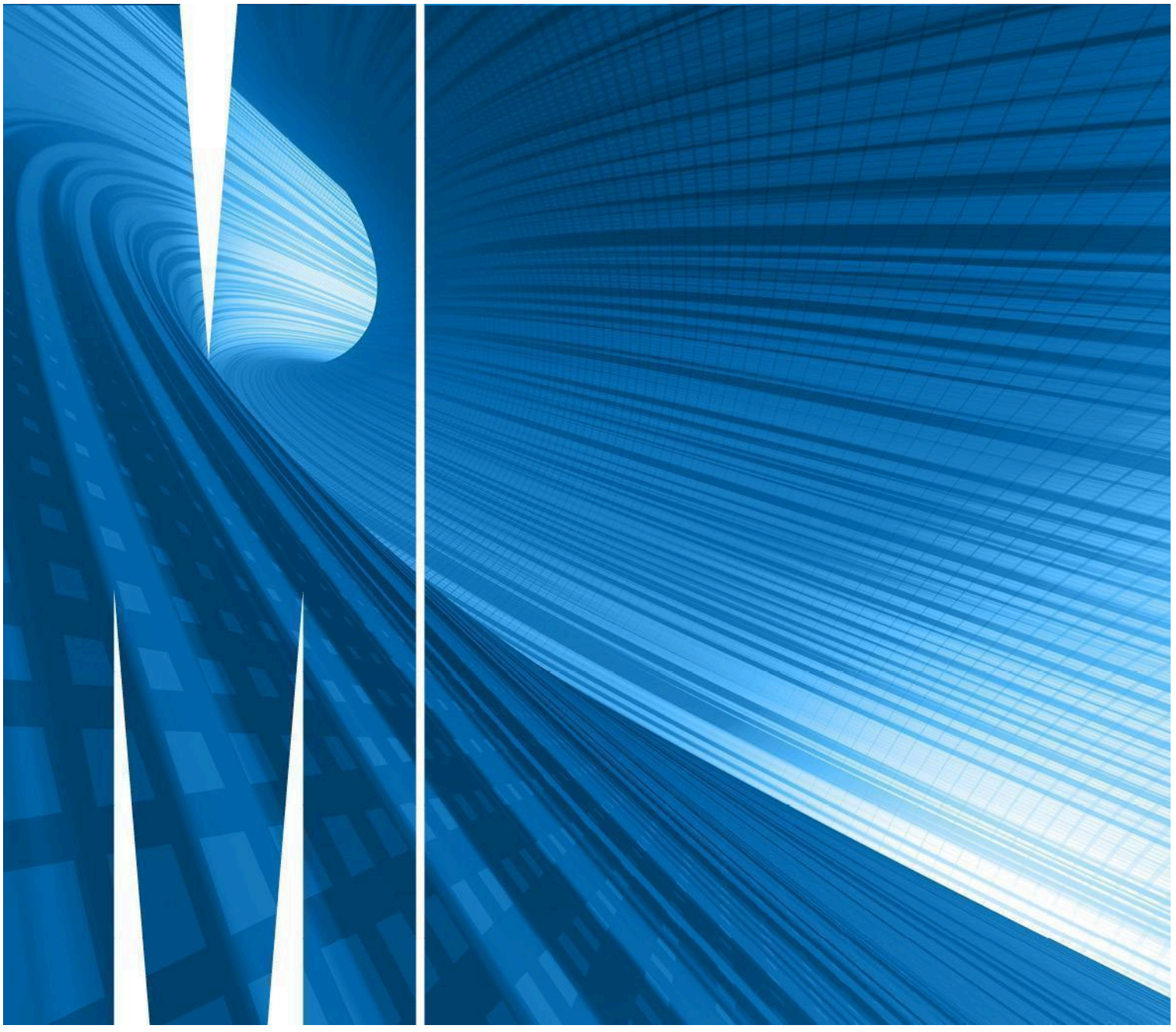
MONASH University

Risk and Compliance Unit

Group Governance, Risk and Policy

# Monash University Group Risk Management Framework



MONASH University

# CONTENTS

# VICE-CHANCELLOR'S FOREWORD

In a rapidly changing world, risk and compliance are now widely regarded as integral components of organisational management across various industries and sectors.

The diversity and complexity of Monash University's operations, across all its campuses and locations, make effective management of risk and compliance especially important and, at times, challenging.

As a global institution, Monash continuously seeks to review and enhance the suitability, adequacy and effectiveness of our risk management framework, policies and supporting tools.

This new Group Risk Management Framework is designed to better encompass all elements of the Monash Group, and to highlight the importance of risk management as a responsibility of every staff member.

The new Framework is accompanied by a new Group Risk and Compliance Management Policy, Group Risk Management Procedure, and Group Compliance Management Procedure.

Implementation of the Framework, Policy and Procedures will substantially enhance Monash's risk and compliance management maturity. It will take time and effort, and I look forward to your assistance so that we can reach better decisions that will help us to accomplish the goals set out in *Impact 2030*.

I encourage all staff to openly discuss risk and compliance matters with their managers, guided by the values and goals of *Impact 2030*, and by Monash's Risk Appetite Statement. Such matters include both 'downside' risks that could present a barrier to accomplishing our strategy, and 'upside' risks that need to be taken in pursuit of it.

Professor Sharon Pickering

Vice-Chancellor and President

MONASH University

## CONTEXT - THE MONASH GROUP

Monash University has over several decades become a global, complex and highly successful organisation comprising tens of controlled entities, associated entities, unincorporated "entity-like" structures, and a host of investments either directly or through its subsidiary, Monash Investment Holdings Pty Ltd. The number of such entities continues to increase, and the logic of Monash's strategy, *Impact 2030*, is that such growth is likely to accelerate as the University seeks to exert its influence in the world more directly. The term "Monash Group" is used to describe this collection of entities under the Group Governance Framework approved by Council. A visual map of the Monash Group is provided at Appendix 1.[1]

*Impact 2030* conceives of governance as a foundation for organisational sustainability, that is in turn a precondition to accomplishing strategic goals. Governance and risk are closely related: governance, broadly conceived, includes management of risk; from a different perspective, governance is central to mitigation of risk. The value of the 'Monash Group' concept to Monash's approach to governance is implicit in *Impact 2030*, which emphasises the importance of collaboration across different parts of the Monash global network of campuses and presences.

This Framework adopts a Group-wide approach to management of risk and compliance and the associated policy and procedures are titled accordingly. A Group-wide approach to risk management is essential, because a risk that materialises in a Group entity inevitably has consequences for the University itself.

The principles of managing risk and compliance are the same across the Group, but of course the context for managing risk and compliance in different parts of the Group varies significantly. In the case of unincorporated structures within the University, the various faculties bear both similarities and differences from a risk and compliance perspective. The same is true for institutes and centres, which are governed by the Institutes and Centres Policy and Procedure. In the case of controlled entities, some operate in multiple national jurisdictions - World Mosquito Program Ltd and Monash College Pty Ltd. Other major operating controlled entities are confined to a single country - Monash University Malaysia Sdn Bhd, and the entities that comprise Monash Indonesia. Compliance with the laws and regulations of jurisdictions outside Australia entails significant risk, especially for entities operating in developing countries (as a number of the Group's entities do), due to differences in language, culture and legal systems.[2]

## INTRODUCTION TO RISK AND COMPLIANCE MANAGEMENT

While they might seem distinct, risk management and compliance management are inherently intertwined, forming a symbiotic relationship that is crucial for the sustainable success and growth of any organisation. For the Monash Group ('Monash'), effective risk and compliance management is dependent on the governance structure, systematic management practice, and especially risk culture. Understanding the trade-off between risk and reward should be the common objective throughout the risk management life cycle. Establishing and maintaining a culture of compliance is the basis for successful and sustainable operations.

Risk governance is the formal structure used to support risk-based decision-making and oversight across the Monash Group. The risk governance structure needs to be appropriate to Monash's size, activity mix and complexity, to enable the organisation to fulfil its purpose and goals. One such model that has been widely adopted is the Three Lines Model,[3] and the full adoption of the model - especially ownership of day to day accountability for risk and compliance management throughout the organisation - is key to successful risk and compliance management.

Good risk and compliance management reflects the iterative and routine nature of risk and compliance management practice. It is important to avoid placing excessive emphasis on achieving short-term results, deliverables, or a rigid "tick-box" mentality. Instead, consistency and pragmatism should be the key characteristics of Monash's risk management practice, demonstrated in the design and implementation of risk management policies, procedures and processes.

## RISK CULTURE

The risk and compliance management international standards stress that the risk culture of an organisation is a pivotal factor that determines its success in accomplishing its purpose. Risk culture refers to the collective attitudes, behaviours, and values within an organization regarding risk management and decision-making. A positive risk culture - one where staff at every level appropriately manage risk as an intrinsic part of their day-to-day work - drives good risk outcomes.

---

[1] Note that, while many controlled entities within the Monash Group are required to be consolidated in Monash University's annual accounts by virtue of the University's control or influence over them, not all entities are consolidated in this way yet are part of the Monash Group.

[2] Deloitte, *Governance of Subsidiaries: A survey of global companies* (2013), 13.

[3] The IIA'S Three Lines Model - An update of the Three Lines of Defense.

A number of factors shape risk culture. Of particular importance is 'the tone from the top'. The risk culture of the Monash Group is strongly influenced by the Council, Council committees and senior executives. Equally, all those in leadership roles at Monash should play a part in valuing and creating a positive risk culture. Other factors that are important in building a positive risk culture include: strategy, accountability, transparency, an environment in which it is safe to escalate bad news, embedding risk and compliance expectations in employment arrangements, and allocating adequate resources.

## PURPOSE AND APPROACH

This Monash Group Risk Management Framework (GRMF) articulates Monash's approach to risk management in principle; outlines the high-level roles and responsibilities; and documents the key risk management framework components. The GRMF offers guidance on adopting prudent practices in risk management, emphasising the need for a well-developed risk culture, and explaining the notion of an integrated framework. The GRMF is future-oriented: it outlines the pathway for embedding risk and compliance management practice and enhancing maturity. The related policy and procedure focus on current activities and provide more detail on specific roles and responsibilities.

The GRMF is guided by ISO 31000:2018 Risk Management – Guidelines, ISO 37301:2023 Compliance management systems - Requirements with guidance for use, the Victorian Government Risk Management Framework, and for cross-industry better practice the Australian Prudential Regulatory Authority's Prudential Standard CPS 220 Risk Management. Necessary modifications have been made to ensure the GRMF fits Monash's size, activity mix and complexity.

## SCOPE

The Group Risk Management and Compliance Policy and related Procedures that give effect to the principles set out in the GRMF define the scope of coverage with respect to entities within the Monash Group. These entities should adopt the GRMF in principle, and any proposed significant deviation[4] from the GRMF should be approved by the Council Audit & Risk Committee (A&RC).

As with any management process, risk management has its limitations:

- risk management does not produce decisions, but rather informs decision-making processes; and
- it is impossible to predict all possible risks in detail. Therefore, risk management does not guarantee an absence of negative consequences.

[4] Any risk management framework that is directly contrary to the Monash GRMF's purpose and approach or is based on other standards.

# GOVERNANCE OF RISK AND COMPLIANCE

The management of risk and compliance at Monash reflects the institution's model of governance.

The **University Council** sits at the apex of that model. The *Monash University Act 2009* provides that the Council is responsible for "overseeing and monitoring the assessment and management of risk across the University, including university commercial activities." In particular, the Council:

- approves this Framework;
- oversees the implementation of this Framework (including matters of governance and resourcing);
- sets the Monash Group's risk appetite and approves the Group Risk Appetite Statement; and
- approves the Group Risk Profile.

The University Council has delegated to the **Council** Risk & Audit Committee (R&AC) various responsibilities in the oversight and monitoring of risk and compliance management. The R&AC's Terms of reference provide for the Committee to assist Council in discharging its governance and oversight responsibilities in relation to the University's financial reporting, internal control system, risk management framework, legislative and regulatory compliance, ethical matters and internal and external audit functions.

The **Vice-Chancellor** makes an attestation in the University's annual report that the University has risk management processes in place to manage its key risk exposures. Accordingly, the Vice-Chancellor is ultimately accountable for:

- having prudent risk and compliance management practices to manage risk and compliance obligations across the Monash Group; and
- the overall risk culture and maturity across the Monash Group.

The Vice-Chancellor is advised by a number of senior executive committees that play an important role in the management of risk and compliance:

- the Vice-Chancellor's Group (VCG), which reviews all risk and compliance reports and other documents that proceed to the A&RC or Council;
- the Vice-Chancellor's Executive Committee ("VCEC"), which focuses on matters of University strategy, policy and budget, including the capital development and information technology plans;
- the Vice-Chancellor's Global Campus Executive Committee ("GCEC"), which advises the Vice-Chancellor on strategic matters and strategically-relevant operational matters to maximise the effectiveness and efficiency of the Monash global network.; and
- the Senior Management Forum ("SMF"), which serves as a discussion forum in which to explore pertinent strategic or operational matters.

The Provost and the Deputy Vice-Chancellor (International) both play a central role in managing risk and compliance, being responsible for leadership of the 10 Monash Faculties and of the day to day operations of overseas campuses and presences (with the exception of Malaysia) respectively. The Pro Vice-Chancellor and President (Malaysia) reports directly to the Vice-Chancellor.

More generally, the senior managers of the Monash Group play key roles as risk owners, compliance owners, and legal compliance officers, as described below and in the Group Risk and Compliance Management Policy. The Group Risk Management Procedure and Group Compliance Management Procedure outline the role of those who support risk owners and compliance owners, as risk champions and compliance champions.

**Controlled entities** are accountable through the Vice-Chancellor to the University Council and R&AC.

Under Monash's Model Constitution for Wholly-owned Entities (WOEs), the University may require such an entity to establish its own audit and risk committee (an approach to be extended to all controlled entities). The Model Constitution provides for specific mechanisms to manage risks in WOEs in a way that is consistent with the Group-wide approach. If the University (as the sole shareholder or member) decides that a WOE should have its own risk and audit committee:

- the membership of the entity's committee must be nominated by the Chair of the Council R&AC;
- the entity must prepare an annual internal audit plan for approval by the Council R&AC;
- minutes of the meetings of the entity's committee must be submitted to the Council R&AC; and
- the University's Director of Internal Audit must be invited to attend meetings of the entity's committee as an observer.[5]

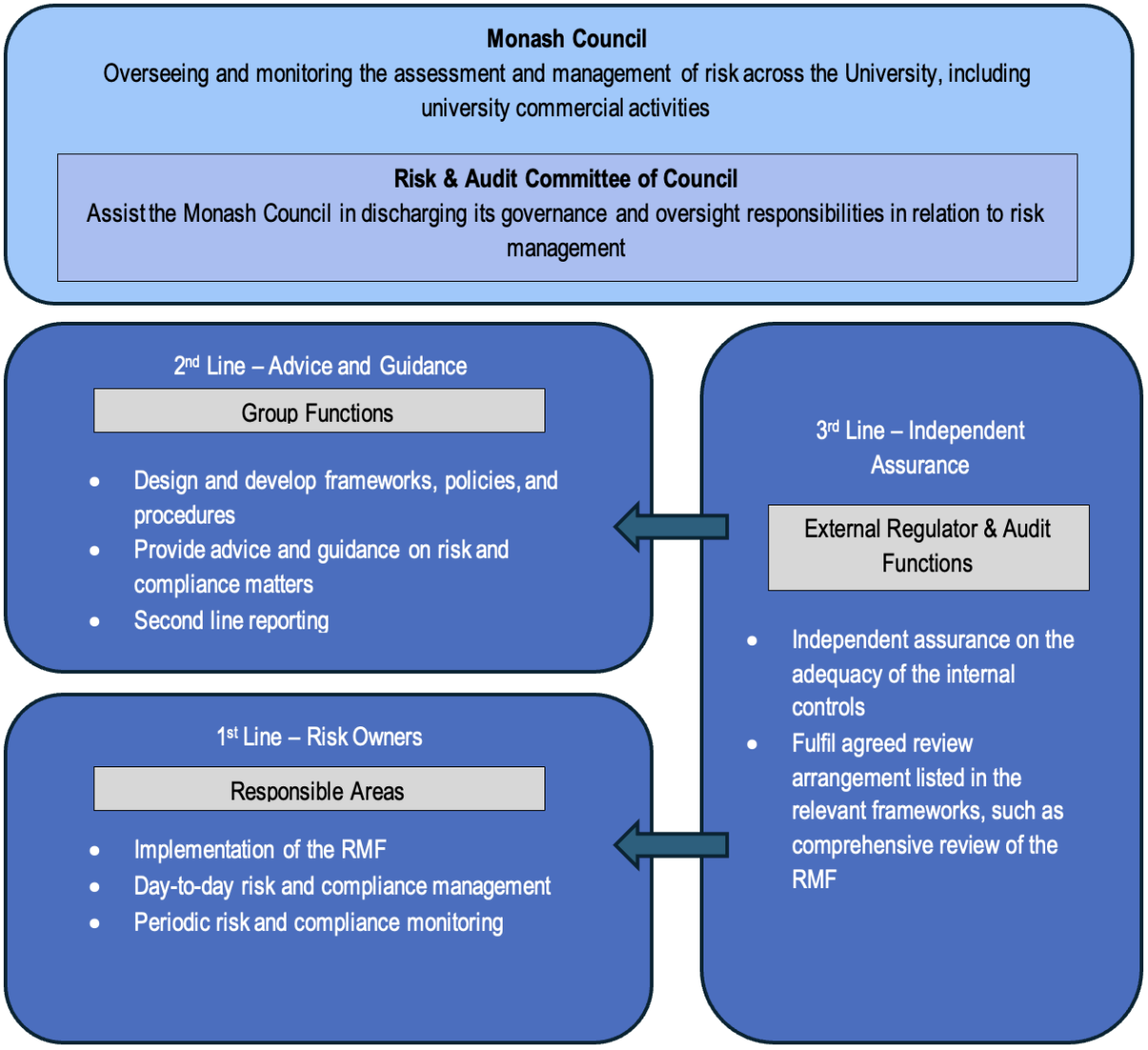
[5] Model Constitution, Clause 11.

Each audit and risk committee of a controlled entity assists the relevant board to discharge the board's responsibilities for the oversight of risk and compliance management. In addition, such committees provide relevant information to the 'Group' R&AC on a regular basis.

## THE THREE LINES MODEL

Monash's risk governance arrangements are intended to provide the University Council, Council standing committees, and senior management with the relevant information to oversee and manage the Monash Group's risks. The risk governance model depicted below shows the relationship between each of the three lines. This model enables risks to be reported and escalated in accordance with Monash's governance and accountability arrangements.

The Three Lines Model provides the structure for risk management and internal controls within an organisation by defining roles and responsibilities in different areas and the relationship between those different areas. Given the size, activity mix and complexity of Monash, the purpose of adopting and optimising the Three Lines Model is to embed risk management accountabilities and responsibilities across the whole of the Monash Group, without significant changes to Monash's current operating structure.




### First Line

The first line comprises all staff who are accountable and responsible for activities and processes within Monash to manage risk and compliance. Risk and compliance owners are responsible for activities and processes that arise from the day-to-day management of risk and compliance, including making decisions. The roles and responsibilities of risk and compliance owners, risk champions, Legal

Compliance Officers (LCOs) and compliance champions are defined in the Group Risk and Compliance Management Policy and its supporting procedures. Where appropriate, they are also incorporated into position descriptions. Further details on roles and responsibilities are detailed in the Group Risk and Compliance Policy.

A vital tenet of the Three Lines Model is that the first line is accountable and responsible for:

- Effective implementation of the GRMF, including adequate resourcing to enable consistent risk and compliance management practice;
- Ensuring decisions made are consistent with the Risk Appetite Statement; and
- The day-to-day management of risk and compliance which is consistent and integrated with the GRMF.

## Second Line

The second line at Monash comprises two key elements:

- **Risk and Compliance Unit (RCU):** The RCU is the second line function at the Group level and provides the overarching approach to managing risk across all risk categories, conducting oversight and challenge activities pertaining to the implementation and operation of the GRMF, thereby providing an holistic view of the risk landscape across the Monash Group. In implementing the GRMF, RCU seeks to identify better practices in particular responsible areas and communicate them across the Group.
- **Group Functions with Specialist Risk and Compliance Expertise:** These Group functions house dedicated risk and compliance professionals focused on specific risk categories, such as Occupational Health and Safety (OHS), Cyber Security, Finance and Human Resources. They provide oversight, and where necessary challenge, of risk and compliance assessment and reporting within their respective domains, using their expertise and close ties to operational activities. Such oversight and challenge roles are embedded within the remit of the relevant Group function, supported where appropriate by an approved third party.

It is acknowledged that some Group functions, like the Cyber Risk and Resilience team, hold both first-line (managing cyber risks within their own function) and second-line (overseeing cyber risks across the Group) responsibilities. This potential conflict is managed through clear position descriptions, policies and procedures that ensure effective segregation of duties and prevent conflicts of interest.

In general, the second line supports the Council, its committees and the Vice-Chancellor by:

- Designing and developing risk and compliance policies, procedures, processes, and information technology systems that support the First Line to manage their risks in line with the Group's overall approach and risk appetite;
- Objective review of, and advice on the consistent implementation of the risk and compliance management framework across the Monash Group, including the data and information captured;
- Providing professional advice and support, including training, to the Council, its Risk and Audit Committee (R&AC), management committees and the first line on risk and compliance related matters.
- Carrying out independent reviews to assess whether the First Line has controls in place to mitigate risks, and that they have tested that those controls are designed properly and are operating effectively.

The Executive Director, Governance, Risk and Policy, with support from the Risk and Compliance Unit (RCU) is accountable for a number of specific activities:

- Developing and maintaining the GRMF, Group Risk Appetite Statement (RAS) and the Group Risk Profile;
- Developing and maintaining risk and compliance policies, procedures and tools applicable to every kind of subject matter;
- Maintaining and reviewing the list of material compliance areas;
- Promoting awareness of risk and compliance through communications activity, including identifying and notifying relevant areas about forthcoming or potential regulatory changes in Australia;
- Providing oversight and where necessary challenge in reporting to management committees and R&AC. This role includes attending to:
    - the consistent and effective implementation of the GRMF across the Monash Group;
    - the data and information captured, the completeness and appropriateness of risk identification and assessment, the ongoing effectiveness of risk controls, and the execution of risk mitigation action plans;
    - the use of (or lack of) risk information in the decision-making process at both strategic and operational levels;

- emerging risk and compliance issues; and
- the level of risk accepted and its relationship to Monash's risk appetite, and any necessary escalation to senior management, management committees, controlled entity boards, Council committees or Council; and

- Providing independent advice, guidance, and training on risk and compliance management matters to the Vice-Chancellor, responsible area heads, and senior executive committees, and through the Vice-Chancellor to Council and the R&AC.

RCU is not responsible for day to day risk and compliance management activity across the Monash Group - that is the role of the First Line, to be carried out in accordance with the Group Risk and Compliance Policy and supporting procedures and more specific policies and procedures in specific categories of risk such as OH&S, Cyber Security, Finance and Human Resources.

## Third Line

The third line comprises the external regulator(s) and the Internal Audit function (undertaken by a combination of Monash staff and an external provider under a contractual co-sourcing arrangement). The role of the Internal Audit is to provide independent assurance to the University. Detailed responsibilities can be found in the Internal Audit Charter.

For further details on roles and responsibilities refer to the Group Risk and Compliance Management Policy and the associated Group Risk Management Procedure and Group Compliance Management Procedure in the Policy Bank.

# GROUP RISK MANAGEMENT FRAMEWORK (GRMF) COMPONENTS

The Victorian Government Risk Management Framework (VGRMF) defines a risk management framework as a "Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.[6]

Monash's GRMF is built on a clearly defined Risk Management Strategy (RMS) and the following foundational elements:

- The Council-approved Risk Appetite Statement (RAS);
- Documented Risk Profiles and Material Compliance Areas;
- Documented Risk and Compliance Controls;
- Dedicated Risk and Compliance Functions;
- Approved Policies, Procedures and Tools;
- Risk and Compliance reporting.

The integrated GRMF and its components are summarised graphically below:


# GROUP RISK MANAGEMENT STRATEGY (GRMS)

The design of Monash's GRMS acknowledges that Monash' strategy– *Impact 2030* – creates unique challenges and opportunities. A customised approach to risk management is required to ensure that methods, mitigation strategies, and reporting mechanisms are tailored to Monash's purpose, goals and values. The GRMS must also take account of other dimensions of Monash's organisational context, including structures, policies, systems, processes, and organisational culture. All of these dimensions of organisational context are reflected in internal and external relationships and the associated interdependencies.

[6] https://www.dtf.vic.gov.au/sites/default/files/document/Victorian%20Government%20Risk%20Management%20Framework%20-%20August%202020.pdf

Operationally, to embed a culture of risk management, the GRMS must be integrated into other elements of organisational governance and management beyond the GRMF and the associated policy, procedures, systems and processes. This integration extends beyond policies to governance and management of major programs/projects, delegations of authority, and even role descriptions. By weaving risk considerations into everyday decision-making, Monash can identify and manage potential risks early, preventing them from escalating. Further, aligning risk management with performance management through position descriptions, reporting, and evaluation activities allows Monash to track the effectiveness of mitigation strategies and continuously adapt its approach to the evolving external and internal context. This closed-loop system fosters accountability and ensures risk management remains a dynamic and responsive process, supporting Monash's pursuit of its strategy.

Monash's GRMS takes an evidence-based approach to managing risk and compliance matters. This means that day-to-day management activities are integrated with the best available risk management information, and risk management activities are designed to produce demonstrable evidence, where risk management information will be collected and shared, key decisions will be documented, and data custodianship will be allocated. Additionally, processes and information technology systems will be established and implemented to support such activities and further integrate risk and compliance management into daily operations and performance management.

The GRMS utilises risk profiles that directly correlate with, and therefore underpin the management of risk and compliance in pursuing, the goals outlined in *Impact 2030* and the supporting plans (including portfolio, faculty and entity plans). Risk profiling is a systematic process of identifying, assessing, and managing risks associated with a plan, project or activity. The risk profile informs the development of risk management actions such as mitigating, avoiding or accepting those risks. Regular monitoring and review are necessary to ensure that the risks and risk management strategies remain relevant and effective over time.

Group-wide risk management should be an integral component of the University's strategic planning process, utilising the Group and operational risk profiles. This approach ensures that potential threats and opportunities - both external and internal - are identified, evaluated, and managed proactively in line with the University's strategic goals and its risk appetite. By integrating risk profiling into strategic planning, the University not only anticipates potential challenges but also capitalises on opportunities, ensuring the resilience and sustainability of its endeavours. This alignment means that the University's strategic goals are pursued with a comprehensive understanding of the risks involved, thereby optimising decision-making, resource allocation, and stakeholder confidence.

At the local level, the integration of the risk profile approach is fundamental to informed decision-making in planning and resource allocation. Through integrating this approach into daily management practices, the University does not merely react to risks (including risks of non-compliance); rather it ensures that risks are actively identified, evaluated, and managed in alignment with the University's goals and its risk appetite. This approach enables decision-makers to strike a balance between potential threats and opportunities, driving both innovation and efficiency; it also offers the prospect of solving multiple problems at once; and of course where necessary it allows an investment case for risk reduction to be made. As a result, the risk profile approach empowers decision-makers with the foresight and agility to navigate uncertainties, ensuring that actions taken are not only effective but also aligned with the broader vision of the University.

Of course, the use of a risk profile in decision-making is only beneficial if the decision-maker strives to bring as much objectivity as possible to the decision at hand. Material biases, whether due to a conflict of interest or otherwise, will distort decision-making. Monash's Integrity and Respect Policy and the associated Conflict of Interest Procedure prescribe principles and processes that seek to avoid such biases. Adherence to them is of great importance in risk-based decision-making.

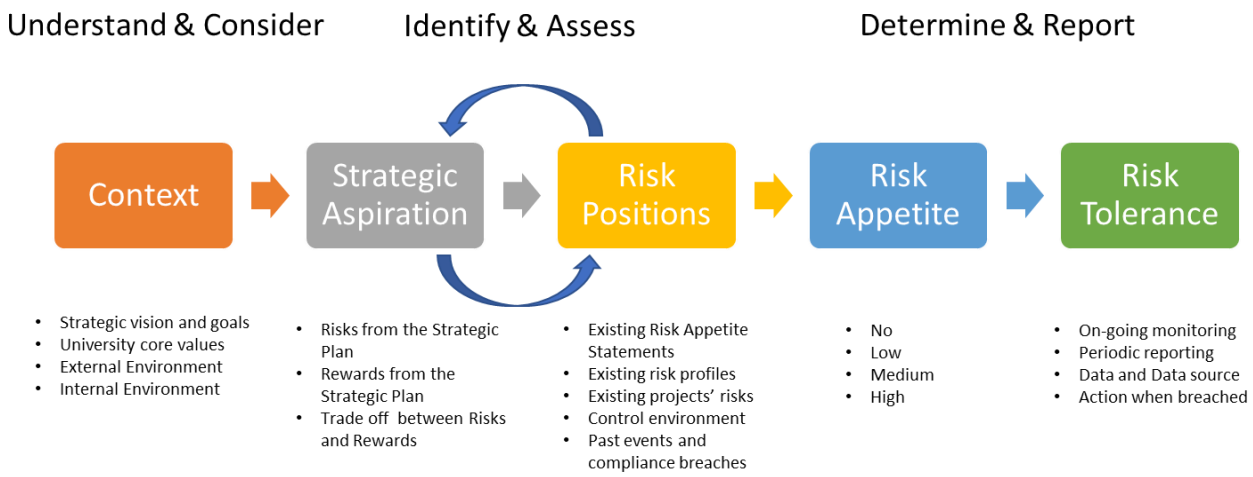
## 1. Risk Appetite Statement

Monash's Group Risk Appetite Statement (RAS) is used to communicate the Council's expectations of the degree of risk that Monash is willing to accept, in pursuit of its strategic and operational objectives (risk appetite). In operation, the RAS serves a dual purpose. For the Council, it acts as a critical oversight tool, providing clear guidelines to ensure alignment with strategic goals. For the broader Monash community, it translates into actionable directions, informing decision-making at all levels by outlining the parameters of acceptable risk, and fostering a culture of risk awareness.

Below are the key features of Monash's approach to the RAS:

- The Council is responsible for setting Monash's risk appetite and approving the RAS. This approval demonstrates the Council's fulfilment of its oversight duties and sets a clear commitment to risk management. With a Council-approved statement, the entire Monash Group has a transparent and consistent approach to risk-based decision-making, contributing to a culture of risk awareness throughout the group.

- The RAS presents for each risk type, the maximum level of risk that Monash is willing to operate within, as far as possible expressed as a risk tolerance (Averse, Cautious, Balanced, or Open), based on its risk appetite, Group and operational risk profiles, and control environments. In other words, the RAS defines how much risk Monash is willing to take, and the RAS translates that tolerance into practical boundaries for every strategic and operational activity across the Monash Group.
- The RAS is augmented where possible by quantitative and qualitative Key Risk Indicators (KRIs), that are monitored and reported on to assess compliance with the RAS.
- The RAS is reviewed annually in a process co-ordinated by RCU and the Executive Director, Governance, Risk and Policy;
- The RAS is a key artefact in strategic planning - and as the Group strategy develops, the RAS needs to be reassessed. This bi-directional relationship ensures that the RAS remains aligned with the evolving strategic direction, and that the strategy and its implementation are informed by the latest risk and assurance insights.
    - The RAS sets the risk tolerance, and this tolerance level influences the objectives pursued and the level of risk considered acceptable to achieve those goals;
    - Conversely, as the strategy and its implementation evolve, the envisioned future state can influence the RAS. New strategic directions might expose Monash to a different degree or different type of risk, prompting a reassessment of the RAS and its risk tolerance.
- Although the RAS development and review process is often presented as sequential, in practice, it is more iterative, as depicted in the figure below. This interdependence between the RAS and strategic planning is crucial for effective risk management and assists Monash in understanding the tradeoff between risk and reward.




## 2. Risk Profile and Material Compliance Areas

**Risk Profile**

Monash maintains a Group Risk Profile that captures the most significant Group risks, with reference to Monash's strategic plan, supporting plans and the Group RAS. The impact of risks on Monash's strategic goals is reviewed in establishing the Group Risk Profile, and assessed by the senior executives (direct reports to the President and Vice-Chancellor) who individually or jointly own each Group risk. Actions are developed as necessary to achieve the desired balance between the delivery of strategic priorities and appropriate risk mitigation.

To support the day-to-day management of the Group Risk Profile, an Operational Risk Profile - a subset of the Group Risk Profile - will be captured at the responsible area level (faculty, controlled entity or central function). Subsequently, the ownership of each risk should be assigned to an appropriate individual with consideration of the impacts of each risk, as well as the ability of each risk owner to take the necessary steps to effectively manage the risks. This management includes not only the direct allocation of resources but also the exercise of influence through collaboration to complete the required activities.

The Group Risk Profile and the Operational Risk Profile are linked through a common risk taxonomy. This standardised classification mechanism allows for a consistent approach to risk identification and assessment, and facilitates the "top-down" and the "bottom-up" understanding of how operational risks interact with and potentially influence the broader Group risks. A common taxonomy allows the integration of the Group and operational risk profiles, providing a holistic view of Monash's risk landscape.

Both the Group Risk Profile and the Operational Risk Profile, are recorded in the designated risk register. They are monitored and assessed on an ongoing basis and updated as necessary to reflect any significant change driven by either internal or external factors. A formal reassessment of all Risk Profiles by risk owners should be undertaken at least annually and otherwise where circumstances have changed significantly.

Furthermore, the risks identified in the Group Risk Profile and the Operational Risk Profile are assessed and managed in accordance with the risk management process (lifecycle), as depicted in the diagram below. For more details about the risk management process (lifecycle), please refer to the Group Risk and Compliance Policy and the Group Risk Management Procedure.

**Diagram 1 - RISK MANAGEMENT PROCESS (Lifecycle)**


*Source: ISO 31000, Risk management – Guidelines, https://www.iso.org/iso-31000-risk-management.html*

Risk owners predominantly sit in the **First Line** and typically have the following responsibilities:

- Understand the operating context and strategic objectives;
- Identify the risks that could prevent the achievement of the strategic objectives;
- Review the RAS as it relates to the strategic objectives and associated risks;
- Consider the causes and consequences of the identified risks and assess Current and Target risk ratings;
- Determine what actions (if any) are needed to shift the Current risk rating to the Target risk rating;
- Understand regulatory and operating impacts on specific processes related to the relevant risks;
- Understand the linkage between operational risks and Group risks;
- Form a view on the elements that exist to manage the risks - the existing controls (including policies and processes) and additional mitigation actions (with treatment plans) that are in progress or need to be taken;
- Ensure that there is adequate monitoring and reporting in place on the effectiveness of these elements;
- Work with the relevant stakeholders to complete mitigation actions;
- Conduct periodic review and re-assessment of the risks;
- Ensure the applicable risks are accurately recorded and maintained in the risk register;

- If appropriate, nominate Risk Champions (RCs) and Legal and Compliance Officers (LCOs) to undertake administrative activities (other than attestation) on their behalf. Where such nomination occurs, the relevant activities must be reflected in the position description of the role held by the nominees.

**Compliance Management Program**

The University is subject to a wide range of regulatory compliance obligations under applicable laws, regulations, standards, and codes of practice. In addition, the University must uphold its contractual obligations and maintain adherence to its own policies.

All University staff are responsible for compliance with relevant regulatory and contractual obligations, and adhering to relevant policies.

The effective implementation of a compliance management program requires the allocation of sufficient resources to compliance owners and LCOs, with appropriate managerial support.

**Material Compliance Areas**

Regulatory compliance risk is the risk of legal or regulatory sanctions, material financial loss, or loss of reputation that Monash might suffer if it failed to comply with a regulatory compliance obligation.

The following six (6) material compliance areas have been identified as being key areas of regulatory compliance risk for the Monash Group:

1. Educational Integrity and Quality;
2. Research Integrity and Quality;
3. Institutional Integrity;
4. Safeguarding People;
5. Information Security; and
6. Financial Integrity and Standing.

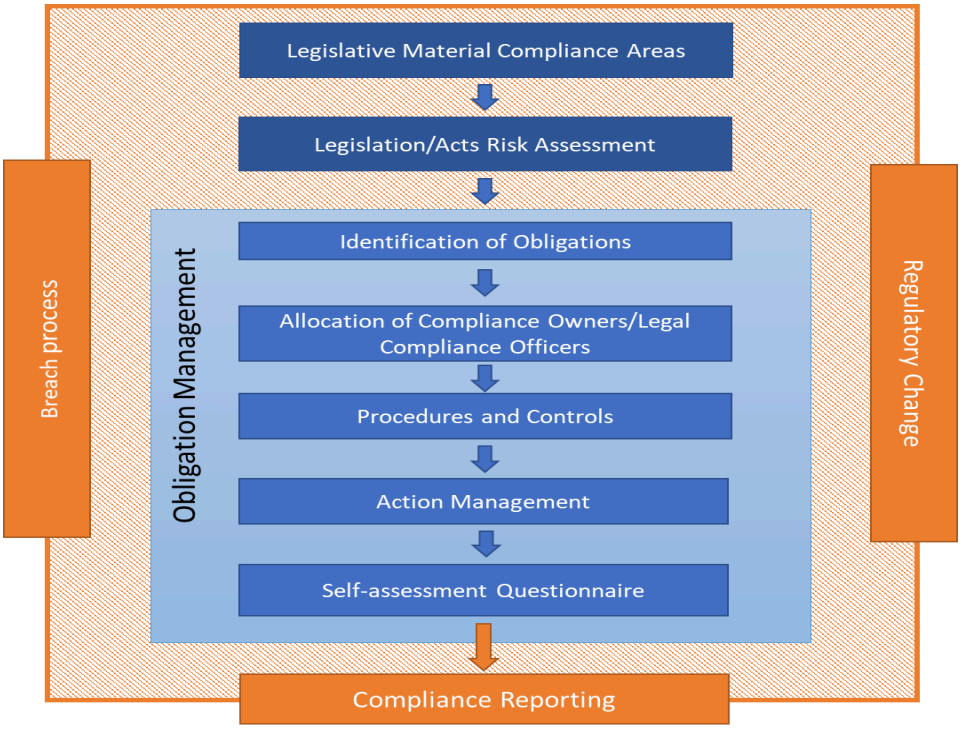
These areas present the greatest exposure for the University in accordance with the RAS and the Group Risk Profile. The majority of these compliance areas are in keeping with the Tertiary Education Quality and Standards Agency's focus on areas that it considers to pose the greatest risks to students and the integrity, quality, and reputation of the higher education sector.

Given the greater risk exposure within these areas, a stronger focus and resourcing model should be implemented to ensure the identified material compliance areas are assessed regularly, allowing for active monitoring and identification of issues. These material compliance areas and the key acts, regulations and codes within them have been identified to guide the setting of priorities for Monash's compliance management work according to the degree of regulatory compliance risk.

Material compliance areas are recorded, monitored and assessed on an ongoing basis. Any significant change due to either internal and/or external factors should also be reflected. A formal reassessment of the material compliance areas should be undertaken at least annually by the senior executive with the assistance of the RCU.

Furthermore, the obligations identified under each of the material compliance areas are managed in accordance with the compliance management process (lifecycle), as depicted in the diagram below. For more details about the compliance management process (lifecycle), please refer to the Group Risk and Compliance Policy and the Group Compliance Management Procedure.

**Diagram 2 - COMPLIANCE PROCESS (Lifecycle)**




*Source: Risk and Compliance Unit, https://www.intranet.monash/risk-compliance*

## 3. Risk and Compliance Controls

Risk and compliance controls ('controls') are designed and implemented to manage and mitigate risks, and reasonably assure the achievement of the strategic objectives. Controls are directed to the key causes of a risk and are intended to satisfy compliance obligations.

Controls are communicated to and understood by relevant staff. The sufficiency and effectiveness of control design and operation should be assessed annually to ensure that those controls continue to be adequate and effective in mitigating risk and achieving strategic objectives and performance targets, and satisfying compliance obligations. Weaknesses in the adequacy or effectiveness of controls, along with related mitigation actions, should be recorded, allocated, and tracked through to completion by utilising the control register.

Control Owners predominantly sit in the First Line and typically have the following responsibilities:

- Understand the end-to-end process used to manage or make decisions;
- Consider the 'control input and output dependencies' within the owned process;
- Identify regulatory and/or University (contractual or policy) compliance requirements within the process;
- Design and implement the requisite controls to mitigate the risks adequately (including compliance risks);
- Establish and maintain a controls self-assessment program to test the sufficiency and effectiveness of existing controls and identify any control deficiencies (whether caused by design or ineffective implementation);
- Where control deficiencies have been identified, ensure action plan(s) are developed to address the deficiencies;
- Ensure progress in implementing the action plans is reported regularly, and the plans are completed on time to remedy any identified deficiencies;
- Ensure controls are up to date with changes to compliance requirements; and
- Record and maintain information about controls in the control register.

## 4. Risk and Compliance Functions

RCU is the University's designated central/group advisory function for risk and compliance management. RCU sits in the Second Line and has the following responsibilities:

- Assist the R&AC and Council to develop and maintain the GRMF;
- Design and maintain the Monash Group risk and compliance management policy and procedures;
- Design and maintain the risk and compliance tools and information system;
- Provide independent and objective review and advice, oversight, and monitoring in relation to the implementation and operation of the GRMF and its constituent elements; and
- Provide analysis and reports on the adequacy and effectiveness of risk management (including internal controls) to senior executives, R&AC and Council to assist them to fulfil their respective roles in relation to risk and compliance management.

In order for the RCU to fulfil its responsibilities effectively and efficiently, it needs to:

- Be operationally independent of First Line and Third Line functions;
- Be adequately staffed by appropriately trained and competent persons who have sufficient authority to perform their role effectively;
- Have access to the Vice-Chancellor through the Executive Director, Governance, Risk and Policy; and
- Have the necessary authority to obtain information relevant to risk and compliance from people and systems across the Monash Group.

Group Functions with Specialist Risk and Compliance Expertise (Second Line)

As noted above, the Monash Group maintains specialist risk and compliance expertise within the group functions for some specific risks of major significance, such as OHS, cyber security, and research ethics and integrity. These Group functions provide targeted second line oversight for their respective risk and compliance domains, such as topic-specific training, advice, and challenge where necessary. In addition, these areas perform the role of first line risk owners for their own respective functions. Due to the nature of such dual responsibilities, these Group functions should ensure effective segregation of duties and prevent conflicts of interest, by establishing clear position descriptions, business rules, and processes. Detailed information on these specialist risk and compliance areas is provided on their respective websites and in the policies that they administer.

## 5. Policies, Procedures and Tools

RCU, as the central risk and compliance advisory function, designs and maintains the Group risk and compliance management policy and procedures. These documents have a number of functions: to support the annual risk and compliance attestation required in Monash's annual report; to provide the Monash Group with clear direction on appropriate approaches to risk management; and to seek to ensure compliance with internal processes and controls, as well as with external regulatory requirements. Specific risk and compliance policies and procedures are owned and managed by relevant specialised areas, but the general approach to risk and compliance should adhere to the principles established in the GRMF. The Risk and Compliance Management Processes are outlined in Diagram 1 and 2 lifecycle outlined below.

The Group Risk and Compliance Management Policy and procedures are designed to describe:

- The process for identifying and assessing risks and compliance obligations;
- The process for establishing, implementing and testing mitigation strategies and control mechanisms for risks (including compliance risks);
- The process for communicating, monitoring, and reporting risks, including escalation procedures for the reporting of material events and compliance breaches;
- The mechanisms for monitoring and seeking to ensure ongoing compliance with regulatory and self-subscribed obligations;
- The process for pursuing consistency in risk management practice across the Monash Group;
- Consequence management processes for non-compliance with the approved Group risk management policy and procedures;
- The process for review of the GRMF;
- The requirements for maintaining the Group risk management policy and procedures, and their integration with Monash's Policy Framework and related policies and procedures; and
- Support and general risk management guidance on other Monash frameworks, policies and procedures developed and maintained by specialised areas to manage specific types of risk and compliance obligations.

These documents are also supported by designated tools, including:

- Risk Assessment Guidance and Definitions - refer Appendix 2. This tool includes a risk taxonomy and risk assessment tables for likelihood, impact and combined risk heat map to aid the risk management process (Risk Assessment Guidance and Definitions);
- A dedicated risk and compliance information system, which serves as the central repository for the capture and storage of risk data and metrics, including risk profiles, compliance obligations, metrics and controls; and
- Other systems developed and/or maintained by specialised areas, such as SARAH (for OHS incident reporting), Policy DMS (for the Monash Policy Bank) and PURE (for research contracts).

### 6. Risk and Compliance Reporting

Risk and compliance management practices are monitored and the results reported to senior management and governance bodies to assist Monash to accomplish its strategic goals. Executive management committees, Council committees and Council receive periodic reporting on Group Risks linked to the progress of strategic and operational plans, and major initiatives. The information in such reports is maintained by the Group Risk Owners.

Regular, accurate and timely information concerning the University's risk profiles, adherence to the RAS, and material compliance areas depends on a robust data framework that enables the collation of data on risk measures across responsible areas. The quality of such data should be regularly assessed to ensure its adequacy for timely and accurate measurement, assessment and reporting on all risks across the University. It should provide a sound basis for making decisions and ongoing visibility of actions undertaken to manage risks identified.

Reports should be timely, clear and available to relevant stakeholders across University management committees; and in accordance with the Group Governance Framework (GGF). The GGF outlines the corporate governance reporting requirements for all incorporated entities and certain unincorporated structures within the Monash Group.

## CONTINUOUS IMPROVEMENT AND EVALUATION OF THE RISK MANAGEMENT FRAMEWORK

The Council, through the R&AC, evaluates the effectiveness of the GRMF in identifying and managing risks. Monash's GRMF and its components are periodically reviewed, with the results reported to the R&AC.

During the initial implementation of the Framework, RCU will undertake an annual review of progress in consultation with relevant management committees. The findings will be reported to R&AC and used to inform the rolling implementation plan. Together with relevant changes to the external and internal context, they will also inform any desirable changes to the Framework and relevant policies and procedures, to improve their suitability, adequacy and effectiveness, including modifications driven by existing practice needs.

The Group Risk and Compliance Management Policy and supporting procedures are reviewed every three years, in accordance with the normal review cycle for Monash policies and procedures.

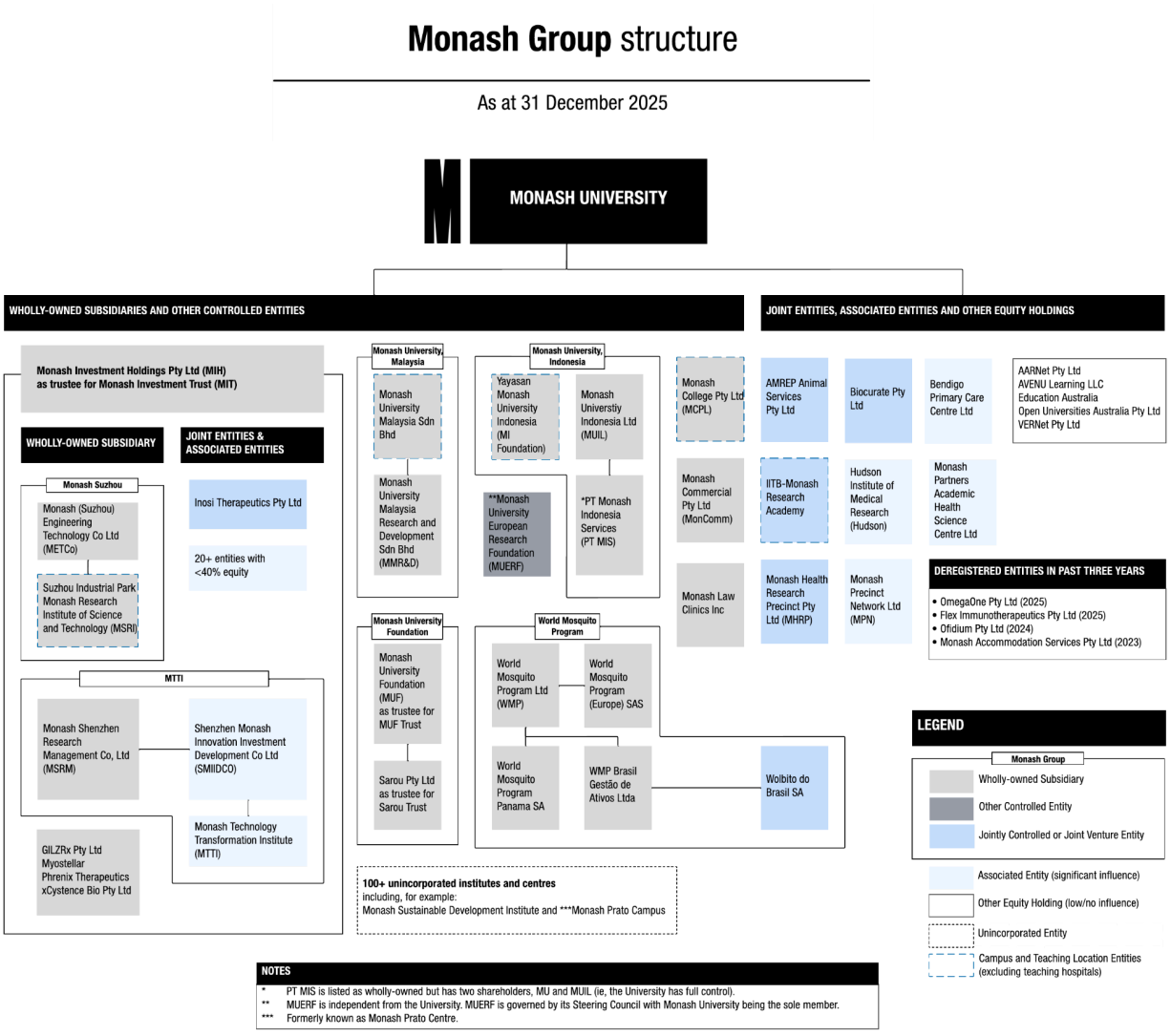
A comprehensive review by operationally independent, appropriately trained and competent persons (this may include external consultants) should be undertaken at least every five years.

A comprehensive review of the GRMF assesses whether:

- The Framework is implemented and effective;
- It remains appropriate for Monash, considering its current strategic plan;
- It remains consistent with the Council's risk appetite;
- It is supported by adequate resources; and
- It is accurately documented.

# APPENDIX 1 - THE MONASH GROUP

Note: refer to Group Risk and Compliance Policy for risk reporting scope



# APPENDIX 2 - RISK ASSESSMENT GUIDANCE AND DEFINITIONS

Monash's Risk Assessment Guidance and Definitions provides the risk assessment tables for likelihood and impact. The fundamental combined risk matrix is as depicted in below.

## RISK MATRIX

A Risk Matrix matches specific Likelihood Ratings and Impact Ratings to a Risk Rating of Low, Medium, High or Extreme.

| LIKELIHOOD | IMPACT | | | | |
|---|---|---|---|---|---|
| | Insignificant | Minor | Moderate | Major | Catastrophic |
| Almost Certain | Medium | High | High | Extreme | Extreme |
| Likely | Low | Medium | High | High | Extreme |
| Possible | Low | Medium | Medium | High | High |
| Unlikely | Low | Low | Medium | Medium | High |
| Rare | Low | Low | Low | Medium | Medium |

*Table 1: Risk matrix*

Likelihood is assessed by reference to different periods of time (e.g. probability within one year, or more than one year, or within the life of the project or the planning period).

Impact is assessed by reference to the following categories:

- Financial
- Human Resources
- ICT
- Service Delivery
- Research
- Teaching and Learning
- Student Experience
- Regulatory Compliance and Legal
- Health, Safety and Environment
- Brand and Reputation

MONASH University

## DEFINITIONS

| | |
|---|---|
| Three Lines Model | An approach to providing structure around risk management and internal controls within an organisation by defining roles and responsibilities in different areas and the relationship between those different areas. |
| Control | Any process, policy, device, practice or other actions that modify the likelihood and/or consequence of a risk. The establishment of controls within processes provides protection, and their effectiveness strengthens the ability to manage and mitigate the associated risks and compliance obligations. |
| Controls Assessment Program | A program may include a rotational mix of control effectiveness testing via first-line self-assessments, internal audit control testing procedures, and pressure testing on a recurring basis. |
| Control Effectiveness | Control effectiveness testing involves regular reviews of controls to ensure they are designed and operating effectively to minimise the risks they are intended to mitigate. |
| Control Owner | Individuals who have the accountability and authority to manage controls. Typically, the control owner is a first line role. |
| Compliance Owner | Compliance owners are responsible for ensuring there are effective internal controls in place to monitor regulatory compliance within their business or functional area. |
| Current Risk | The level of risk after considering the current controls and controls' effectiveness at the time of assessment. |
| Key Risk Indicator (KRI) | Key Risk Indicators (KRI's) are metrics used to measure performance against the defined risk appetite and risk tolerance. They provide a way to quantify and monitor each risk. Effective KRIs help in proactive risk management by providing an early signal of increasing risk exposures. |
| Legal Compliance Officer (LCO) | A Monash staff member with local expertise and knowledge of a particular area of the University's operations who consults with the Risk and Compliance Unit to identify and maintain the University's regulatory obligations relevant to the activities of their work area. |
| Monash Group | Monash University and all its subsidiaries listed below:<br>● Monash Accommodation Services Pty Ltd<br>● Monash College Pty Ltd<br>● Monash Investment Trust<br>● Monash University Foundation Trust<br>● Monash (Suzhou) Engineering Technology Co Ltd<br>● Suzhou Industrial Park Monash Research Institute of Science and Technology<br>● Monash University Indonesia Ltd<br>● Monash University Malaysia Sdn. Bhd<br>● World Mosquito Program Ltd<br>● PT Monash Indonesia Services<br>● Yayasan Monash University Indonesia |
| Responsible area | For the purpose of this framework, each of the below-listed areas is referred to as a 'responsible area' (unless indicated otherwise): Monash University Australia (each faculty & each central function), Monash University Malaysia, Monash University Indonesia, Monash Suzhou, Monash University Prato Centre, Monash College Pty Ltd, World Mosquito Program. |
| Risk | Effect of uncertainty on objectives. |

| | |
|---|---|
| Risk appetite | The types and amounts of risk that an organisation is willing to accept in the pursuit of its strategic and business objectives. |
| Risk culture | Risk culture refers to the system of beliefs, values and behaviours throughout an organisation that shapes the collective approach to managing risk and making decisions. A positive risk culture is one where every person in the organisation believes that thinking about and managing risk is part of their job. |
| Risk management | Coordinated activities to direct and control an organisation with regard to risk. |
| Risk management framework | Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. |
| Risk management process | Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk. |
| Risk Owner | Individuals who have the accountability and authority to manage risk. Typically, risk owner is a first line role. |
| Risk profile | A description of any set of risks. The set of risks can contain those that relate to the whole organisation (or Group) or part of the organisation. The risks are typically presented as a list or on a heat map. |
| Risk register | Record of information about identified risks. |
| Risk tolerance | Risk Tolerance represents the practical application of Risk Appetite (refer definition above).<br><br>Risk Appetite involves qualitative statements. Risk Tolerance operationalises these statements using quantitative measures (where possible) that set boundaries and thresholds of acceptable risk taking. Risk Tolerance enables more effective monitoring and review and informs actions to be taken (for eg. escalation) when tolerance thresholds are approaching, or are reached. |
| Target Risk | The level of risk after considering the expected effect of agreed actions that have not yet been implemented. |

MONASH University

## GOVERNANCE

| | |
|---|---|
| Supporting policy | Group Risk and Compliance Management Policy |
| Supporting document | Group Risk Management Procedure<br>Group Compliance Procedure<br>Group Governance Framework |
| Related legislation & Standards | Tertiary Education Quality and Standards Agency (TEQSA) Act 2011 (Cth)<br>Higher Education Standards Framework (Threshold Standards) 2021 (Cth)<br>Monash University Act 2009 (Vic)<br>Non-Obligatory:<br>Financial Management Act 1994 (Vic)<br>Standing Directions 2018 Under the Financial Management Act 1994 (Vic)<br>ISO 31000:2018 Risk Management – Guidelines<br>ISO 37301:2021 Compliance Management Systems standard - Requirements with guidance for use<br>APRA Prudential Standard CPS 220 Risk Management |
| Category | Risk and Compliance |
| Approval | Monash University Council (19 June 2024) |
| Endorsement | Audit & Risk Committee (31 May 2024)<br>VCG (22 May 2024) |
| Document owner | Executive Director, Governance, Risk and Policy |
| Date effective | 1 July 2024 |
| Review date | 1 July 2027 |
| Version | V1.0 FINAL |
| Content enquiries | riskandcompliance@monash.edu |

MONASH
University