

International Technical Institute

(01-8270)

**RISK MANAGEMENT POLICY AND PROCEDURE**

# Contents

1. [Introduction 3](#_bookmark0)
   1. [Purpose of the Policy 3](#_bookmark1)
   2. [Policy owner 3](#_bookmark2)
2. [Understanding Risk Management 3](#_bookmark3)
3. [Responsibility 3](#_bookmark4)
   1. [Board 4](#_bookmark5)
   2. [Chief Financial Officer 4](#_bookmark6)
   3. [Risk Owner 4](#_bookmark7)
   4. [General responsibilities 4](#_bookmark8)
4. [Risk management procedure 5](#_bookmark9)
   1. [Summary of procedure 5](#_bookmark10)
   2. [Risk management process 5](#_bookmark11)
   3. [Risk Management methodology 6](#_bookmark12)

[Appendix A – Risk Assessment Matrix and Risk Register 8](#_bookmark13)

BOARD APPROVED Page 2

# Introduction

# Purpose of the Policy

All activities undertaken by International Technical Institute (**ITI**) carry an element of risk. The exposure to these risks is managed through the practice of Risk Management. In managing risk, it is the Company's practice to take advantage of potential opportunities while managing potential adverse effects. Managing risk is the responsibility of everyone in the Company.

This policy outlines the Company’s risk management process and sets out the responsibilities of the Board, the CEO, the Audit and Risk Committee, the Director, senior management, and others within the Company in relation to risk management.

# Policy owner

The Chief Executive Officer and Director Compliance is the policy owner of the Risk Management Policy and Procedure for ITI. The Finance Manager will still have oversight over the risk management program for ITI.

# Understanding Risk Management

Risks have been described in terms of combination of the consequences of an event occurring and its likelihood of occurring.

Risk is the chance of something happening that will have an impact on objectives and risk management can be described as the culture, processes and structures that are directed towards realising potential opportunities whilst managing an adverse effect.

ITI’s risk management system is designed to identify the risks it faces and has measures in place to keep those risks to an acceptable minimum. The existence of risk presents both threats and opportunities to ITI.

Risk owners have been assigned responsibility for the identified risks in the Risk Register. ITI’s risk assessment matrix is used as the benchmark in planning and implementing the risk management measures. It takes into consideration the nature, scale, and complexity of the business.

The risk management process consists of the following main elements:

***Identify***: identify a risk (threats or opportunities) and document the risks captured by the risk register owner.

***Assess:*** the primary goal is to document the net effect of all identified threats and opportunities, by assessing:

* Likelihood of threats and opportunities (risks);
* Impact of each risk;
* Proximity of threats; and
* Prioritisation based on scales.

***Plan:*** preparation of management responses to mitigate threats and maximise opportunities.

***Implement:*** risk responses are actioned.

***Monitor and review:*** monitor and review the performance of the risk management system and changes to business initiatives.

***Communicate:*** provide regular reports to management team / Audit and Risk Committee at agreed times.

Risks are effectively managed by ITI through the effective implementation of various controls, which include:

* Board approved risk management framework;
* Documented policies and procedures;
* Maintenance of registers;
* Implementation of risk based systems and processes;
* Ongoing monitoring of regulatory obligations;
* Checklists to guide activities and project plans to record actions; and
* Internal and external reporting.

# Responsibility

# Board

The Board of ITI Limited, through the Audit and Risk Committee, has responsibility under its Charter to review and report to the Board that:

1. the Committee has, at least annually, reviewed the ITI’s risk management framework to satisfy itself that it continues to be sound and that ITI is operating with due regard to the risk appetite set by the Board, and effectively identifies all areas of potential risk;
2. adequate policies and processes have been designed and implemented to manage identified risks;
3. a regular program of audits is undertaken to test the adequacy of and compliance with prescribed policies; and
4. proper remedial action is undertaken to redress areas of weakness.

# Finance Manager

The Finance Manager of ITI has responsibility under this policy for:

* Monitoring compliance with this policy;
* Reporting to the Board on compliance with this policy;
* Developing, implementing, and monitoring systems, management of policies and procedures relevant to the business, including facilitating review by the executive on a regular basis; and
* Maintaining the risk register.

# Risk Owner

The risk owner (as noted in the Risk Register) is responsible for ensuring on a daily basis that the relevant operational procedures and controls implemented to treat each risk area are adequate and effective. If a control or procedure is not adequate and effective in treating the risk, the risk owner should report this, with a recommendation for an alternative risk treatment, to the Finance Manager for escalation to the Chief Executive Officer and Director Compliance and ultimately approval by the Board.

# General responsibilities

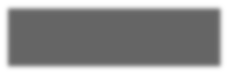
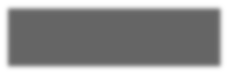
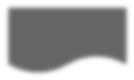
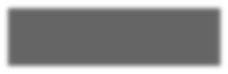
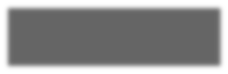
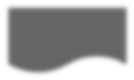
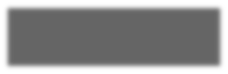
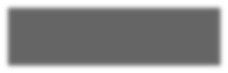
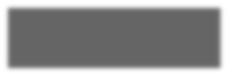
Every ITI staff member is responsible for effective management of risk including the identification of potential risks. Management is responsible for the development of risk mitigation plans and the implementation of risk reduction strategies. Risk management processes should be integrated with other planning processes and management activities.

Where there is legislation in place for the management of specific risks (such as Occupational Health and Safety) this Risk Management policy does not relieve ITI of its responsibility to comply with that legislation.

Managers are accountable for strategic risk management within areas under their control, including the promotion and training of the risk management process to staff.

# Risk management procedure

# Summary of procedure



**Risk Register Review**

**Risk Register Amended**

**Communicate and Consult**

**Analyse Risks**

Risk Assessment Matrix

Update Risk Register

**Treat Risks**

**Evaluate Risks**

**Monitor and Review**

**Identify Risks**

**Establish Context**

# Risk management process

The risk management system is dynamic and is designed to adapt to ITI’s developments and any changes in the risk profile over time. Compliance measures are used as a tool to address identified risks.

The risk management system is based on a structured and systemic process which takes into account ITI’s internal and external risks.

The main elements of the risk management process are as follows:

* **Communicate and consult** – communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.
* **Establish the context** – establish the external, internal and risk management context in which the rest of the process will take place – the criteria against which risk will be evaluated should be established and the structure of the analysis defined.
* **Identify risks** – identify where, when, why and how events could prevent, degrade, delay or enhance the achievement of ITI’s objectives.
* **Record risks** – document the risks that have been identified in the risk register.
* **Analyse risks** – identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk by analysing the range of potential consequences and how these could occur.
* **Evaluate risks** – compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.
* **Treat risks** – develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.
* **Monitor and review** – it is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement. Risks and effectiveness of treatment measures need to be monitored so that changing circumstances do not alter priorities.

ITI’s risks may come from any internal or external event which, if it occurs, may affect the ability to efficiently and effectively operate:

* **Internal risks** – those risks that specifically relate to ITI’s business itself and as such as generally within its control. They include risks such as employee related risks, including conduct related risks, strategic risks, and financial risks.
* **External risks** – those risks that are outside the control of ITI. They include risks such as market conditions, digital disruption, cyber-security, privacy and data breaches, sustainability, climate change and legislative change.

Risks are effectively managed by ITI through the effective implementation of various controls, which include:

* Board approved risk management framework;
* Maintenance of risk register; and
* Regular review of risks and controls, particularly as the business changes.

Risk management can be applied at many levels in an organisation. It can be applied at a strategic level and operational level. It may be applied to specific projects, to assist with specific decisions or to manage specific recognised risk areas.

# Risk Management methodology

The methodology adopted by ITI for managing and treating its risks can be defined as follows:

1. Document a risk management framework (ie the context)
2. Identify the general activities involved in running the business (ie risk categories)
3. Identify the risks involved in undertaking the specific business activity by asking the questions:
   1. What could happen?
   2. How and why could it happen?
4. Rate the likelihood of the business activity not being properly performed. Likelihood is assessed to the assumption that there are no existing risk management and compliance processes in place. It is assessed as either **Almost Certain**, **Likely**, **Possible**, **Unlikely** and **Rare**.
5. Rate the consequence of not properly performing the business activity - damage can be quantified in terms of financial loss to investors and/or ITI itself. It is assessed as **Catastrophic**, **Major**, **Severe**, **Serious and Minor**.
6. Assign the inherent risk rating based on a combination of the risk rating. Low and medium risks may be considered acceptable and therefore minimal further work on these risks may be required. The rating may be assessed as **Critical, High**, **Significant**, **Medium** and **Low**.
7. Decide whether a control (eg policy, procedure, checklist, reporting mechanism or account reconciliation) is necessary given the level of risk, based on likelihood and consequences and if so, identify control.
8. Assess whether the existing controls are adequate and allocate the responsibility of monitoring the control to treat the risk. This will integrate risk management and compliance to daily activities and facilitate appropriate control of operational risk.
9. Raise awareness about managing risks across the organisation through communicating the policy and responsibilities.
10. Routinely monitor and review ongoing risks so can risk can be effectively managed The Risk Assessment Matrix and Risk Register format are shown in Appendix A.

# Appendix A – Risk Assessment Matrix and Risk Register

**Risk Consequence Severity**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Consequence Type** | **Minor** | **Serious** | **Severe** | **Major** | **Catastrophic** |
| Financial Loss | < $1m | $1m-5m | $5m-$10m | >$10m | Threatens viability of Company |
| Reputation Loss |  |  |  |  |  |

**Likelihood Probability & Frequency**

|  |  |  |
| --- | --- | --- |
| **Likelihood Rating** | **Description** | **Probability** |
| Almost Certain | Known to happen often | > 95% |
| Likely | Could easily happen | 50% - 95% |
| Possible | Could happen & has occurred before | 15% - 50% |
| Unlikely | Hasn’t happened yet but could | 5% - 15% |
| Rare | Conceivable, but only in extreme circumstances | > 5% |

**Control Effectiveness**

|  |  |
| --- | --- |
| **Control Effectiveness** | **Description** |
| Effective | The control design meets the control objective and the control is operating the majority of the time |
| Partially Effective | The control design mostly meets the control objective and/or the control is normally operational but occasionally is not applied when it should be, or not as intended |
| Ineffective | The control design does not meet the control objective and/or the control is not applied or is applied |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minor** | **Serious** | **Severe** | **Major** | **Catastrophic** |
| **Medium** | **High** | **Critical** | **Critical** | **Critical** |
| **Medium** | **Significant** | **High** | **Critical** | **Critical** |
| **Medium** | **Medium** | **Significant** | **High** | **Critical** |
| **Low** | **Low** | **Medium** | **Significant** | **Critical** |
| **Low** | **Low** | **Medium** | **Medium** | **High** |

**Risk Assessment Matrix**

**5. Almost Certain**

**4. Likely**

**3. Possible**

**2. Unlikely**

**1. Rare**

**CONSEQUENCE**

**Likelihood Rating**

**LIKELIHOOD**

|  |  |
| --- | --- |
| Critical | Extreme risk - detailed research and management planning required at senior levels |
| High | High risk- immediate senior management attention needed |
| Significant | Significant risk - Senior management attention needed |
| Medium | Moderate risk - Management responsibility must be specified |
| Low | Low risk - Manage by routine procedures |

**Risk Assessment Template**

|  |  |  |  |
| --- | --- | --- | --- |
| **Area/Department** |  | **Risk Register ID** |  |
| **Date of Risk Assessment** |  | **Risk Category** |  |
| **Risk Owner** |  | **Assessment Conducted By** |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Establish the Context** | | **Risk Description** | | | | **Effectiveness of Controls** | | **Analysis** | **Evaluation** |
| **Objective** | **Context** | **Risk Source** | **Description** | | | **Current Control(s)** | **Control Rating** | **Risk Rating** |
| *State the relevant objective the risk relates to (e.g. strategic, business, project, clinical)*  *Describe Intent, purpose and outcomes* | *List internal and external factors that influence this risk in relation to objectives* | *Where the risk originates (e.g. regulatory requirements, political changes)* | *Something might occur which {****Cause(****s)} the {****Event****} that leads to an {****Impact****/Consequence(s)}* | | | *Such as a process, policy, practice, device* | *Refer to control effectiveness rating (Refer to Appendix E – Risk Rating Criteria)* | *Use likelihood and consequence table and risk matrix. Rate the risk based on the current controls and their effectiveness (Refer to Appendix E – Risk Rating Criteria)* | *Based on the outcomes of the risk analysis, risk evaluation assists in deciding which risks need treatment and the priority for treatment implementation.* |
| Business objective:  Increase service productivity to core clients by 10 % in 1 year | Obsolete technology; budgetary constraints; change in management | Change in management; change in government funding; changes in legislation | **Cause**  E.g. Failure to maintain client service management system | **Event**  E.g. Leads to delays in service delivery | **Impact**  E.g. Results in poor service level to core clients | Governance committee; policies and procedures; quality improvement plans | High, Medium or Low | Rating = Likelihood x Consequence | Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered. Options for treatment may include:   * Avoidance of risk * Pursuing risk * Removing risk source * Changing likelihood * Changing consequence * Sharing risk with another party * Retaining the risk |

**RISK REGISTER**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Risk** | **Owner** | **Consequence** | **Likelihood** | **Inherent Risk Level** | **Controls** | **Control Effectiveness** |
|  | **Risk Area** |  |  |  |  |  |  |
| 1. | Risk name and description |  |  |  |  |  |  |