RISK MANAGEMENT POLICY

1. Purpose

1.1 This document applies to the Innovative Institute of Australia, its courses, its clients (students), and its controlled entities (collectively, "IIA", "Institute", "the Institute", "we", "us", "our"), and to students.

1.2 The purpose of this policy is to

i. Identify, manage, and regularly review risks affecting compliance with standards, business development, students, and staff.

ii. Manage financial risks by maintaining a robust financial plan, along with appropriate monitoring and oversight of the financial position, performance, and cash flows.

iii. Establish and maintain a system for identifying, managing, and transparently disclosing real or perceived conflicts of interest.

iv. Provide a framework to measure the effectiveness of compliance strategies based on the assessed risk to expose the need for additional risk controls where required.

v. Provide a framework for all Institute staff to participate in decision-making on risk controls based on the agreed risk.

2. Definitions

2.1 Risk is the possibility of an event or condition occurring that may have a negative impact on an organisation's objectives, resources, reputation, or stakeholders. It combines two key factors:

i. Likelihood: The probability or chance of the event occurring.

ii. Consequence: The potential impact or severity of the outcome if the event does occur.

2.2 Effective risk management involves identifying these risks, assessing their likelihood and impact, and implementing controls to reduce the likelihood of occurrence and minimise the potential impact.

2.3 Conflict of interest occurs when an individual's personal, financial, or other interests interfere with, or have the potential to interfere with, their ability to make impartial and objective decisions in their professional role. Conflicts of interest can arise in situations where:

i. Personal gain: An individual stands to gain personally (financially, materially, or otherwise) from decisions or actions they make on behalf of their organisation.

ii. Relationships: Close personal relationships (such as with family or friends) could influence, or appear to influence, the person's decisions.

iii. Competing loyalties: The individual has obligations to another entity (like another employer, client, or organisation) that could compromise their loyalty to their primary organisation.

iv. Outside interests: An individual's external activities (such as outside employment, investments, or board memberships) may create competing interests or affect their ability to act in the best interests of the organisation.

v. Gifts or benefits: Receiving gifts, benefits, or favours from a third party that could influence decision-making or create an appearance of bias.

2.4 An education agent refers to an entity (in or outside Australia) that

vi. Engages in any of the following activities in relation to a provider:

A. The recruitment of overseas students, or intending overseas students;

B. providing information, advice or assistance to overseas students, or intending overseas students, in relation to enrolment;

C. otherwise dealing with overseas students, or intending overseas students; and

vii. is not a permanent full-time or part-time officer or employee of the Institute.

2.5 Agent Agreement refers to the agreement between the Institute and the agent, including the schedules.

2.6 CRICOS refers to the Commonwealth Register of Institutions and Courses for Overseas Students.

2.7 ESOS Act refers to the *Education Services for Overseas Students Act 2000 of the Commonwealth of Australia*.

2.8 National Code refers to the *National Code of Practice for Providers of Education and Training to Overseas Students 2018*.

2.9 Prospective student/applicant/client refers to a person who intends to become, or who has taken any steps towards becoming, an 'overseas student' or 'intending overseas student' as defined by the *ESOS Act*.

2.10 DHA refers to the Department of Home Affairs.

2.11 OSHC refers to the Overseas Student Health Cover.

2.12 eCoE refers to the electronic Confirmation of Enrolment.

2.13 2025 Standards for RTOs refers to the *National Vocational Education and Training Regulator (Outcome Standards for NVR Registered Training Organisations) Instrument 2025*.

3. Policy

3.1 Risk management is intended to promote high-quality training and assessment, and to be analysed against the compliance requirements, focusing on

i. Outcome Standards for Registered Training Organisations 2025
ii. Compliance Requirements for Registered Training Organisations 2025
iii. Credential Policy for Registered Training Organisations 2025

iv. Financial Viability Risk Assessment Requirements 2021

v. Data Provision Requirements 2020

vi. Disability Standards for Education 2005

vii. Relevant legislative obligations, including but not limited to:

A. National VET Regulator Act

B. Fair Trading law

C. Privacy law

D. Work Health and Safety law

E. Employment law

F. Anti-discrimination law

G. Consumer protection law

3.2 Financial risks: The CEO is responsible for preparing a financial forecast on a calendar-year basis, supported by an annual review of market and break-even analyses to ensure the Institute delivers services that support financial viability. An Annual Financial Delivery Plan is finalised by mid-November.

i. Financial forecast for the following calendar year. To include market analysis and course break-even analysis – By 15th October

ii. Annual Delivery Planning Meeting – By 31st October

iii. Financial year reporting by 15th November

iv. Annual Delivery Plan finalised – By 15th November

3.3 Financial risk: The CEO is responsible for ensuring financial stability, allocating resources efficiently, and planning for future growth or needs. The Institute will identify potential financial risks and develop contingency plans to address them, with a focus on delivering courses that support our financial stability.

3.4 Financial risk: The CEO is responsible for monitoring the Institute's financial performance, including cash flow, and meeting with accounting advisors to stay informed about the Institute's financial position and its impact on the delivery of training and assessment.

3.5 Conflicts of interest: All staff must understand the Institute's Conflict of Interest Policy, be responsible for avoiding conflicts of interest, and promptly and in good

faith disclose any conflict or potential conflict. All staff must complete a Conflict of Interest Disclosure Form before working with the Institute. The CEO will review disclosed conflicts to assess potential impacts on objectivity, confidentiality, or fairness. Depending on the nature of the conflict, the following actions may be taken:

i. The individual may be removed from decision-making related to the conflict.
ii. The individual may be asked to resolve the conflicting financial interest.

3.6 Third-party arrangement: Each third-party arrangement presents a different level of risk to the Institute's compliance requirements. This risk is influenced by the complexity of each individual arrangement regarding the scope of services delivered, the commercial arrangement, and the type of third-party entity.

3.7 Review identification: Risks are identified through the following methods

i. An annual risk assessment identifies potential risks within the Institute's activities, processes, and environment.

ii. The Institute encourages staff, trainers, and students to report risks or concerns as they identify them.

iii. Routine inspections of training facilities and equipment to identify hazards and potential risks.

iv. Review past incidents, complaints, and feedback to identify risks.

3.8 Risk Assessment: In this policy, the risk assessment focuses on management and compliance risks, aims to prevent non-compliance, evaluates the effectiveness of self-assurance strategies, and supports informed decisions that balance quality and efficiency. All assessments must be recorded using the Risk Assessment Form.

3.9 Risk Assessment: The Institute has two core objectives: delivering high-quality services that meet best-practice regulatory standards, and operating efficiently to ensure financial viability and growth. While these priorities can compete, risk assessment and management provide the framework to balance quality and profitability through informed decision-making.

3.10 Risk Assessment: The following methods ensure that all staff understand risk management.

v. **Identify the risk criteria**. The Institute will conduct a planned risk assessment to identify specific regulatory requirements and focus on one at a time.

vi. **Confirm the risk context**. The Institute will have a deep discussion of compliance requirements and recognise the unique aspects of the operating context that may inform our assessment of risk, such as student numbers, locations, modes of delivery, funding sources, types of clients, numbers and capabilities of staff, etc.

vii. **Brainstorm the risk**. Once the Institute has confirmed the regulatory requirement and established the operating context, it then brainstorms the possible negative impacts that could occur if we fail to comply with the requirement (the risks). What could happen if the Institute is non-compliant? Non-compliance may affect the Institute's registration with the national regulator; it may negatively impact the service the student receives; the Institute may suffer a loss of reputation in the market; there may be a financial loss, etc. It is important to consider these risks, big and small, and not to get stuck just identifying the same risks every time. What are the specific risks that relate to each requirement?

viii. **Identify current controls**. After understanding the risks, the Institute will take effective measures to mitigate them. Before assessing the likelihood and consequences of these risks, it is important to review the existing controls we have in place and to determine whether they are effective.

ix. **Rate the risk**. The Institute uses the likelihood and consequence tables and its criteria to identify potential non-compliant. The Institute then uses the assessed likelihood and consequences, along with the Risk Evaluation Matrix, to rate the risk. As an example, if the Institute had a likelihood of “Possible” and a consequence of “Major”, we would rate the risk as “High Risk”.

x. **Risk acceptance**. The Institute will not accept a risk level that exceeds

Moderate. If the assessed risk rating is "High Risk" or "Extreme Risk", additional risk controls would be needed to bring the risk rating down to Moderate or lower. This is where the Institute needs to make decisions about quality vs. efficiency. The challenge is to identify additional risk controls that are smart and efficient whilst minimising the impact on students and avoiding additional heavy work processes for staff. This often requires a full consideration of the work process and identifying the point in the process where we can improve to reduce the likelihood of a risk eventuating.

xi. **Identify additional controls**. Decreasing the consequences of a risk event often involves implementing resilience strategies that the Institute implements after the risk eventuates, such as an IT systems recovery plan if the IT system is taken offline or is subject to a security breach. From this perspective, consequence reduction strategies can be considered "reactive" to a risk that has already eventuated. In contrast, likelihood reduction strategies can be considered "proactive" to prevent the risk from ever occurring.

xii. **Work process**. It is important to establish a work process and consider opportunities to improve it. Work processes are commonly comprised of the following components:

A. Inputs to the work process, such as learning materials, assessment tools, IT systems, equipment, facilities, consumables, etc.

B. Skills, knowledge and attitude of those performing the work.

C. Supervision or oversight of the work being performed.

D. Outputs that are produced in the performance of the work.

E. The work process that both precedes and follows the work being performed (upstream / downstream work process).

F. Policies and procedures that guide how the work should be performed.

G. Forms, tools, templates, checklists, and diagrams that support the work.

H. IT systems are used in the performance of the work process.

I. Training and development in support of those performing the work.

J. Quality controls or quality review of the work.

K. Timeframes or deadlines relating to the work.

L. Documentation and record keeping of the work.

M. Reporting arrangements relating to the work.

N. Feedback and continuous improvement of the work.

xiii. When considering strategies to reduce the likelihood or consequences, the above components, which are present in almost all work, are worth considering, identifying additional controls that both support quality work outcomes and are efficient. The objective is to control risk to a moderate level or below whilst also supporting the Institute's productivity.

xiv. **Rate the risk again**. If the Institute decides to take control before a high-risk rating, the Institute should re-rate the risk to determine how the additional controls have influenced the rating. If the risk is still considered above Moderate, the Institute should review the previous steps and consider what additional controls could be applied. If the risk is on Moderate or below, the Institute should record this note for the final risk rating. This final risk rating is referred to as the “residual risk”. This is the risk that remains even after all controls have been implemented.

xv. **Implement new controls**. Following a risk assessment, the Institute will have identified new risk controls that were agreed upon. These new controls need to be developed into the current operating arrangements, introduced to those responsible for implementing them and implemented. This is to be achieved through the continuous improvement process. Following a risk assessment, the outcomes or recommendations that emerged are to be recorded in the risk assessment record, raised as an opportunity for improvement using the Continuous Improvement Report, and referred to the regular management meeting for further consideration and action.

xvi. **Respect**. When a risk assessment activity is organised, it will usually involve reviewing multiple risk criteria in one day. There are often too many to complete within the available time, so it is important to make the most of the time and work through the risk assessment for each criterion efficiently. This means staying focused, minimising any unrelated chatter, and not getting bogged down in points that do not have a big influence on the outcome. Here are some guidelines to follow when organising and participating in a risk assessment:

A. Clearly state objectives and boundaries at the start, reminding everyone to stay focused.

B. Assign a facilitator to actively manage and redirect discussions.

C. Use a structured agenda for the day and follow it strictly.

D. Set and enforce clear time limits for assessing each risk criterion.

E. Use a 'parking lot' to capture side issues for later consideration.

F. Prioritise critical risks early and focus on them first.

G. Encourage participants to provide brief, concise contributions.

H. Gently but firmly redirect conversations back on track when they drift.

I. Agree on ground rules for managing discussions and interruptions.

J. Treat each other with respect and value each person's input.

xvii. The following table provides some examples of consequence reduction strategies (reactive strategies) and likelihood reduction strategies (proactive strategies):

Examples of Likelihood reduction (proactive) strategies	**Examples of Consequence reduction (reactive) strategies**
● Improving the inputs to a process, such as the learning content or assessment tools. ● Providing training to staff performing tasks to improve performance. ● Introducing work aids such as checklists or technology tools. ● Introducing quality control points to ensure outcomes being reported are valid and accurate. ● Introduce quality review points to evaluate the performance of an ongoing process. ● Establishing policy and procedure to support work performance. ● Introducing decision controls, such as limited authority or delegation.	● Having a contingency plan for when a trainer is not available such as a casual replacement trainer who can cover. ● Establishing emergency action procedures in the event of a building emergency. ● Putting in place first aid procedures and first aid equipment to respond to an accident or injury. ● Having continuity arrangements to carry on with service delivery if normal arrangements are interrupted, such as moving training online. ● Establishing suitable insurance coverage for public liability, loss and damage or volunteer protection.

• Establishing timeframes for work components or deadlines. • Establishing reporting arrangements to support decision-making.	• Having access to counselling services in the event of a traumatic event. • Establishing an IT system backup and recovery arrangement in the event of an IT system failure.

3.11 Work Health and Safety (WHS) / Occupational Health and Safety (OHS). WHS/OHS risks are reviewed regularly across all campus facilities. Any non-compliance leads to immediate action or suspension of activities. Staff and students are trained in workplace safety and reporting procedures.

3.12 Public liability insurance. The Institute must hold public liability insurance that covers all the organisation's operations for the entire period in which the organisation is registered. Public liability insurance, along with other relevant insurance, is an important risk-reduction strategy to mitigate the likely consequences of a risk eventuating. The CEO is responsible for establishing ongoing public liability insurance coverage for the Institute, retaining a record of it, and being able to produce it on request. The following considerations are to be given to the level of public liability insurance that the Institute requires:

xviii. Industry type and risk profile.

xix. Regular business activities and interactions.

xx. Potential for injury, damage, or claims.

xxi. Historical claim frequency.

xxii. Contractual or regulatory insurance requirements.

xxiii. Annual business turnover and financial scale.

xxiv. Number of employees and subcontractors.

xxv. Industry standards for insurance coverage.

xxvi. Business location and premises condition.

xxvii. Maximum financial exposure from potential claims.

xxviii. Client or customer coverage expectations.

xxix. Cost and affordability of insurance premiums; and

xxx. Professional recommendations from insurance advisors.

3.13 Record keeping. Risk assessments are documented and stored using the approved template.

4. Measures

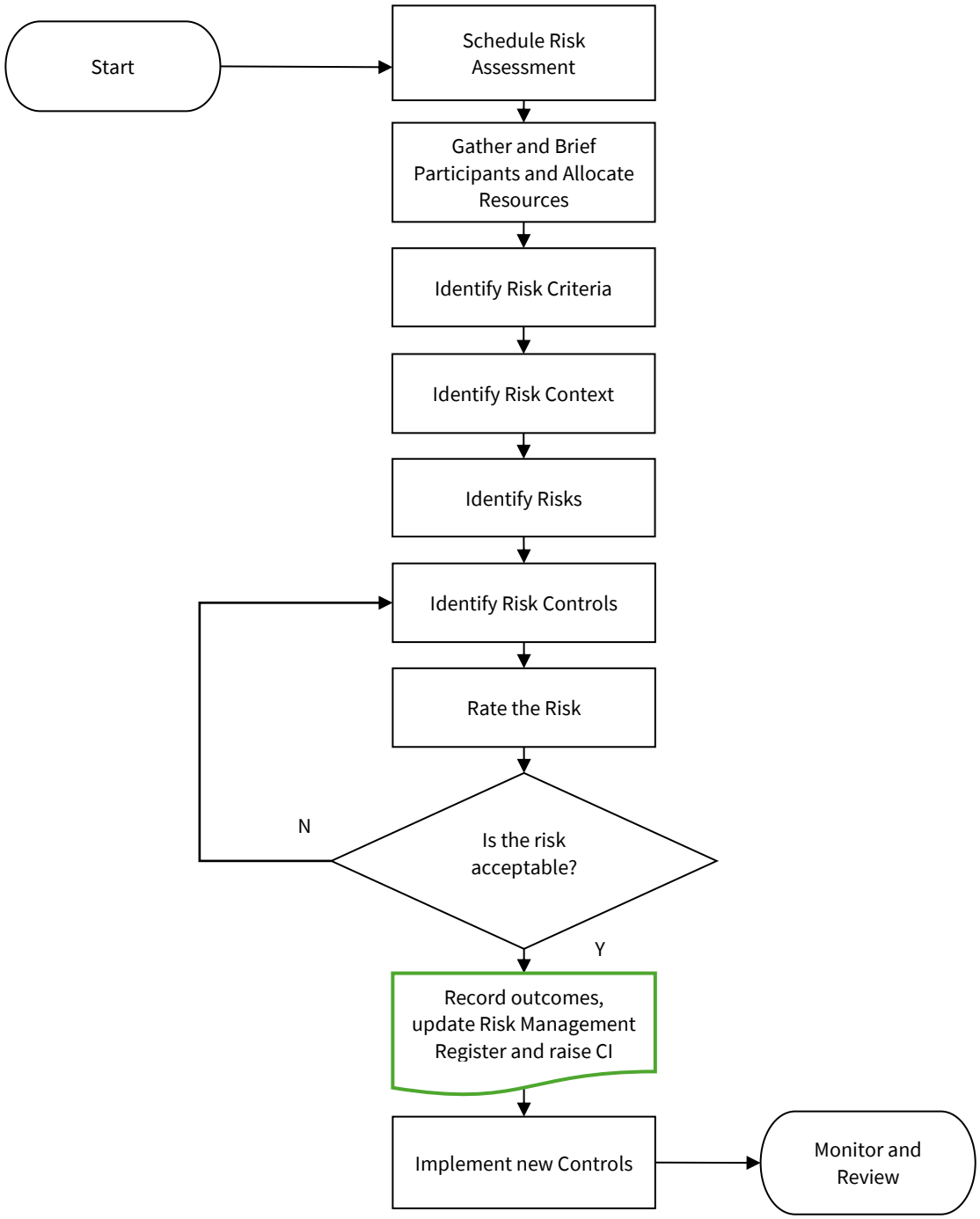
Steps		Person/s responsible
i.	**Schedule risk assessment** Schedule the activity well in advance to allow people to plan and be available to participate. Identify the personnel to participate based on their knowledge of the current operation and their ability to contribute. Consider inviting additional staff members who would benefit from exposure to the activity for their professional development. Identify the risk criteria to be prioritised on the day. Organise access to relevant forms and the current risk register for reference. Ensure the availability of materials to support the activity, including post-it notes, whiteboard, butcher's paper, easel, stationery, computer, and projector. Organise a morning tea and a lunch as an incentive to encourage personnel to attend.	CEO

ii.	**Brief participants and allocate resources** Brief participants and allocate resources. Provide a brief reminder of the risk assessment process and the ground rules for the day. Remember to: ● Clearly state objectives and boundaries at the start, reminding everyone to stay focused. ● Set and enforce clear time limits for the assessment of each risk criteria. ● Explain the use of a 'parking lot' to capture side issues for later consideration. ● Identify the priority risk criteria to address. ● Encourage participants to provide brief, concise contributions. ● Remind everyone to treat each other with respect and value the input of each person.	CEO
iii.	**Identify the risk criteria** Identify the regulatory requirement and establish clear risk assessment criteria. Begin by selecting one specific regulatory requirement, clearly defining the criteria against which risks will be assessed. Typically, this involves focusing on a single clause from a regulatory standard relevant to the Institute.	CEO and participants
iv.	**Confirm the risk context** Engage in a thorough discussion to ensure all stakeholders understand the selected regulatory requirement, defining clearly what compliance look like. Consider the operational factors relevant to this regulatory requirement, such as the number and diversity of students, delivery modes, delivery locations, funding sources, client types, and staff capabilities, as these elements can influence how compliance is interpreted and implemented.	CEO and participants

v.	**Identify the risks** Identify and discuss all possible risks or negative impacts arising from non-compliance with the regulatory requirement. Consider the identified risks, risks to registration with the national regulator, adverse effects on student services, potential reputational damage, financial losses, and other specific issues relevant to the chosen requirement. Encourage input to capture a comprehensive list of risks, avoiding repetitive or narrow considerations.	CEO and participants
vi.	**Identify current risk controls** Identify existing preventive or corrective measures currently in place to manage identified risks. This includes assessing the competence and training of staff, effectiveness of existing policies and procedures, adequacy of resource allocation, quality assurance practices, and management oversight. Evaluate whether these current controls are functioning effectively and reliably.	CEO and participants
vii.	**Rate the risk** Using the predetermined likelihood and consequence rating tables, work together to determine the likelihood and consequence of potential non-compliance occurring, considering existing control measures. Reach consensus as a group, valuing each participant's input. Apply these evaluations to the Risk Evaluation Matrix to establish the initial risk rating (e.g., High, Moderate, or Low).	CEO and participants
viii.	**Is the risk acceptable** The Institute does not accept a risk rating that is higher than Moderate. A risk rating of High or Extreme are unacceptable. In such cases, additional control measures must be identified and implemented to reduce risk to an acceptable level.	CEO and participants

ix.	**Identify additional risk controls** Identifying additional risk controls involves considering the relevant work process and distinguishing between reduction strategies for both likelihood and consequence.	CEO and participants
x.	**Rate the risk again** Once additional control measures have been identified and agreed upon, reassess the risks using the same likelihood and consequence rating tables and the Risk Evaluation Matrix. If risks remain above the acceptable level, repeat the process of identifying additional controls. Continue this iterative process until reaching an acceptable residual risk rating (Moderate or lower), clearly documenting the final risk rating and agreed measures. Clearly record the outcomes of the risk assessment, including final residual risk ratings, all agreed-upon control measures, and assigned responsibilities.	CEO and participants
xi.	**Report new risk controls via the Continuous Improvement process** Record the final recommendations and outcomes in the Risk Assessment Form and raise a Continuous Improvement Report for all outcomes for consideration at a future management meeting. Update the Risk Management Register.	CEO
xii.	**Move on to the next criteria and repeat the process** Once you have completed the risk assessment process relevant to that criteria, identify the next criteria and move straight on to repeat the process.	CEO and participants

5. Flow chart


Start
Schedule Risk Assessment
Gather and Brief Participants and Allocate Resources
Identify Risk Criteria
Identify Risk Context
Identify Risks
Identify Risk Controls
Rate the Risk
Is the risk acceptable?
N
Y
Record outcomes, update Risk Management Register and raise CI
Implement new Controls
Monitor and Review

VERSION HISTORY

Version Number	Date	Summary of changes
1.0	September 2021	New policy
2.0	July 2025	Revised and updated to include the changes according to the Standards for Registered Training Organisations (2025).
3.0	December 2025	Revised and updated to include the changes according to the ESOS 2000 Act.