

---

# Risk Management Framework Policy

Version number	6
Approved by	Corporate Governance Board
Date of approval	31 October 2023

## Purpose

Sydney Institute of Higher Education (SIHE) recognises that effective risk management is critical to rigorous governance, improving decision making and enhancing outcomes and accountability. By management processes, SIHE will have insight and transparency over operational functions, change/growth, disruptive, and emerging risks across higher education.

SIHE recognises that risk and uncertainty can never be entirely eliminated, however, effective risk management processes can work to mitigate the negative effects of any risks that may occur. SIHE must ensure that risk management processes are integrated throughout its governance structures and planning and review procedures and are consistently applied.

## Scope

The *Risk Management Framework Policy outlined in this document* applies to all SIHE current and planned operations, and all individuals involved, whether they are SIHE staff, students, or visitors.

This document provides the structure and tools that will facilitate the use of a consistent risk management process, whenever decisions are being made in SIHE. The principles and procedures of this document must be applied consistently across all projects, operations, processes, and activities at all levels of SIHE to ensure resources to treat risks are applied efficiently and effectively.

The *Corporate Governance Board* is ultimately accountable for the decisions made in SIHE and therefore they need to have confidence that the important issues are being managed and that SIHE will achieve its objectives. The Board receive information on SIHE's management of risk through reporting provided from the *Audit and Risk Committee*.

Standards 6.2 and 6.3 of the *Higher Education Standards Framework (Threshold Standards) 2021* stipulate that governing bodies identify material risks and managed and mitigate risks effectively and maintain oversight of academic and research integrity, including monitoring of potential risks.

## Objectives

The *Risk Management Framework Policy* provides the foundations and organisational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout

---

SIHE.

- Risk Management processes and guidelines will be embedded into SIHE strategic objectives to enable SIHE to take a proactive approach to risk that is crucial to the continuity of SIHE's operations.
- All risks at SIHE will be identified and managed and all staff will be aware of risk management processes relevant to their roles.
- All risk assessments will be conducted in a transparent manner in order to facilitate open lines of communication at SIHE.
- A risk assessment will be completed for all strategic and operational decisions where there is any area of uncertainty to enable:
  - better identification of opportunities and threats.
  - more effective allocation and use of resources.
  - improved stakeholder confidence and trust.
  - a clear understanding by all staff of their roles, responsibilities, and authorities for managing risk, which encourages a high standard of accountability.
  - improved compliance with relevant legislation.
  - better corporate governance; and
  - the development of a more risk aware organisational culture through enhanced communication and reporting of risk.

## Responsibilities

Throughout SIHE, key roles and governance forums have responsibilities for actioning the requirements of the Risk Management process.

### ***Corporate Governance Board***

The *Corporate Governance Board* is responsible for the regular monitoring of risks and uncertainties with regards to SIHE overall operations.

Risk management will be on the agenda of all the *Corporate Governance Board's* meetings, during which the *Corporate Governance Board* will:

- Review all risk management processes, including all monitoring and mitigation strategies
- Delegate appropriate risk management responsibilities
- Review all delegated risk management responsibilities
- Review any instances where a risk eventuated, was identified or mitigated in the preceding period.

The *Corporate Governance Board* will assess SIHE monitoring/mitigation processes with regard to each specific risk and identify corrective actions needed to address the underlying causes of known risks.

### ***Audit and Risk Committee***

The *Corporate Governance Board* delegates responsibility for monitoring and advising the Board on risk management to the *Audit and Risk Committee*.

The *Audit and Risk Committee* must:

- Provide advice on and oversee the implementation of the *SIHE Business Continuity Plan*
- Identify, establish mitigation strategies for, and monitor risks
- Develop and maintain a detailed Risk Register that provides a comprehensive record of risks to SIHE's operation, outlines risk characteristics, outline each risk's rating and management strategies for each risk, and outline recovery strategies for the eventuality that the risk occurs.
- Ensure that staff are trained in critical incident management procedures and day-to-day risk management responsibilities
- Provide regular reports and advice to the *Corporate Governance Board* about a broad range of risks at SIHE, particularly risks of non-compliance with the Threshold Standards 2021
- Respond as necessary to requests from the *Corporate Governance Board* for advice, policy amendment, or other work as needed.
- Must conduct an internal audit once per year of the *Risk Register* and *SIHE Risk Management Framework Policy*.
  - The audit will:
    - examine the effectiveness of the SIHE risk management processes.
    - ensure all risks and their effects are effectively categorised and managed.
    - identify any new or prospective risks The findings of the audit will be communicated to the *Corporate Governance Board*, who will take appropriate action based upon its findings.

### ***Academic Board***

The *Academic Board* is responsible for risk management in relation to academic quality and integrity.

The *Academic Board* will take preventative action to mitigate against the following academic misconduct risks:

- Misrepresentation
- Fabrication
- Cheating
- Plagiarism
- Misuse of intellectual property For more information refer to the *SIHE Academic Integrity and Conduct Policy*.

The *Academic Board* will undertake extensive program reviews on a five-yearly basis, which will include risks posed to the quality of the program.

This information will be used to inform risk management processes as they relate to academic matters. For more information regarding program reviews refer to the *SIHE Program Review and Continual Improvement Policy*.

### ***SIHE Staff***

All *SIHE staff* have a responsibility to mitigate risks that may eventuate during their employment to the best of their ability.

All staff should report any risks or prospective risks to the *Audit and Risk Committee* upon discovery. If a

risk is deemed a critical incident, then the procedures outlined in the *Critical Incident Response Policy* should be followed.

## Framework

The Risk Management Framework will seek to enable effective risk management by:

- 1) providing tools that are integrated into business processes
- 2) creating the foundations required to build capability across the organisation to identify, assess and manage risks
- 3) creating and maintaining a risk-aware culture by adopting the risk appetite into all strategic decision-making processes
- 4) providing consistent structure for a common platform for risk management which includes the process for identifying, assessing, mitigating and reporting on risks
- 5) enabling the continual improvement and maturity of risk management performance using available data and metrics.

The Risk Management Framework at SIHE categorises risks into five categories:

- Strategic
- Corporate
- Higher Education
- Operational
- Finance

### Strategic Risks

Strategic Risks are those risks that can impact the achievement of SIHE's business objectives and

Risk Management Framework Plans, procedures and guidelines strategies, thus failing to demonstrate value for money to shareholders.

The *Audit and Risk Committee* will complete a Strategic Risk assessment annually and report to the *Corporate Governance Board* to assist with planning and monitoring the business.

Strategic risks may include:

- Business continuity
- Competition
- Student enrolment
- Poor management
- Planning
- ad-hoc or activity based

### Corporate Risks

Corporate Risks are those risks that are caused by non-compliance with legislative, regulatory and policy or procedural requirements, including the Threshold Standards. The *Academic Quality Committee* will

---

complete an academic risk assessment annually and report to the *Academic Board* to assist with planning and monitoring the quality of educational practices as SHIE. The *Academic Quality Committee* will monitor the academic risks throughout the year.

Corporate Risks may include:

- Stakeholder management
- Council approval
- Industrial action
- Privacy
- Intellectual property

### Higher Education Risks

Higher Education Risks are those risks that occur as part of SIHE undertaking its business and often feed into a Key Risk. These might include risks associated with the achievement of business objectives. There are a number of specific functional risk assessments undertaken, including:

- Loss of TEQSA approvals
- Systems failure
- Student complaints
- Loss of program accreditation
- Loss of agents
- Teaching quality

### Operational Risks

Operational Risks are those risks that occur as part of SIHE undertaking its business and often feed into a Key Risk. These might include risks associated with the achievement of business objectives. At the operational level there are a number of specific functional risk assessments undertaken, including:

- Significant change in business operations
- Systems failure
- Poorly managed incidents
- Workplace accidents
- Health and safety
- Key people
- Skill shortage

### Finance Risks

Finance risks are those risks that result from the failure of maintaining necessary levels of funding. The *Audit and Risk Committee* should report annually to the *Corporate Governance Board* on the comparable market rates and provide advice on the need to raise or secure funding.

Finance Risks may include:

- Lack of funding
- Cashflow

- Intellectual property
- Fraud
- Exchange rates

## Risk Appetite

Risk appetite relates to the amount of risk that SIHE is prepared to accept in pursuit of business operations and strategic objectives. Statements of risk appetite assist management in assessing the appropriate level of controls to mitigate risks.

Risk appetite levels are defined for different areas of operations and quantified in this document, refer to Table 8 - Risk Appetite. Low level or insignificant risks are generally considered to be acceptable.

In many instances some level of risk is unavoidable or encouraged, however the impacts of the proposed actions and decisions should be properly identified, evaluated, and communicated and managed to ensure that exposures are acceptable.

Not all risk management can be formalised, therefore considerable reliance is to be placed on the skill, experience and judgement of personnel to take risk-based decisions that are reasonable, justifiable and in line with the SIHE objectives.

## Procedure

Detailed below are the steps for undertaking a risk assessment.

Risk Assessments should be undertaken by people who have detailed knowledge of the functional area being assessed, persons with overall responsibility and where practical a member of the Audit and Risk Committee.

Risk Assessments are judgmental in nature and are designed to direct attention to certain areas rather than be a precise quantification of any impact on SIHE. For instance, a risk that has a minor impact and is effectively controlled would not require any further treatment actions.

The process of risk management being used at Sydney Institute of Higher Education is consistent with AS/NZS ISO 31000:2009: *Risk Management - Principles and Guidelines* for risk management. The process is summarised in **Figure 1**.



Figure 1 - Risk Management Process

## Communicate and Consult

Effective communication and consultation ensure that stakeholders interests are considered and understood and those accountable for implementing the risk management process understand the basis on which decisions are made and the reasons why specific actions are required.

The owner of a risk shall ensure that employees affected by an identified risk, have information, including controls and risk treatments communicated to them. Employees who work or interact with risks identified in the *Risk Register* will have the relevant components of the *Risk Register* communicated to them.

## Establish the Context

Establishing the context of the risk management process involves the determination of the goals, objectives, strategies, scope, and parameters of the activities of the organisation where the risk management process is being applied. Consideration of both the external and internal context and the context of the risk management process is essential in this step.

Establishing external context requires building an understanding of external stakeholders and the extent to which this external environment will impact on the organisation's ability to achieve objectives.

External stakeholders have been identified as:

- Government
- Regulators
- Shareholders
- General community
- Local communities
- Students
- Consultants
- Agents

Internal context is anything within the organisation that can influence the way in which an organisation will manage risk. The internal context requires the understanding of elements within the organisation and the way they interact, such as culture, internal stakeholders, processes, structure and strategy. Internal stakeholders are all employees, the *Corporate Governance Board*, the *Academic Board*, the *Academic Quality Committee*, and the *Audit and Risk Committee*.

- Strategic
- Corporate
- Higher Education
- Operational
- Finance

Risk Category	Risk	Objective
Strategic	Failure to demonstrate value for money to shareholders	Achieve growth and financial targets
Corporate	Failure to comply with legislative, regulatory and policy/procedural requirements	Efficient and effective operations
Higher Education	Failure to attract and retain students and compliance with Higher Education regulations.	Attract and retain students. Maintain compliance with regulations.
Operational	Failure to attract, retain and develop key people in a safe work environment	Maintain a stable workforce with the required skill sets within a safe working environment. Efficient, effective and profitable operations.
Finance	Failure to maintain necessary funding levels	Raise and secure funding at best available market rates

**Table 1 - Risk categories and the objectives for each risk category**

## Identify Risks

It is critical that risk identification is carried out effectively and consistently to identify all sources of risks that are relevant to the risk assessment. The aim is to generate a comprehensive list of risks based on those events that could create, enhance, prevent, negatively affect, accelerate or delay the achievement of objectives.

The following areas should also be considered when identifying the risks to be assessed:

- Sydney Institute of Higher Education strategies
- Legal or other compliance requirements such as codes of practice, standards or guidelines
- Regulatory or stakeholder feedback
- Previous hazards or incidents and identified causes
- Changes to business operations or the introduction/alteration of new equipment or processes.

All SIHE risks are documented in the *SIHE Risk Register*. The *SIHE Executive Management Team* is responsible for maintaining an accurate risk register and reporting to the *Audit and Risk Committee*. At a minimum, all identified risks should be recorded with:



- Risk name
- Description and cause of risk
- Risk owner

The SIHE *Risk Register* is reviewed by the *Audit and Risk Committee* six times per year, with updates provided to the *Corporate Governance Board* after every *Audit and Risk Committee* meeting.

1. Strategic risk identification: Strategic risks are identified as part of the strategic planning process. The aim of identifying strategic risks is to improved outcomes while minimising adverse impacts on SIHE goals and objectives.
2. Corporate risk identification: Corporate risks are identified on an ongoing basis. This may include legal or other compliance requirements, as well as regulatory of stakeholder feedback.
3. Higher Education risk identification: Risks associated with being a Higher Education provider are identified on an ongoing basis. These risks are the risks to the operations of SIHE. This may include legal or other compliance requirements, as well as regulatory of stakeholder feedback.
4. Operational risk identification: Operational risks are associated with a significant change of a business operation and are typically identified at the commencement of the change, with updates provided throughout implementation. Once the change is fully implemented, any outstanding risks should be absorbed by the appropriate risk identification category.
5. Fiance risk identification: Finance risks can result from the failure of maintaining necessary levels of funding and have a significant impact on business sustainability.

Strategic	People	Operational	Finance	Regulatory
Business Continuity	Health & safety	Loss of TEQSA approvals	Lack Funding	Stakeholder management
Competition	Key people	Systems failure	Cashflow	Council approval
Student enrolment	Teaching quality	Tenant complaints	Intellectual Property	Industrial Action
Poor management	Skill shortage	Poorly managed incidents	Fraud	Privacy
Planning		Workplace accidents	Exchange Rates	
		Loss of Agents		

**Table 2 - Sydney Institute of Higher Education Risk Profile**

## Analyse Risks

The Risk Analysis must be undertaken to understand the risk characteristics and determine the consequences and the likelihood of the event.

It is important to determine the relevance of each risk in order to understand how best to treat them. Each risk identified shall be assessed and ranked in accordance with Table 3 - Consequence Table to determine its level of severity.

Risk analysis involves:

- Identifying the likelihood of the risk occurring
- Identifying the potential consequence or impact that would result if the risk was to occur

- Identifying controls currently in place to manage the risk by either reducing the consequence or likelihood of the risk
- Assessing the effectiveness of current controls

Area of Impact	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
<b>Overarching definition</b>	<i>Requires some effort to minimise impact</i>	<i>Requires moderate levels of resources and management input</i>	<i>Significant event which can be managed under normal procedures</i>	<i>Critical event requiring management attention</i>	<i>Disaster with potential to lead to collapse</i>
Financial (AUD)	Loss of < \$100,000	Loss of \$100,000 - \$500,000	Loss of \$500,000 - \$1 million	Loss of \$1 million - \$5 million	Loss of >\$5 million
Health/ Safety	Minor injury/ illness to individuals	Temporary disability to individuals or minor fines for breaches of duty	Serious harm to individuals and prosecution for breaches of duty by the company. Increased risk of injury to employees or public.	Single fatality or significant, long-term harm or injury and prosecution for breaches of duty against the company and individual Directors/officers	Multiple fatalities and prosecutions for breaches of duty against the company and individual Directors/officers
Operational / Process	Little or no impact	Some inefficiencies and/or delays in delivery of services. No impact on students.	Inability to provide key support services in accordance with minimal expected service levels (billings; payroll; training). Minor impact or temporary disruption to students.	Delays and inefficiencies in core processes and systems impacting significantly on students.	Critical processes and/or systems not available for extended period.  Inability to perform core customer functions.  Prolonged inability to provide basic services.
Reputation	Little or no impact	Individual complaints. No impact on staff morale.	Local, temporary adverse media.  Limited impact on	On-going local, State or national adverse media coverage.	Extended national or international adverse media coverage.

**Table 3 - Consequence Table**

For risks rated other than insignificant, determine what management strategies and/or controls are in place to address the risks. The controls identified in treating the risks can be categorised into either preventative controls, detective controls or mitigating controls.

The type of control utilised would be dependent on the risk and the cost/benefit obtained from introducing such controls. Management must assess how effective and efficient these strategies and/or controls are in managing the identified risk.

In some cases, there may be too many inefficient controls in place that may be restricting the achievement of business objectives, these controls may need to be removed. The level of control assigned to each risk, must reflect the risk tolerance of SIHE.

For risks with a rare likelihood but an extreme consequence the decision to treat may not be justifiable on economic grounds but these risks may still be treated based on other grounds, such as stakeholder perceptions. These risks should be periodically reviewed to identify any changes in consequences and likelihood. This should especially be done after a major event in the higher education sector.

Likelihood Rating	Description
5 Almost certain	Experience or available data strongly suggests that the event will occur at least once during the next 12 months.
4 Likely	Experience or available data suggests that a similar event will occur at least once during the next 18 months.
3 Possible	The event might occur at least once during the next 18 months.
2 Unlikely	It is improbable that the event will occur at least once under normal conditions during the next 18 months.
1 Rare	It is unforeseeable that the event will occur at least once or may only occur in exceptional circumstances during the next 24 months.

**Table 4 - Risk Likelihood Table**

Consequence						
Likelihood		5 Catastrophic	4 Major	3 Moderate	2 Minor	1 Insignificant
5 Almost Certain		Very High (25)	Very High (20)	High (15)	High (10)	Medium (5)
4 Likely		Very High (20)	High (16)	High (12)	Medium (8)	Medium (4)
3 Possible		High (15)	High (12)	Medium (9)	Medium (6)	Low (3)
2		High (10)	Medium (8)	Medium (6)	Low (4)	Low (2)

	Unlikely					
1 Rare		Medium (5)	Medium (4)	Low (3)	Low (2)	Low (1)

**Table 5 - Risk Matrix**

The consequence and likelihood are then used to determine the risk rating, but ranking them in the following categories:

- Risk analysis should consider the controls that are currently in place and effective for controlling each risk as identified in the SIHE Risk Register. Evaluating the effectiveness of existing controls includes consistency of application, understanding of the content of controls and documentation of controls, where appropriate. Each control is aimed at bringing the risk to an acceptable level. Controls are rated in accordance with the controls matrix.
- Once the existing controls have been identified and evaluated, the residual risk shall be calculated by using the residual risk rating matrix as show in Table 6 by using the residual rating definitions shown in Table 7.
- This is the level of risk remaining provided the existing controls are in place, effective and those exposed to the risk are aware of these controls .

Control Rating	Description
<b>Strong</b>	Segregation of incompatible functions; effective management review; reliable reporting; effective control design which is well implemented.  No significant concerns
<b>Adequate</b>	Some control weaknesses identified, however overall controls appear to be satisfactory and are partially effective.  Requires management attention within 6 months
<b>Fair</b>	Controls are operating some of the time; many control breakdowns not identified or actioned adequately.  Management attention required within 3 months
<b>Poor</b>	Controls are not considered to be reliable / effective / sufficient  Urgent management attention required.

**Table 6 - Limited Controls Matrix**

Residual Risk Rating	Definition
<b>VERY HIGH</b>	Very high residual risk is generally unacceptable. Comprehensive consideration by senior management required to ensure that the residual risk remaining is consistent with corporate objectives and risk appetite. If not, detailed research and planning required to mitigate risk.

<b>HIGH</b>	Senior management attention required to assess the acceptability of remaining net risk or required mitigation measures. Management need to ensure that necessary mitigation actions are carried out and the risk does not increase by actively monitoring any changes to the control environment, consequence and likelihood.
<b>MEDIUM</b>	Management to ensure that the control environment, consequence and likelihood does not substantially change. Consider the implementation of any additional cost effective controls.
<b>LOW</b>	Manage by routine procedures and be mindful of changes to nature of risks. Consider the implementation of any cost effective internal controls.

**Table 7 - Residual Risk Rating Definitions**

## Evaluate Risks

The residual risk ranking is used to evaluate risks. Risk evaluation determines whether further risk treatment actions are required to bring the risk within an acceptable level and which risks should be prioritised.

When determining whether further treatment required, SIHE's risk appetite and risk tolerances should be considered, as well as the actual and perceived consequences to external and internal stakeholders. Legal and regulatory requirements may also impact the risk elevation.

At the end of the evaluation process, a list is to be generated of priorities for the treatment of risks, with each risk being assigned a risk owner who ensures all aspects related to the risk are managed.

Risk evaluation also involves the review of the achievement of objectives for each risk category.

Risk appetites are defined as follows:

- Low Appetite - Where risks are identified, they will be immediately addressed. Risks will be avoided and mitigated wherever possible, and risks will be taken with utmost caution.
- Moderate Appetite - SIHE will take a thoroughly informed and considered approach to taking risks.
- High Appetite - Based on extensive planning and best available information, risks will be taken in the pursuit of SIHE strategic objectives.

Key Business Operation	Risk Appetite	Rationale
Governance	Low appetite.	Effective governance is crucial to the ongoing viability, good reputation, and efficient operation of SIHE. Governance structures are necessary to SIHE's strategic planning and achievement of strategic objectives. Thus, SIHE has low appetite for governance risk.
Program delivery	High risk appetite for innovation and improvement.  Low risk appetite for low quality in any aspect of	The delivery of quality higher education programs is primary objective of SIHE. SIHE seeks to bear risks in the pursuit of learning and teaching innovation and improvement in response to student needs.  However, in accordance with its strategic objectives, SIHE has a low risk appetite for low quality in learning and teaching practice and resources.

	program delivery.	
Compliance	Low appetite.	SIHE is dedicated to maintaining compliance with relevant legislation, regulation, industry codes and standards, as well as its own constitution, policies, and procedures. SIHE acknowledges that the ongoing viability of its operations relies on maintaining compliance, in particular compliance with legislation and regulatory requirements. Hence, SIHE has low appetite for compliance risk.
Student recruitment	Moderate risk appetite for new market development.	Within reason, SIHE seeks to bear risks in order to open new international student markets to pursue its strategic objectives.
Financial management	Low appetite for financial mismanagement.  Moderate risk appetite for expenditure in pursuit of strategic objectives.	Sound financial management is integral to the sustainability and ongoing viability of SIHE’s higher education operations. SIHE acknowledges its financial commitment to staff, students, stakeholders, and regulatory bodies. SIHE has low risk appetite for financial mismanagement.  Within reason, SIHE seeks to bear financial risks in order to pursue its strategic objectives.
IT infrastructure	High risk appetite for innovation and improvement.  Low risk appetite for low quality or inaccessibility.	IT infrastructure is crucial to program delivery and administrative and record-keeping functions at SIHE. SIHE seeks to bear risks in the pursuit of IT infrastructure innovation and improvement in response to student needs.  However, in accordance with its strategic objectives, SIHE has a low risk appetite for low quality or inaccessibility of IT infrastructure.
Student services	High risk appetite for innovation and improvement.  Low risk appetite for low quality or inaccessibility.	SIHE’s student services are essential to supporting students both academically and non-academically throughout their programs. SIHE is committed to making high-quality support services available to all students in order to meet the strategic objective: “Develop an academic environment that supports all aspects of the student experience.”  SIHE seeks to bear risks in the pursuit of the innovation and improvement of student services in response to student needs.  However, in accordance with its strategic objectives, SIHE has a low risk appetite for low quality or inaccessibility of student services.
Administration	High risk appetite for innovation and improvement.  Low risk appetite for low quality.	SIHE must maintain effective administration processes to ensure that its operations run smoothly, including functions such as updating and maintaining records, processing payrolls, and responding to enquiries. SIHE seeks to bear risks in the pursuit of innovation and improvement of administration processes.  However, in accordance with its strategic objectives, SIHE has a low risk appetite for low quality of administration processes.

Table 8 - Risk appetite

## Risk reporting and escalation

When a risk is identified it should be notified/escalated, according to Table 9. That delegate should assess whether the risk is mitigated to a level that is within SIHE's risk appetite, considering the cost and effectiveness of controls and the residual risk consequences.

If the risk is within a range that is tolerable to SIHE, then the risk is approved, included in a risk register and periodically monitored for any changes in the risk profile. If the risk is not considered to be within SIHE's tolerance, then the risk should be recorded, treatment plans developed, implemented and monitored.

Monitoring should identify when risk levels increase due to changes in the environment or ineffective control. If risk ratings increase, then those risks should be escalated in accordance with the diagram below. Risk or control owners should undertake a review of the residual risk when treatment actions are implemented to assess whether the action was effective.

All risks should be recorded in a risk register. Risks that are deemed to be at an acceptable level of tolerance should be monitored regularly and trends should be analysed to identify systemic events or causes to be escalated. Control methods need to be reviewed to measure effectiveness and to determine the impact of changes in the environment on a residual risk. Risks that are deemed to not be at an acceptable level must be accompanied by a treatment plan, tracking the plans actions, while monitoring

Risk Matrix - Risk Assessment	Escalation Recipient	Timing
Very High	Audit & Risk Committee (A&RC) then Board	Immediately advice A&RC, then A&RC advise the Board
High	A&RC then Corporate Governance Board	Next A&RC meeting, then A&RC advise the Board
Medium	Executive Management Team	Next meeting of the Executive Management Team
Low	Executive Management Team	Next meeting of the Executive Management Team

Table 9 - Risk escalation

## Treat Risks

Risk treatment involves examining possible treatment options to determine the most appropriate action for managing a risk and consideration of a cost-benefit analysis, whereby the cost of the treatment is compared to the likely reduction in risk that will occur. The purpose of the risk treatment is to reduce the level of risk to the Target Residual Risk Rating, set by the *Corporate Governance Board* and will reflect SIHE's risk appetite.

Risk treatment options to be considered include:

- Avoid the risk - do not start or continue with the activity or change the business process or objective to avoid the risk.

- Change the consequence - undertake actions aimed at reducing the impact of the risk.
- Change the likelihood - undertake actions aimed at reducing the occurrence of the risk.
- Share/transfer the risk - transfer all or part of the ownership and liability to a third party.
- Retain the risk - the level of risk is considered acceptable.

It may be necessary that in order to pursue a strategic or growth opportunity, additional risk may be taken on. The relevant risk management processes should be applied to any such circumstances as appropriate.

Identified risk treatments shall be supported by an action or management plan that documents the necessary steps required for successful implementation.

## Monitoring and Review of Risks

The *Corporate Governance Board* has overall accountability for managing risks.

The Board, the *Audit and Risk Committee* and Executive Directors will conduct ongoing monitoring of risks as part of the risk identification and assessment process. In addition, the entire *Risk Register* will be formally reviewed on at least an annual basis with results reported to the *Audit and Risk Committee* and the Board.

Existing controls of accepted risks should be monitored for effectiveness. A number of processes can be used to monitor the effectiveness of a control. These include but are not limited to:

- Auditing
- Asset, equipment or workplace inspections
- Training or awareness programs
- Project management planning, monitoring and review; Job safety and environmental analyses
- Incident investigations
- Hazard reporting and correction
- Regulatory compliance monitoring
- Emergency or crisis exercise
- At regular intervals to ensure consistency and accuracy of Sydney Institute of Higher Education's risk management program.
- When changes to Sydney Institute of Higher Education's strategies have occurred.
- Where changes to legal or other compliance requirements such as codes of practice, standards or guidelines may impact the operations of Sydney Institute of Higher Education.
- Upon receipt of regulatory or stakeholder feedback that may impact the objectives of Sydney Institute of Higher Education.
- Where incident investigations have identified the failure of existing controls or the failure to manage risks.
- Where internal or external audits have identified gaps in Sydney Institute of Higher Education's governance processes or systems failures.
- Changes to business operations or the introduction/alteration of new equipment or processes.

A risk review or review of the *Risk Register* shall determine:



- The accuracy of the risk description.
- The relevance of the risk information in relation to the scope and context of Sydney Institute of Higher Education's operations.
- The adequacy and effectiveness of existing controls (including the addition of implemented risk treatments).
- Whether the agreed target risk has been achieved.
- The new residual risk ranking based on the success of the implemented risk treatments.
- Whether the level of risk is considered to be acceptable.
- Any new risk treatments if the risk is not acceptable.
- A revised target risk based on the additional risk treatments identified.

The review shall ensure that successfully implemented risk treatments are classified as existing controls on the relevant *Risk Register* and that these controls are being monitored for effectiveness. the trends, control methods and changes in environment.

## Relationship with other processes

Risk management needs to be integrated with existing business processes to maximise risk management benefits and opportunities.

Some of the key business processes to be aligned with risk management are:

- Business planning (including formation of budgets, business continuity, workforce planning, and IT strategies) - Identifying risk during the planning process may result in a strategy/activity being excluded due to associated risks being too high or unmanageable. The identification of risk allows for a clearer assessment of realistic delivery times for strategies/activities.
- Marketing Strategy - Risk analysis impacts on the way the organisation engages with stakeholders.
- Performance Management - Sydney Institute of Higher Education's people management processes ensure that individual performance plans include responsibilities for risk ownership and implementation of risk treatments.

## Policy Implementation and Monitoring

The *Corporate Governance Board* delegates responsibility for the day-to-day implementation of this policy to the *Audit and Risk Committee*.

The *Audit and Risk Committee* will develop and maintain the *Risk Register*, identify, monitor, and establish risk mitigation strategies, and provide regular reports to the Corporate Governance Board.

The *Academic Board* will monitor and mitigate risks in relation to academic quality and integrity.

SIHE staff will identify and mitigate risks that may eventuate during their employment.

## Review Schedule

This policy will be reviewed by the *Corporate Governance Board* annually.

Version History				
Version number:	Approved by:	Approval date:	Revision notes:	Next review date:
1	Corporate Governance Board	4/09/2017		
2	Corporate Governance Board	16/10/2017		
3	Corporate Governance Board	05/02/2018		05/02/2021
4	Corporate Governance Board	30 September 2022	Standard Review. No changes required. Risk Register itself has been modified and is updated annually.	30 September 2025
5	Corporate Governance Board	31 October 2023	Reviewed and made changes in line with Governance structure, risk register and Risk Framework and Risk Process. Action item 8.b. of CGB meeting.	31 October 2026
6	Corporate Governance Board	31 October 2023	After consultation with the Audit and Risk Committee members, the Risk Management Policy, Procedure and Framework combined into one document to simplify use and ensure compliance.	31 October

End of document: "Risk Management Framework Policy"









Document ID: 8662, Revision No : (10), Created : January 6, 2020 12:52 pm, By : anushka.manandhar@sihe.edu.au, Last updated : October 30, 2023 1:26 pm, Updated by : courtney.nelson@sydneyinstitute.edu.au, Next Review by : Nigel, , Review Scheduled For : February 5, 2021

Produced & Printed : Tuesday 31st of October 2023 04:37:31 AM "Sydney Institute of Higher Education ABN 49 618 742 813 TEQSA PRV14323 CRICOS 03866C"

### Related Documents

	<a href="#">Academic Integrity and Conduct Policy</a>
	<a href="#">Anti-Fraud and Corruption Policy</a>
	<a href="#">Conflict of Interest Policy</a>
	<a href="#">Program Review and Continual Improvement Policy</a>
	<a href="#">Critical Incident Response Policy</a>
	<a href="#">Delegation of Authority Policy</a>
	<a href="#">Financial Management Policy</a>
	<a href="#">Risk Register</a>

---

		<a href="#"><u>Business Continuity Plan</u></a>
		<a href="#"><u>Strategic Plan</u></a>
		<a href="#"><u>Audit and Risk Committee - Terms of Reference</u></a>
		<a href="#"><u>Academic Board - Terms of Reference</u></a>