projects and initiatives, and that all material functions, procedures, systems, programs, business activities within their areas of responsibility are subject to periodic risk review. f) Ensuring risk registers and compliance obligations registers are established and maintained for their areas of responsibility. g) Ensuring treatment plans are implemented.
Audit and Risk Committee	The Audit and Risk Committee: a) Provides oversight of the University's Risk and Compliance Management Frameworks and associated programs. b) Endorses amendments to the University's Risk and Compliance Policy and Risk Assessment Matrix, which will be reviewed annually. c) Reports annually to the University Council on the status of the risk and compliance programs and associated outcomes. d) Is invited to endorse the Vice-Chancellor's annual attestation statement.
Academic Board	The Academic Board is responsible for: a) Oversight of all academic governance risks.
University Council	The University Council is responsible for: a) Overseeing and monitoring the assessment and management of risk across the University, including commercial undertakings and approving the University's Risk Assessment Matrix b) Overall responsibility for ensuring the University fulfils its legal obligations and effectively manages any risk exposure resulting from any legal compliance failures.