RISK MANAGEMENT POLICY

Policy/Document Approval Body:	Governance Board
Date Created:	4 March 2010
Policy Custodian:	Dean of Engineering
Policy Contact:	Accreditation and Compliance Manager
File Location:	W:\Data - ALL.Standard\Policies and Procedures\EIT Policies and Procedures
Location on EIT website:	http://www.eit.edu.au/organisation-policies
Review Period:	Three years from date of commencement
Revision No:	10
Date of Revision:	23 November 2021
Date Approved:	16 December 2021
Date Commenced:	17 February 2022

1.0 Purpose

The purpose of this procedure is to set out the way EIT intends to manage the risks involved in all of its activities that maximise opportunities and minimise adversity. Effective risk management requires:

- a strategic focus.
- forward thinking and active approaches to management.
- a balance between the cost of managing risk and the anticipated benefits.
- contingency planning in the event that mission critical events are realised.

Risk management also provides a system for the setting of priorities when there are competing demands on limited resources

2.0 Scope

This policy applies to all the professional staff, students and academics currently attending or working for EIT or who have attended in the past. It relates to risk management within EIT.

3.0 Objectives

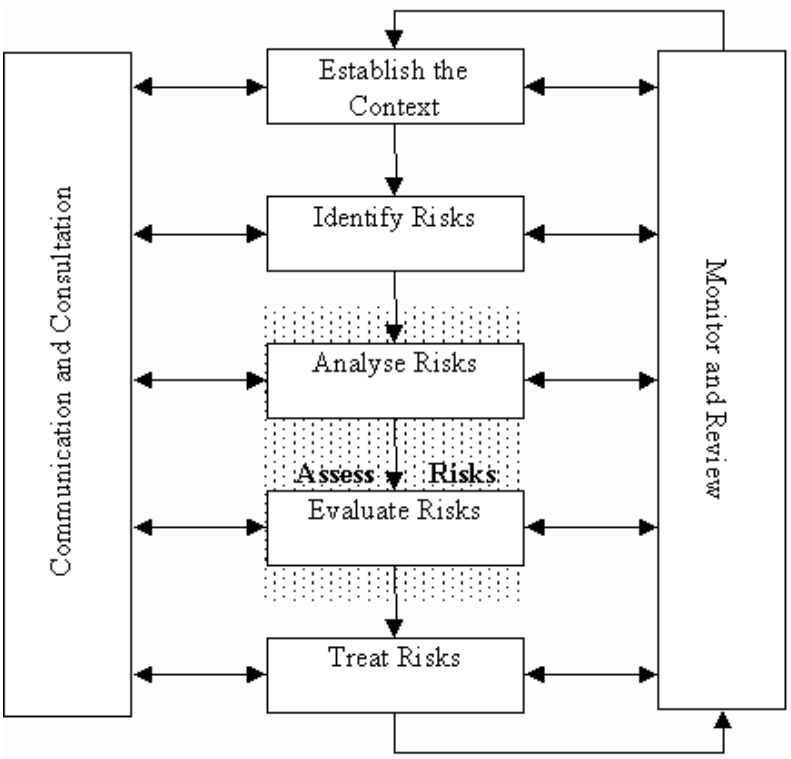
Risk Management is the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects within EIT. Risk is inherent in all academic, administrative and business activities. Every member of EIT's community continuously manages risk. Formal and systematic approaches to managing risk have evolved and they are now regarded as good management practice. As a consequence, EIT acknowledges that the adoption of a strategic and formal approach to risk management will improve decision-making, enhance outcomes and accountability.

4.0 Implementation

EIT will maintain procedures to provide a systematic view of the risks faced in the course of our academic, administrative and business activities. Where appropriate these procedures will be consistent with the Standards Australia risk management standard, AS/NZS ISO 31000:2009, Risk management - Principles and Guidelines. This will:

- **Establish a context**. This is the strategic, organisational and risk management context against which the rest of the risk management process in EIT will take place.
- **Identify Risks.** This is the identification of what, why and how events arise as the basis for further analysis.
- **Analyse Risks.** This is the determination of existing controls and the analysis of risks in terms of the consequence and likelihood in the context of those controls. The analysis should consider the range of potential consequences and how likely those consequences are to occur. Consequence and likelihood are combined to produce an estimated level of risk.
- **Evaluate Risks**. This is a comparison of estimated risk levels against pre-established criteria. This enables risks to be ranked and prioritised.
- **Treat Risks.** For higher priority risks, EIT is required to develop and implement specific risk management plans including funding considerations. Lower priority risks may be accepted and monitored.
- **Monitor and Review.** This is the oversight and review of the risk management system and any changes that might affect it. Monitoring and reviewing occurs concurrently throughout the risk management process.
- **Communicate and Consult.** Appropriate communication and consultation with internal and external stakeholders should occur at each stage of the risk management process as well as on the process as a whole.

Schematically, the risk management process is depicted in the following diagram.



4.1 Responsibility for Risk Management

General

Every staff member of EIT is responsible for the effective management of risk including the identification of potential risks. Management (both academic and administration/operations) is responsible for the development of risk mitigation plans and the implementation of risk reduction strategies.

Dean of Engineering/ CEO

The Dean is accountable for ensuring that a risk management system is established, implemented and maintained in accord with this policy. Assignment of responsibilities in relation to risk management is as defined in this policy. The Dean is also responsible for reporting progress on identification and mitigation of risks via an annual report to the Governance Board or at a greater frequency, if required.

Governance Board

The Governance Board is accountable for the oversight of the processes for the identification and assessment of the risks and reviewing the outcomes of the risk management processes and actions in the Risk Register.

Collectively it is responsible for:

- The formal identification of strategic risks that impact upon EIT's mission.
- Allocation of priorities.
- The development of strategic risk management plans.
- Reviewing progress against agreed risk management plans and communicating this to EIT.

Academic Board

The Academic Board is accountable for the oversight of identifying academic risks and providing advice to the Governance Board for inclusion in EIT's Risk Register.

Finance Manager

The Finance Manager (also referred to as the Accountant) is accountable for EIT's insurance portfolio and financial processes and will take responsibility for relevant risk management issues.

Human Resources Manager

The Human Resources Manager is accountable for the occupational health and safety and workers compensation portfolio, procedures and administration.

Accreditation and Compliance Manager

The Accreditation and Compliance Manager is responsible for monitoring compliance risk and meticulously recording the narrative of risk and disseminating the assessment to all role players.

Generic Sources of Risk and their Areas of Impact

Identifying sources of risk and areas of impact provides a framework for risk identification and analysis. A generic list of sources and impacts will focus risk identification activities and contribute to more effective risk management.

Generic Sources of Risk

Each generic source has numerous components, any of which can give rise to a risk. Generic sources of risk include:

- Commercial and legal relationships including, but not limited to contractual risk, product liability, professional liability and public liability.
- Economic circumstances. These can include such sources as profitability, bad debts, student loan arrangements, currency fluctuations, interest rate changes, taxation and changes in fiscal policy.
- Human behaviour such as riots, strikes and sabotage.
- Natural events. These can include fire, water damage, earthquakes, vermin, disease and contamination.
- Political circumstances such as legislative changes or changes in government policy that may influence other sources of risk.
- Technology and technical issues. Examples of this include innovation, obsolescence, equipment failure and reliability.
- Management activity and control such as poor safety management, the absence of control and inadequate security.
- Individual activity including, misappropriation of funds, fraud, vandalism, illegal entry, information misappropriation and human error.

Areas of Impact

A source of risk may impact on one area only or on several areas at EIT. Areas of impact include:

- Asset and resource base including personnel.
- Revenue and entitlements.
- Costs both direct and indirect.
- People.
- The community.
- Performance.
- Strategy and business planning.
- Timing and schedule of activities.
- The environment.
- Intangibles such as reputation, goodwill and the quality of life.
- Organisational behaviour.
- Governance.
- Regulation and compliance.
- Reputation.
- Academic quality and integrity.

4.2 Risk Assessment

Risk assessment is undertaken across the areas of impact or categories of risk using judgements for managing identified risks and their impact on the organisation. A Risk Management Register records the key risks identified together with controls and their treatment. Initially risks are assessed on an inherent basis, considering the likelihood and impact of the risk without taking into account the controls in place. This helps to understand the importance of controls in mitigating risk. For each risk identified, there are single or multiple controls in place to address the risk and prevent future reoccurrence. The Risk Management Register is monitored and reviewed regularly.

4.2.1 Quantitative Risk Approach

This section outlines how to apply ratings to the risks identified.

Inherent Risk

The likelihood of the risk occurring needs to be established, as well as the impact rating, should the risk occur. The inherent risk rating represents the level of risk in the absence of a control environment and is arrived at after measuring the likelihood and the impact of an event occurring. The Likelihood and Impact Rating are multiplied together to obtain the Inherent risk rating, and then entered into the Risk Management Register.

Likelihood of Risk

1 Very Low
2 Low
3 Medium
4 High
5 Very High

Illustrative Likelihood Scale		Description	Occurrence	Probability
Very High (almost certain)	**5**	Expected to occur in most circumstances	Multiple / 12 months	> 80%
High (likely)	**4**	Will probably occur in most circumstances	Once / 12 months	61 – 80%
Medium (possible)	**3**	Might occur within a 5-year time period	Once / 12 months – 5 years	41 – 60%
Low (unlikely)	**2**	Could occur during a specified time period	Once / 5 – 10 years	21 – 40%
Very Low (rare)	**1**	May only occur in exceptional circumstances	Once / > 10 years	< 20%

Impact of Risk

1 Insignificant
2 Minor
3 Moderate
4 Serious
5 Very Serious

The following table is used to guide the assessment of impact on each identified risk. It does not provide examples of all categories or risks contained in this plan.

Category of Risk	Illustrative Impact Scale				
	Insignificant 1	**Minor 2**	**Major 3**	**Critical 4**	**Extreme 5**
Compliance or Legislation	Oversight on reporting activity that is under control. No penalty, imprisonment or accountability implications.	Minimal non-compliance to relevant regulation or legislation. Penalty may be incurred. Some accountability implications, but would not affect key operations.	Medium level of non-compliance with regulation or legislation. Possible jeopardy to registration and accreditation, penalty and/or imprisonment.	Non-compliance with regulation or legislation. High possibility of loss of registration and accreditation or individual/corporate penalty and/or imprisonment.	Non-compliance with regulation or legislation affecting closure of business activities and/or large penalty (individual/corporate) and/or imprisonment.

Category of Risk	Illustrative Impact Scale				
	Insignificant 1	**Minor 2**	**Major 3**	**Critical 4**	**Extreme 5**
Damage to Reputation	Minimal adverse publicity in local press. Letters received and printed but no further action taken. Reputation would remain intact.	Adverse publicity in local/state press. Letters to Editors, with follow up comments from the readership or interested parties. Public perception may alter slightly with no significant damage.	Extended negative local/state, plus national media coverage. Requirement to manage key stakeholders. Considerable adverse public reaction resulting in some damage to reputation.	Longer-term local/state and nationwide coverage. Increase focus on management of a broader group of stakeholders. Adverse public reaction resulting in major disruption.	Extended negative coverage. Requirement to implement a communication plan for all stakeholders. Major adverse repercussions affecting public standing of the Institution.
Operations	No interruption to service. Inconvenience to localised operations.	Some disruption manageable by altered operational routine.	Disruption to key operational areas. Revised planning may be needed to overcome issue.	Significant disruption to teaching / course schedules or key business activities for up to **one week**. Operations would be severely affected, possibly causing depletion of resources.	Critical disruption to services or key business activities for **more than one week**. Operations would be dysfunctional.
Financial	Less than $10,000 No disruption and no need to divert resources from core activities.	$10,000 - $50,000 Quick recovery with no need to divert resources from core activities	$50,000 - $100,000 Gradual recovery with need to divert some resources from core activities.	$100,000 - $200,000 Complex recovery with need to re-evaluate resource allocations and possibly jeopardise financial position.	Greater than $200,000 Recovery would be extremely difficult and there would be significant financial losses.

Category of Risk	Illustrative Impact Scale				
	Insignificant 1	**Minor 2**	**Major 3**	**Critical 4**	**Extreme 5**
WH&S	Incident – no lost time. No injury.	Injury – no lost time. First aid required.	Injury – lost time with possible compensation claim. Medical treatment required.	Fatality or serious injury/stress resulting in hospitalisation.	Multiple fatalities (not natural causes).

An illustrative example of actions arising are:

a. **A Low residual risk** score of 3 or less is considered acceptable to the Institute and will require no further action, other than to ensure the relevant controls are operating effectively. Managers should however review the controls for low risk areas carefully.

b. **A Medium residual risk** score of 4 to 9 may require the implementation of additional controls and reporting to the CEO, unless other qualitative data indicates otherwise.

c. **A High to Extreme residual risk** score of 10 or more will require the implementation of additional controls; prioritization; and reporting to the Governance Board.

Residual Risk

A Residual Risk rating is given after the level of internal control has been assessed. The Risk Priority Status is then applied to determine the urgency of the actions that are required. The table below displays the Residual Risk Ranking.

	Impact				
Likelihood	**Insignificant 1**	**Minor 2**	**Major 3**	**Critical 4**	**Catastrophic 5**
5 – Almost Certain	Medium 5	High 10	High 15	Extreme 20	Extreme 25
4 – Likely	Medium 4	Medium 8	High 12	High 16	Extreme 20
3 – Possible	Low 3	Medium 6	Medium 9	High 12	High 15
2 – Unlikely	Low 2	Low 4	Medium 6	Medium 8	High 10
1 – Rare	Low 1	Low 2	Low 3	Medium 4	Medium 5

4.3 Risk Treatment Options

4.3.1 Actions to Reduce or Control Likelihood

These can include but are not limited to:

- Review and compliance programs.
- Contract conditions.
- Formal reviews of requirements, specifications, design, engineering and operations.
- Inspection and process controls.
- Investment and portfolio management.
- Project management.
- Preventative maintenance.
- Quality assurance, management and standards.
- Research and development; technological development.
- Structured training and other programs.
- Effective governance processes.
- Strategic, operational and tactical planning processes;
- Supervision.
- Testing.
- Organisational arrangements.
- Technical controls.
- Careful monitoring, assessment and synthesis of multiple government directives on disease, security and supply chain interruptions.

4.3.2 Procedures to Reduce or Control Consequences

These can include but are not limited to:

- Contingency planning.
- Contractual arrangements.
- Contract conditions.
- Design Features.
- Business continuity and disaster recovery plans.
- Engineering and structural barriers.
- Fraud control planning.
- Minimising exposure to sources of risk.
- Portfolio planning.
- Pricing policy and controls.
- Separation or relocation of activities and resources.
- Succession planning.
- Insurance.
- Public Relations.
- Ex Gratia Payments.

4.3.3 Risk Management Documentation

To manage risk properly, appropriate documentation is required. EIT staff members conducting or accountable for the activity shall in the first instance conduct the risk assessment and complete the documentation. The risk assessment and documentation is to be reviewed and accepted by the manager or next in line supervisor of the area conducting or accountable for the activity. Where technical expertise or central authority is required, the risk assessment will also be reviewed and countersigned by that party.

For each risk identified, a risk register records:

- Category and source.
- Nature or issue.
- Risk indicators.
- Existing controls/risk mitigation.
- Likelihood and impact.
- Inherent risk rating.
- Residual risk rating.
- Further treatment actions/assessment/.
- Responsible person.

A risk treatment and action plan, if required for extreme residual risk ratings, documents the managerial controls to be adopted and contains the following information:

- Who is responsible.
- What resources are to be used.
- Budget allocations.
- Implementation timetables.
- Details of the control mechanism.
- Frequency of review of compliance with the treatment plan.

5.0 Definitions

Controls	The processes, policies and procedures used to govern EIT's work or any additional controls or mitigating actions taken to deal with a particular situation.
Inherent Risk	The level of risk faced by an organisation before any internal controls are applied.
Likelihood	A qualitative description or synonym for probability or frequency.
Residual Risk	The level of risk faced by an organisation after internal controls have been applied.
Risk	The probability of something happening that will have an impact on the achievement of EIT's objectives. Risk is measured by multiplying consequences and likelihood.
Risk Assessment	The overall process of risk analysis and evaluation.
Risk identification	The process of determining what can happen, why and how.

Risk Indicators	Provide the risk owner with early warning that action may be required to mitigate the risk through stronger internal control or, if it is outside EIT's control to be aware of it and closely monitor. These indicators should be measurable and underpinned with data.
Risk Management	The culture, processes and structures that are directed towards the effective management of current and potential opportunities and adverse effects within EIT.
Risk Management Process	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
Risk Management Register / Risk Management Plan	The summary report of all individual risks within each assessment, which include; risk ratings (inherent and residual), level of control, risk decision, risk owner and summary of key controls and/or mitigating actions.
Risk Owner/ Person Responsible	An individual staff member, who is closely involved with the risk, is able to monitor the risk, initiate action if the risk becomes more serious.
Risk Tolerance	The amount of risk an organisation is prepared to tolerate before action is required.

6.0 Related Documents:

The following policies and procedures are related to this policy:

- EIT/IDC Contingency Plan.
- EIT Risk Management Register.

7.0 Essential Supporting Documents:

- AS/NZS 4360:2004 - Risk Management
- AS/NZS ISO 31000:2009, Risk management – Principles and guidelines.

The University of Cambridge's approach to risk management is the basis of this document together with the relevant ISO principles and guidelines. Naturally the specific risks and descriptions are different; but the general thrust and principles are applicable to EIT.

8.0 Accountabilities

The Governance Board is responsible for review and approval of this policy, with input from the Academic Board with regard to academic risk.

The policy is to be implemented via induction and training of staff and distribution to EIT's community.