Risk Management Framework

Institute of Health and Nursing Australia

Legal entity: Health Careers International Pty Ltd
ABN: 59 106 800 944
ACN: 106 800 944
CRICOS Code: 03386G
RTO ID: 21985

www.ihna.edu.au

1. Executive Summary

At the Institute of Health and Nursing Australia (IHNA), we understand that risk is inherent in our mission to foster a diverse learning community that prepares students for life-enhancing careers in an ever-changing world. A defined approach to identify and manage risks is needed to ensure that everyone understands the nature and magnitude of risks that IHNA is willing (or unwilling) to take in pursuit of its strategic objectives and to ensure the effective management of those risks.

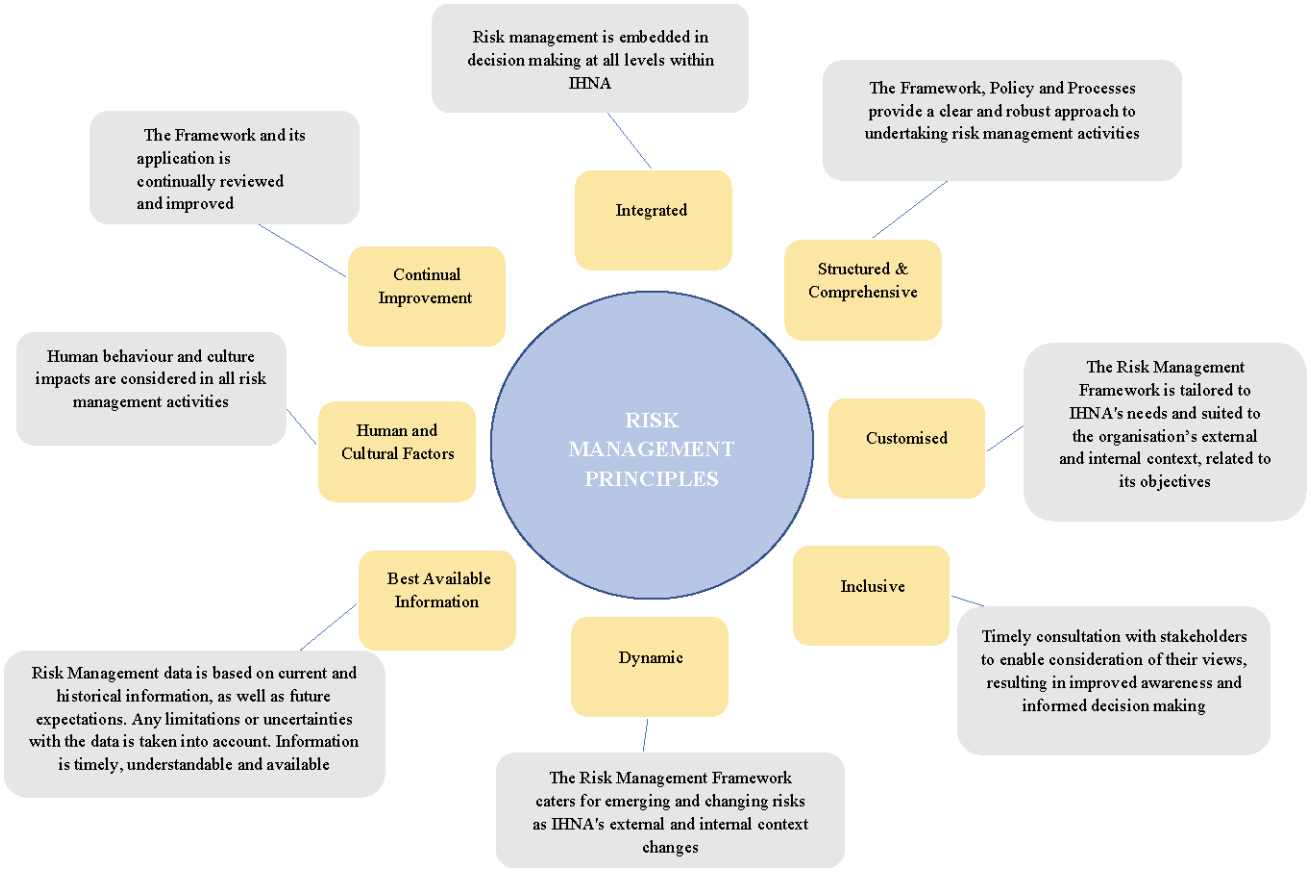
IHNA'S approach to risk management is based on the AS/NZS ISO 31000:2018 Risk Management Principals and Guidelines (ISO 31000). The alignment to ISO 31000 allows IHNA to measure the successful implementation of ITS Risk Management Framework against the value creation and protection principles outlined at Figure 1.

2. Objectives

IHNA'S Risk Management Framework provides an overview of IHNA's approach to risk management and explains how this approach should be implemented and applied across the organisation. The objectives of this framework are to:

- Support IHNA's Risk Management Policy and to provide a common approach to identify, assess, and manage potential risks that may affect the business.
- Describe the governance and oversight of risk management activities;
- Encourage a high standard of accountability at all levels of IHNA;
- Support stakeholders to make decisions about risks that align with IHNA's values, policies, and risk tolerance, and provide decision makers with accurate, timely, comprehensive risk information;
- Encourage closer alignment between risk management and other business functions such as planning, continuous improvement and internal audits;
- Ensure IHNA employees and other stakeholders have access to practical, plain language resources for identifying and managing risks;
- Assist the business in complying with the Australian Stock Exchange Corporate Governance Principles, specifically in relation to risk management.

Figure 1: ISO 2018 Value Creation and Protection Principles



3. Risk Management Framework Architecture

There are four (4) key documents which comprise IHNA's guidance on its risk management framework. These are:

a) **Risk Framework** – This document outlines the approach and structures in place at IHNA to identify, assess, and manage risks. It also describes the reporting and escalation processes at an IHNA- wide level.

b) **Risk Policy** – This document sets the tone from the top, outlining Board and Executive Management commitment to the use of risk management as a driver of decision making. It also outlines the key risk related responsibilities of employees and Governing bodies.

c) **Risk Appetite and Tolerance Statements** – This document provides the decision maker guidance on the level of risk-taking that the Board has determined is appropriate, and when risks need to be escalated or further controlled to bring them into line with Board expectations.

d) **Risk Procedure** – This document provides practical, common-sense guidance on how to apply the risk framework, policy, and appetite statements to manage risks, including risk identification, analysis, treatment, and reporting.

4. Application

IHNA's Risk Management Framework applies organisation wide. It can be applied to all levels of IHNA, in both strategic and operational contexts. The framework applies, but is not limited, to:

a) Corporate planning;
b) Financial management;
c) Legislative and internal compliance;
d) Procurement and contract management;
e) Facilities and asset management;
f) Information Technology and Data Management;
g) Occupational Health and Safety;
h) Workforce Management;
i) Business continuity and disaster recovery;
j) Development and implementation of new services;
k) Development and review of new courses including industry consultation, validation, moderation, annual review, and course performance reporting;
l) Academic integrity including contract cheating and online assessments;
m) Learning and Teaching including student at risk, student satisfaction, graduate outcome and employability;
n) Professional experience placement, Work integrated learning;
o) Partnerships including Joint Ventures, Third party delivery, Recruitment Agents and Clinical placement.

Risk Management Calendar

The table below shows key events and stakeholders involved in activities to ensure that IHNA's approach to risk management stays current.

Task	Actions	Responsible	Stakeholders	Timing
Annual Review of IHNA-wide Risk Framework Documents	• Review Risk Management Framework, Policy, and Appetite Statements – recommended by Audit & Risk Committee for Board Approval • Review Risk Procedure Document and supporting templates – Risk & Compliance Team • Review of risk culture at all levels of IHNA • Review of framework including any assurance reviews	Risk Manager	Executive Management Committee (EMC) Audit & Risk Committee (ARC) Board of Directors Internal Audit	Jun/Jul
IHNA-wide Major Risk Update Exercise	• Undertake environmental scan considering external factors, SWOT analysis and review of strategic objectives to identify changes to IHNA-wide risk profile.	Risk Manager	EMC ARC Board Internal Audit	Mar/Apr

	• Analysis of internal audit findings to inform the risk profile • Analysis of incident trends including student complaint • Compliance obligations review			
Quarterly IHNA Risk Updates	• Review and report changes to the risk profile – including progress with implementing risk treatment plans and changes to risk ratings	Risk Manager	Risk Owners EMC ARC Board	Jun/Jul Sep/Oct Dec/Jan Mar/Apr
Business Unit Risk Profile Exercise	• Undertake exercise twice a year to create/update Business Unit risk profiles.	Risk Manager	Managers Risk Owners	Nov & May
Business Unit Annual Review of Local Risk Appetite	• Considering the IHNA-wide risk appetite, create/update local risk appetite and tolerance statements	Risk Manager	Managers Risk Owners	Nov/Dec

5. Responsibilities

IHNA applies the Three Lines of Defence Model (described in section 13) for clarifying accountabilities within its Risk Management Framework. A key principle of this model is that the ownership and management with risks sits with management and operational staff. The Risk Team's role is to provide oversight, challenge, and guidance to IHNA on the management of risks. The Internal Audit function, along with other assurance activities, provide IHNA with independent assurance as to the effectiveness of IHNA's Risk Management Framework.

For a description of key roles and their risk management related responsibilities, please refer to the IHNA Risk Management Policy.

6. IHNA's Risk Culture & Strategic Risk Culture

6.1. Risk Culture

All IHNA staff have a role to play in managing risk at IHNA. We have a culture where all employees appreciate the importance of risk management and proactively contribute to its framework, policy, process, and practices. It is important to highlight that risk culture is part of IHNA's overall organisational culture – it is not a separate activity. IHNA has the full support of Executive Management, the Audit & Risk Committee, and the Board of Directors to create and maintain a positive risk culture. IHNA's risk culture, its direction and improvement are reviewed annually along with the Risk Management Framework.

IHNA is committed to building a risk management culture where:

- Staff engage constructively with risk and understand thinking about and managing risk is a core part of their role.
- Consideration of risk is incorporated into decision making.
- Staff feel supported by executive management in raising and escalating risks as this is seen as a valuable activity.

IHNA will develop risk culture indicators and reporting to provide regular updates to Executive Management, Audit & Risk Committee and Board of Directors and to inform its annual review of risk culture and the effectiveness of the Risk Management Framework.

6.2. How risk is defined at IHNA

Adopting the ISO 31000:2018 Standard's definition, Risk is the effect of uncertainty on objectives and effect is a deviation from the expected – positive or negative.

Objectives can have different aspects, (such as financial, health and safety, technology, and environmental goals) and can apply at different levels (such as organisation-wide, operational, project, product, and process)

Risk is often expressed in terms of combination of the consequences of an event (including changes in

circumstances) and the associated likelihood of occurrence.

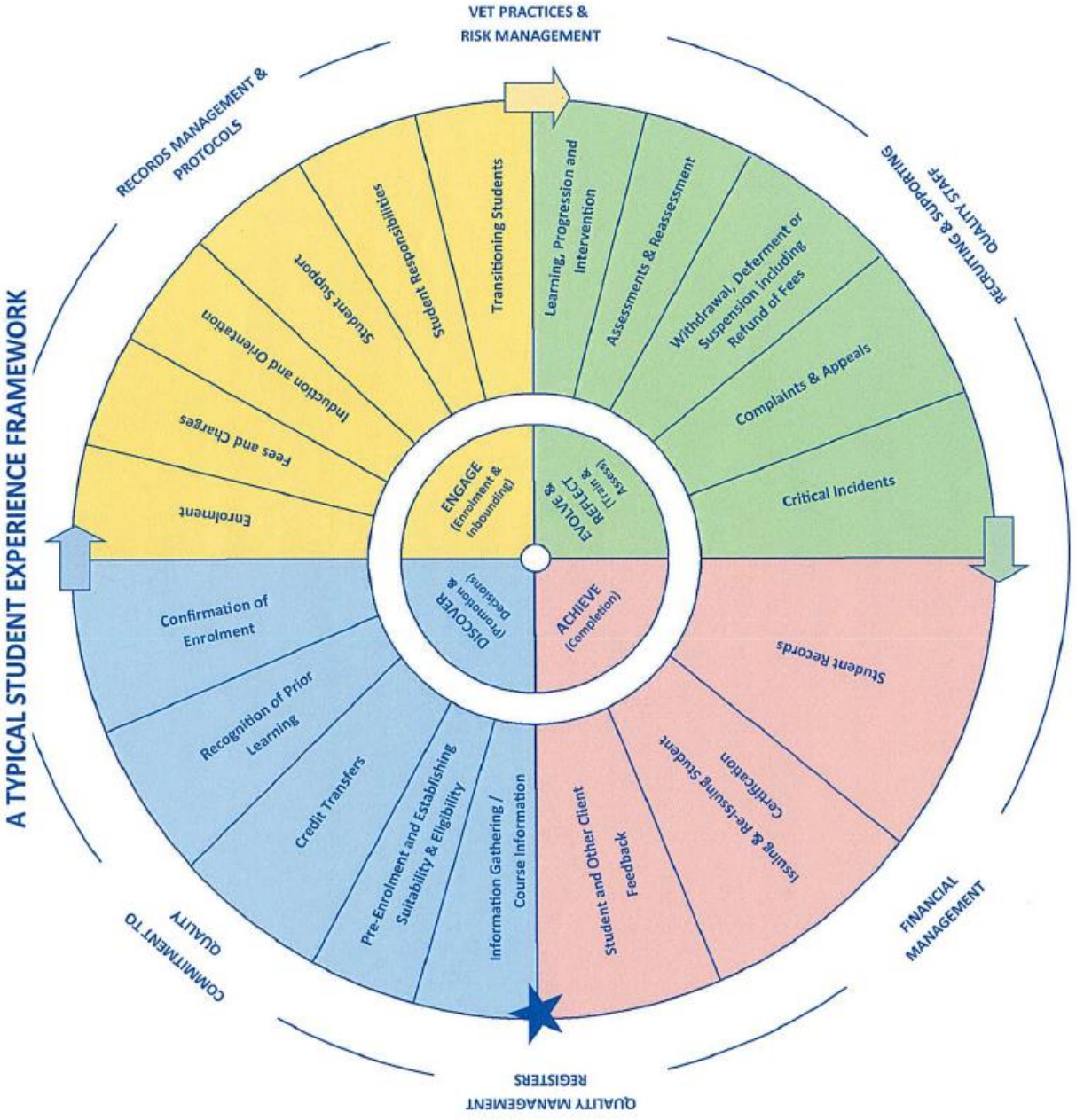
The definition emphasises that risk is not just about downside or adverse events, it is also about missing out on the upside or added value that opportunities bring. IHNA must recognise opportunities in time and capitalise on them. High risk, high reward is often a phrase utilised and highlights the opportunities aspect of risk.

6.3. Objectives of Risk Management

The overall purpose of risk management is the creation and protection of value for IHNA's key stakeholders, through embedding risk information into everyday decision making across the organisation.

The objectives and benefits of IHNA's approach to risk management are to:

a) Establish a positive risk culture;
b) Help IHNA to protect its assets including its reputation;
c) Protect the safety of students and staff;
d) Support achievement of strategic and operational objectives, through early identification and management of risks and opportunities;
e) Encourage innovation;
f) Prevent business disruptions from interrupting IHNA's critical functions;
g) Support sound decision-making and effective resource management;
h) Support adoption of risk treatment strategies that are fit for purpose, cost-effective and reduce risk to an acceptable level.
i) Manage risk and incorporate quality management across the entire students life cycle of student journey.



6.4. Definition and Purpose of the Risk Appetite Statement (RAS)

Fundamental to a robust Risk Management Framework is the development and understanding of IHNA's Risk Appetite. Risk Appetite can be defined as the amount of risk, on a broad level, that IHNA is prepared to take in meeting its organisational goals.

The Board is responsible for determining IHNA's appetite for risk. The Board's risk appetite must align to:

a) the risk culture of IHNA;
b) the vision, mission, and values of IHNA;
c) strategic plan and goals;
d) IHNA's service commitment and student demographic;
e) the financial and budget environment in which IHNA is operating.

The Board recognises that certain risk types that are inherently risky, such as the provision of professional experience placements for students may not be capable of being managed to a level of zero risk. This means that not all risks can be removed; some can be reduced or shared consistent with industry practice; however, these risks are understood, tolerated, controlled, and monitored by Executive Management and the Board. The Board understands that incidents and challenges may occur but does expect that IHNA will learn from these events. For material events, a root cause analysis or other similar investigation is undertaken, and where relevant learnings shared to prevent reoccurrence where possible.

6.5. Approach to Risk Appetite

IHNA sets its risk appetite by:

a) Setting top-down risk appetite statements that define the expected level of risk that IHNA is willing to accept across a range of strategic priorities and consequence areas.

b) As part of the regular review of the IHNA risk profile, determining whether each reported risk, its rating, controls effectiveness and proposed treatments are within or outside appetite.

Appetite vs Tolerance

IHNA defines **risk appetite** as the amount of risk it is prepared to accept during normal operations. Anything outside of its risk appetite must be escalated without delay for decision making about whether the risk can be brought back within acceptable levels and what controls, or resources are required to affect that change.

IHNA defines **risk tolerance** as the upper limit the organisation can bear, or put another way, something that is outside tolerance should not be allowed to occur.

Within Appetite	Within Tolerance	Outside Tolerance
Operations proceeding within expected ranges. Risks within these ranges can be taken by Executive Management	Operations or risks have exceeded the Board's appetite level. Escalation is required to the Audit & Risk	Operations or risks have exceeded the level that the organisation has determined is its upper limit of capacity to manage/absorb.

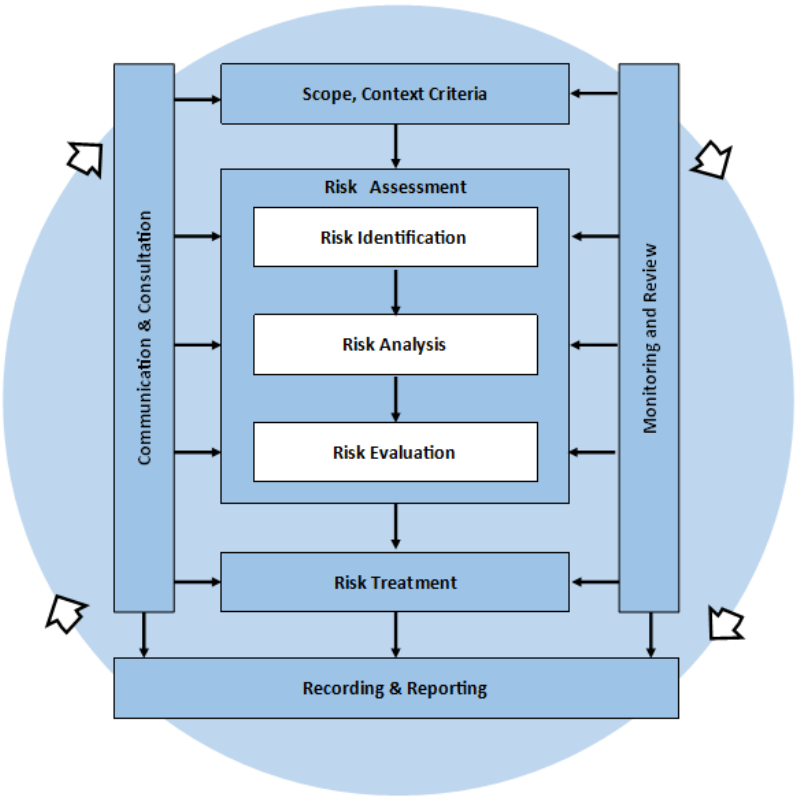
as long as proactively managed.	Committee and Board for monitoring and oversight. Executive Management, with oversight from the Audit & Risk Committee and Board, would seek to bring these risks back to within appetite as quickly as possible.	Typically risks or measures should not be allowed to reach this stage. Escalation is required to the Audit & Risk Committee and Board and may result in the activity ceasing, being modified or significant resources applied to control the risk back to an acceptable level.

It is important to note that **Escalation is required** as soon as a risk or measure exceeds the appetite threshold even where it is within the tolerance range.

Please refer to IHNA's Risk Appetite Statement for detail on IHNA's risk appetite and tolerance levels.

7. Risk Management Process

IHNA has a systematic and integrated risk management process that is effective in managing risk. The risk management process outlined below is aligned with ISO31000 and describes the steps IHNA takes when identifying and assessing a risk:



IHNA's risk management approach often begins with a clear understanding of the outcome it is trying to achieve, defined during the Scope, Context and Criteria phase, and the identification of barriers or roadblocks (risks) to achieving those objectives.

This outcome focused approach to risk management ensures that the risk management process is helping IHNA create and protect value.

To supplement this approach, and to ensure that IHNA has a broad and wide view of all threats and challenges, IHNA will also periodically (at least once a year) conduct environmental scanning and threat analysis exercises to ensure that all possible risks, challenges, and threats (not just those that neatly align to defined goals and objectives) are identified and given appropriate consideration.

IHNA will also ensure that both a top down (Board and Executive Management) and Bottom Up (Operational and Front-Line teams) approach to risk identification occurs annually.

Each year, IHNA will undertake:

1. Board and Executive Management-level workshops to understand and define threats and challenges to achieving IHNA's objectives
2. Board and Executive Management-level assessments of IHNA's Internal and External context through an environmental scan and threat analysis
3. A bottom-up approach to risk identification including:

a. A business unit level identification of risks to achieving objectives at an operational level (reviewed 6-monthly)
b. Analysis of internal audit reports to identify gaps in risk management strategies and controls
c. Analysis of incident trends
d. An annual assessment of IHNA's compliance obligations and how effective its management controls are.

For more detail on each step of the risk management process, refer to IHNA's Risk Management Process document.

7.1 Risk Indicators

In the risk identification stage of conducting a risk assessment, risks identified are classified into one of the following risk indicator groups:

key indicator	Risk Tolerance Statements
Student experience	• In terms of giving its students the best possible academic and research experience, IHNA has made a commitment. To ensure that support is available, accessible, and appropriate, and that students are satisfied and stay engaged with IHNA and their studies, this commitment includes pastoral and cultural components of students' experiences (such as student safety, mental well-being, and welfare) (future alumni). • IHNA has a ***balanced to entrepreneurial*** appetite for risk towards student experience. • ***Higher*** tolerance for pursuing activities and projects that result in student engagement and improve student satisfaction levels and retention rates. • ***Lowest*** tolerance for compromises to the agreed minimum standard for an acceptablestudent learning experience and acceptable research experience.
Research	• IHNA is committed to developing and diversifying its research programs and industry participation, as well as attracting high-caliber students and staff, while preserving the student experience and our reputation. At all times, our endeavors must be ethical and carefully weighed in terms of the likelihood of success and the required expenditure. • IHNA has a ***balanced to entrepreneurial*** appetite for risk towards research. • ***Higher*** potential to pursue research opportunities, partnerships and high-performing employees that contribute to research translation, our outstanding reputation, and improved standings. • ***Higher*** tolerance for responding to and accommodating the industry specific (IndustryEngagement Partners) appetites for applied research. • ***Higher*** tolerance for systems, philosophy and spaces that activate the maximum benefit ofR&D outcomes (utilisation, management of conflict of interest). • ***Lowest*** tolerance for engagement with organisations who don't share our values, or fromwhose association with us will cause unacceptable risk to our reputation and brand and damage our overall engagement with community. • ***Lowest*** tolerance for compromising the quality of research. • ***Zero*** tolerance for research misconduct, breach of relevant National Codes, fraudulent research, or false publication of research data or material.

Teaching	• IHNA is committed to providing a high-quality educational program that meets the future needs of students, employers, industry, and the larger society, as well as to employing highly qualified teaching professionals to offer the program in a transformative and innovative manner, while adhering to mandated Standards and meeting the objectives of IHNA's Academic Commitment. • IHNA has a ***balanced to entrepreneurial*** appetite for risk towards teaching. • ***Higher*** tolerance for pursuing transformative and innovative teaching programs, (processtechniques, recruitment). • ***High*** tolerance for a blended profile of experience or qualifications in the academic /teaching workforce (including people from a non-academic background). • ***High*** tolerance for growing the student cohort (domestic and international) *coupled with a* • ***Low*** tolerance for growing student cohort at expense of students' opportunity to thrive or succeed and low tolerance for compromising IHNA internal standards (entry requirements/English language) and compromising the student experience. • ***Lowest*** tolerance to any compromise to academic integrity (permit mistakes).
Culture and values	• IHNA is conscious of societal and community expectations and values a culture of scholarship, research, sustainability, engagement, social justice, and honesty. IHNA may have to accept some risk to balance competing goals; however, it must always ensure that the possible benefits and risks are fully understood before initiatives are approved, and that reasonable measures to limit unacceptable risk are put in place. • IHNA has a ***balanced*** appetite for risk towards culture and values. • ***Higher*** tolerance for meaningful and innovative involvement inside IHNA, as well as with Industry, the vocational education sector, and the broader community. • ***High*** tolerance for transparency and consultation in our communications. • ***Lowest*** tolerance for failure to declare conflicts and / or manage conflicts of interest. • ***Lowest*** tolerance for improper behaviors or performance that violates the IHNA Code of Conduct and agreed-upon values and behaviours, as well as poor behaviors or conduct those jeopardies academic integrity and/or has a negative influence on IHNA and others (reputational damage). • ***Zero*** Tolerance for unethical or illegal behaviors, as well as conduct that puts individuals in danger or threatens their safety or well-being, such as threatening, harassing, or aggressive behaviors.

Financial viability	• Aside from our determination to meet our efficiency standards, we also need to maintain a healthy financial position as described in our financial statements / reserves / investments. We must place a heavy emphasis on performance measurement and management because we have so many stakeholders relying on us and are entrusted with public funds. • IHNA has a ***balanced*** appetite for risk towards financial viability. • ***Higher*** tolerance for exploring innovative methods for financing our strategic growth objectives. • ***Low*** tolerance for non-compliance with accounting standards & funding contract instructions. • ***Zero*** tolerance for internal fraud; Internal fraud has zero tolerance, and the risk can only be tolerated if all legislative fraud control criteria have been met and the risk has been minimised to the point where additional controls would have a negative cost/benefit ratio.
Service disruption	• IHNA programs and services are available at all times of the day and throughout the year. It's critical that these activities are of good quality, and that the services are available when they're needed. • IHNA has a ***conservative*** appetite for risk towards service disruption. • ***Highest*** tolerance for quality services (best available - associated with property, technology,or people). • ***Moderate*** tolerance for manual systems and non-critical internal system outages, allowing that certain inefficiency and non-critical errors may occur if they do not violate regulations, violate privacy, or result in litigation. • ***Low*** tolerance towards widespread or sustained industrial action by staff, resulting in serviceinterruption. • ***Lowest*** tolerance for service interruption to critical systems, or to systems at critical times;or for service disruption that will impact the safety and wellbeing of students, staff, and community. • ***Zero*** tolerance for deliberate misuse or inappropriate use of systems that results in outages to critical systems, or to systems at critical times.
Safety and health	• A safe working environment for all workers, students, visitors, and contractors is a top priority at IHNA. • IHNA has a ***conservative*** appetite for risk towards safety and health. • ***Low*** tolerance for lost time or injury in areas where there is inherent risk in the nature and locationof some activities and environments. • ***Zero*** tolerance for death or permanent disability because of violating or failing to follow specified safety protocols, as well as for lost time or harm because of violating prescribed safety protocols or standards.

Regulatory and compliance	• With our important stakeholders, investors, regulators, government industry partners and community, we should not jeopardise our reputation for integrity and professionalism. • IHNA has a ***conservative*** appetite for risk towards regulation and compliance. • ***Zero*** there is zero tolerance for legal and compliance violations. While minor breaches are inevitable given the intricacies of business and the settings in which we operate, there should be no excuse for negligent or purposeful violations of legislation or standard operating procedures.
Environmental and social responsibility	• IHNA is committed to protect sustainable campuses and building strong platforms for collaborating with the community on environmental protection (and address climate change). • IHNA has a ***balanced to entrepreneurial*** appetite for risk towards environmentaland social responsibility. • ***Higher*** tolerance for activities and initiatives that prioritise sustainability and diversity and inde and engage with relevant communities. • ***Lowest*** tolerance for adverse environmental impacts or breaches from our activities.

7.2 Risk category

Risk Category	Description
Reputational risk	The term "reputational risk" refers to the possibility that negative publicity, public perception, or uncontrollable events will harm IHNA's reputation, consequently hurting its income.
Strategic	Strategic risks have the potential to impact achievement of IHNA's strategic objectives.
Operational	Operational risks are identified by Business Units in relation to their business plans.
Regulatory and Compliance	Regulatory Risks relate to IHNA's registration, accreditation, regulatory policy, and compliance requirements essential for the ongoing operations of the organisation

These categories are helpful to understand the appropriate audience and escalation points for each risk type (e.g., strategic risks are important to Executive Management and the Board regardless of risk rating), and to inform conversations on appropriate treatment strategies.

To provide useful reporting to the Board and the broader business, IHNA will also classify its risks in relation to the consequence categories defined in this Risk Management Framework. More than one category may apply to one risk:

a) Financial,
b) IT and Equipment,
c) Regulatory and Compliance,
d) Occupational Health and Safety,
e) Business Continuity,
f) Reputation.

7.3 . Analysis Criteria

In the analysis phase of conducting a risk assessment, IHNA determines a risk's rating using the following risk measures and scales:

- Likelihood Table
- Consequence Table
- Controls Effectiveness

With the risk rating being expressed using the Risk Matrix

The detailed process for conducting a risk assessment and using these measures can be found in the Risk Management Process Document.

7.4 Escalation and Monitoring of Risks

IHNA are empowered to manage and monitor their own risks in line with the organisation's risk appetite and tolerance levels. There may be a need to escalate risks that are rated higher than the appetite level, or when controls have been assessed as weak. Risk escalation and monitoring is an important tool for ensuring that risks are known and understood by the people with the authority to appropriately manage them. If an identified risk poses a material risk and requires allocation of substantial risk treatment resources, then the risk is escalated to Executive Management for monitoring.

All risks identified at any level of the organisation, regardless of the risk rating, need to be reported and entered IHNA's Risk Register.

When a risk that requires escalation is identified outside the ongoing quarterly risk review process, escalation to the appropriate recipient in line with the escalation criteria defined below needs to occur quickly.

All strategic and escalated risks are to be reported to Executive Management and the Audit & Risk Committee quarterly. Risk reporting also occurs regularly to the Board through the Risk Compliance and Safety Report and through the CEO's Tier 1 Risks Report.

Table Risk Escalation & Monitoring

Escalation Level	Criteria for escalating management of risks	Criteria for inclusion in reporting (in addition to the column to the left)
ARC & Board	• All strategic risks • Any risk with a residual risk rating of Very High	• Incidents rated moderate and above • Overall risk profile (all risks)

CEO / Executive Management Committee (EMC)	• Residual risk rating of High or above • Residual risk rating of Medium where the control rating is Weak or action plans are > 3 months overdue	• Incidents rated moderate and above • Overall risk profile (all risks)
Business Unit Manager	• Business unit risks with a residual risk rating of Medium or above	• All risks and incidents within their business unit
Responsible Line Manager	• Business unit risks with a residual risk rating at all levels	• All risks and incidents within their sphere of control

Escalated risks that are included in the reporting to the Board, ARC, CEO and EMC may be de-escalated and removed from the report once risk has been managed to a level within risk appetite as agreed by the escalation body.

8 Communicating and reporting Risk Information

8.1 Reporting the Risks

Risk information will be reported to the Executive Management Committee monthly, and the Audit & Risk Committee and Board of Directors quarterly.

Reporting provided will include:

Body	Reporting
ARC & Board	• Risk Snapshot • Escalated Clinical Risks Snapshot • Risk Register – Detailed • Residual Risk Heat Map • Risk Profile (snapshot of all risks including those at lower levels) • Risk and incident trend analysis • End of month Board reporting • CEO's Monthly Tier 1 Risk Report
CEO	• Top Risks Update

Executive Management Committee	• Risk, Compliance and Safety Report, focusing on claims and incident (staff and student) data • End of Month Risk Reporting
Business Unit Manager	• Business Unit Risk Snapshot and Heat Map • Business Unit Risk Register – Detailed

8.2 Risk Communication

IHNA uses several methods to keep its employees up to date with emerging risk trends. This includes, but is not limited to:

- Regular risk management discussions during team meetings at Business Unit level;
- Sharing Quarterly IHNA Risk Profile reports with the Executive Management Committee;
- Ad hoc risk communication sent by the Risk and Compliance Team;
- Best practice and success stories within IHNA are communicated to inspire and encourage other employees.

8.3 Risk Management Strategy & Roadmap

IHNA's Risk Management Strategy and Roadmap is a document that describes the organisation's future vision, direction, and objectives for risk management. It incorporates key strategies to be implemented over the next three years to achieve these objectives and is updated annually. As well as clear statements about the future evolution of the Risk Management Framework and Approach.

8.4 Relationship between Internal Audit and Risk Management

At IHNA, it is expected that the risk management team and internal audit function will collaborate to provide best value to the organisation. This collaboration should occur in developing the internal audit plan and in undertaking risk assessments.

The output from the risk management function will form a key input into the annual internal audit planning process, particularly IHNA's risk profile. The internal audit function should focus on assisting to identify control improvements, for those risks sitting outside of risk tolerance levels, and validating those controls to manage high inherent risks are operating as intended.

Internal Audit report findings need to be taken into consideration by the risk owners, monitoring controls that impact the control effectiveness ratings of key risks.

Periodically, Internal Audit will review the effectiveness of IHNA's Risk Management Framework.

9 Building Risk Capabilities

IHNA staff are expected to have the skills to be able to apply the Risk Management Framework. Requisite competence will be obtained through a combination of formal training and on-the-job learning specifically:

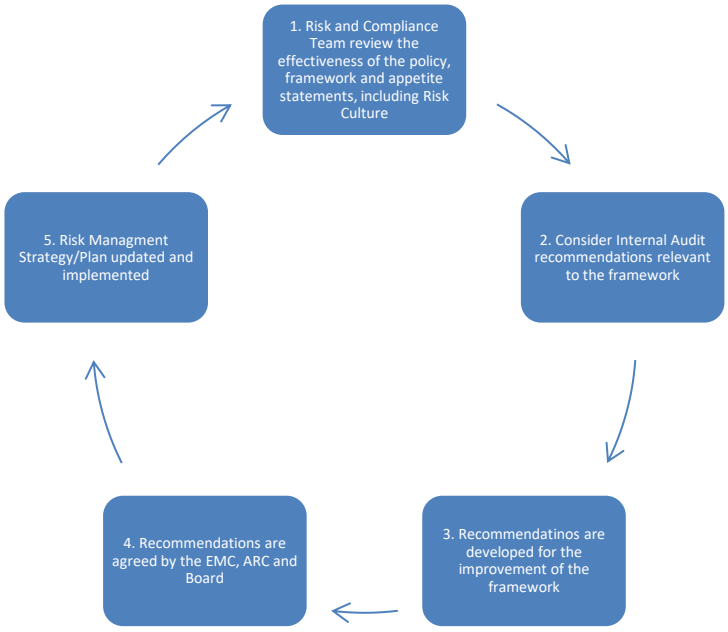
- New starters will be provided risk management training as part of their induction program. New starters with risk owner responsibilities will also be provided additional 1-on-1 training by the Risk and Compliance team.
- Existing staff, requiring upskilling in risk management, will receive refresher training every 1 – 3 years.
- Other staff who require additional risk management skills will receive training tailored to their needs.

Online learning tools, face-to-face classroom style learning and 1-on-1 training methods will be applied as appropriate.

10 Monitoring and Review of the Risk Management Framework

IHNA acknowledges that effective risk management is an ongoing, evolving practice and commit to the annual review of the Risk Management Framework to ensure it remains current and provides a consistent, cohesive, and standard approach to the application of risk management. Continual Improvement of the Risk Management Framework will be implemented through monitoring and analysis of key performance data.

The annual cycle of review for the Risk Management Framework is as follows:



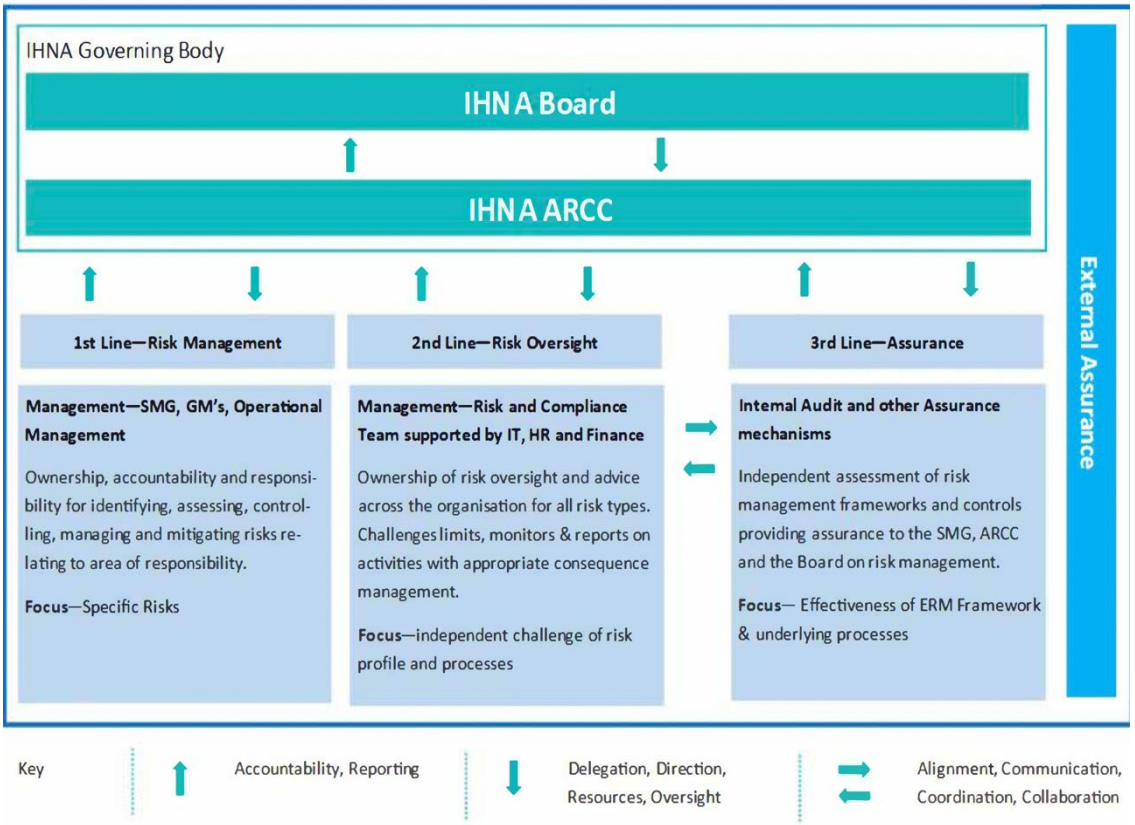
When assessing the effectiveness of the Risk Management Framework and Appetite Statements, the Risk & Compliance Team will consider:

- Internal audit recommendations
- Key Risk Indicator performance and trends
- Changes in the IHNA risk profile over time
- Performance against IHNA's insurance program
- Any changes to IHNA's internal and external operating context
- Any changes to international standards or best practice guidance
- Feedback from staff and management, including feedback from the ARC and Board

13. Three Lines of Defence Model

The three lines of defence model applied at IHNA (shown below) is an integrated model which clarifies accountability for risk management activities across IHNA.

Figure 2: 3 Lines of Defence Model[1]



[1] Source: The Institute of Internal Auditors Three Lines Model. 2020

First Line – The first line represents those that own and manage risk within the business. This may include Business Unit Teams, and Managers. They are responsible for the operational delivery of their area of responsibility, and in turn for managing relevant risks to their areas.

Second Line - Second line roles assist in managing risk and may be focused on specific objectives, for example Compliance or have broader IHNA-wide risk management roles. In IHNA's case, the second line roles would include the Risk and Compliance Team and where necessary bringing in the expertise of other experts within IHNA such as IT and HR. Direct responsibility for managing identified risks remains the role of the first line and within the scope of management.

Third line - Internal Audit, along with the other areas of external assurance outlined below, is the third line of defence. This line provides independent, objective assurance and advice on the effectiveness of governance and risk management. Internal Audit reports findings to management and the Board (via the ARC) to promote and facilitate continual improvement.

At IHNA, the activities of each line of defence are aligned through communication and collaboration. This contributes to the creation and protection of value and helps ensure the reliability and transparency of information needed for risk-based decision making.

Other sources of assurance – IHNA also seeks assurance on the effectiveness of its risk management approach through a range of internal and external quality exercise including:

- External Audit Reports
- Accreditation reviews
- External Regulatory Inspections and Reviews
- And other instances where IHNA's operations are reviewed by a third party.

14. Key Related Documents

- AS/NZS ISO 31000:2018 Risk Management Principles and Guidelines (ISO 31000).
- AS HB 436 – 2013 Risk Management Guidelines (HB 436)
- AS NZS ISO 9001 2016 Quality Management Systems - Requirements
- ASX Corporate Governance Principles and Recommendations – Principle 7
- Institute of Internal Auditors – Three Lines Model (2020)
- IHNA Risk Management Policy
- IHNA Risk Management Processes

Attachment A: Consequence* Assessment Table

Ratings	Financial	IT and Equipment	Regulatory and Compliance	OH&S/WHS	Reputation	Business Continuity
5. Severe	> 10% of EBITDA	▪ Business critical applications down for > 36 hours	▪ Significant loss of accreditation or other regulatory incident that impacts operational ability across IHNA	▪ Death or permanent physical or psychological injury to an employee	▪ Negative media (TV, Newspaper) coverage lasting beyond 3 days ▪ Adverse social media lasting beyond 2 weeks ▪ Loss of confidence from shareholders	▪ Loss of operations across an entire business unit ▪ Permanent cessation or extensive disruption to business-critical functions ▪ Failure to deliver key objectives or services due to sustained workforce unavailability
4. Major	5 to 10% of EBITDA	▪ Business critical applications down for 4 – 36 working hours	▪ Loss of accreditation or other regulatory incident that impacts operational ability at a Business Unit or Campus Level	▪ Permanent physical or psychological injury or condition (able to return to work); or long-term treatment and/or lost time > 3 months	▪ Negative media (TV, Newspaper) coverage lasting up to 3 days day ▪ Adverse social media lasting up to 2 weeks ▪ Significant shareholder dissatisfaction voiced	▪ Loss of operations at multiple sites and/or regions ▪ Short term cessation or extensive disruption to business-critical functions (up to one month) ▪ Uncertain delivery of key objectives or services due to significant workforce unavailability ▪ External data breaches
3. Moderate	3 to 5% of EBITDA	▪ Business applications down for 2 - 4 working hours	▪ Loss of accreditation or other regulatory incident that impacts operational	▪ Short term physical or psychological injury, condition; or treatment and/or lost	▪ Negative media (TV, Newspaper) coverage lasting a single day ▪ Adverse social media lasting up to 1 week	▪ Loss of operations at single site ▪ Significant reduction in ability to deliver business critical

			ability at a Campus ▪ Registration /Accreditation with Conditions notice issued by ASQA and other accreditation bodies.	time < 3 months	▪ Formal complaint lodged to ombudsman or other regulatory body	functions (up to one week) ▪ Late or poor-quality delivery of key objective or service due to temporary workforce unavailability
2. Minor	▪ 1 to 3% of EBITDA	▪ Business critical applications down less than 2 working hours	▪ A dispute that can be resolved through formal mediation ▪ Non-compliance with compulsory administrative or legal processes that can be resolved easily with dialogue	▪ Physical or psychological injury requiring first aid only, no lost time	▪ Isolated media coverage or social media discussions lasting no more than a day ▪ Multiple complaints from patients and/or referrers on the same issue dealt with routinely	▪ Reduction in ability to deliver business critical functions for 1 – 2 days, functions can be delivered elsewhere ▪ Loss of staff reduces service quality in the medium term (up to 2 weeks)
1. Insignificant	▪ 0 to 1% of EBITDA	▪ IT Systems not performing as desired	▪ Verbal complaint, no legal outcome ▪ A dispute that can be resolved through informal negotiation ▪ Non-compliance with low level non-compulsory administrative processes	▪ Non-medical treatment required (no first aid, no follow up with health practitioner)	▪ Minor complaint or issue raised by patient or referrer dealt with routinely	▪ Negligible impact to deliver business critical services within an individual workplace ▪ Loss of staff reduces service quality in the short term (up to 3 days)

Attachment B: Control

Control Effectiveness Rating	Weak	Controls are largely ineffective. They do not provide reasonable assurance that risks will not eventuate.
	Fair	Controls are partially effective in mitigating risk. Improvements are required to provide further assurance that the risk will not eventuate.
	Good	Most controls are designed correctly and are in place and effective. Minor control improvements could be made, but controls already mitigate risk to a tolerable level.
	Excellent	Nothing more to do except review and monitor existing controls. Controls are well designed for the risk, address the root causes and management believes that they are effective and reliable at all times. Controls effectively and efficiently mitigate risk to an optimal level.

Effectiveness Ratings, Likelihood Table and Risk Matrix

Control Effectiveness Rating	Weak	Controls are largely ineffective. They do not provide reasonable assurance that risks will not eventuate.
	Fair	Controls are partially effective in mitigating risk. Improvements are required to provide further assurance that the risk will not eventuate.
	Good	Most controls are designed correctly and are in place and effective. Minor control improvements could be made, but controls already mitigate risk to a tolerable level.
	Excellent	Nothing more to do except review and monitor existing controls. Controls are well designed for the risk, address the root causes and management believes that they are effective and reliable at all times. Controls effectively and efficiently mitigate risk to an optimal level.

Likelihood Assessment Table

Rating	Description
Almost Certain	High level of recorded occurrences and / or strong anecdotal evidence Would be expected to occur in the next 12 months
Likely	Some recorded occurrences and / or anecdotal evidence Could probably occur over a period of 1 to 3 years
Possible	Few, infrequent, recorded occurrences, or little anecdotal evidence Reasonable probability that it could occur over a period of 3 – 5 years
Unlikely	Plausible, but no recorded occurrences or anecdotal evidence May occur over a period of 5 – 10 years
Very Unlikely	Not impossible, but no recorded occurrences or anecdotal evidence May occur only in exceptional circumstances e.g., within 10 years

Risk Matrix

		Consequence				
		Insignificant (1)	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Severe (5)**
Likelihood	**Almost Certain (5)**	**MEDIUM (5)**	**HIGH (10)**	**HIGH (15)**	**VERY HIGH (20)**	**VERY HIGH (25)**
	Likely (4)	**MEDIUM (4)**	**MEDIUM (8)**	**HIGH (12)**	**HIGH (16)**	**VERY HIGH (20)**
	Possible (3)	**LOW (3)**	**MEDIUM (6)**	**MEDIUM (9)**	**HIGH (12)**	**HIGH (15)**
	Unlikely (2)	**LOW (2)**	**LOW (4)**	**MEDIUM 6)**	**MEDIUM (8)**	**HIGH (10)**
	Very Unlikely (1)	**LOW (1)**	**LOW (2)**	**LOW (3)**	**MEDIUM (4)**	**MEDIUM (5)**