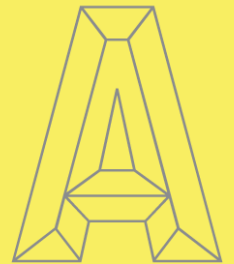


Version 1.4



# ENTERPRISE RISK MANAGEMENT MANUAL



## Document Control

Document Title	Category	PD Number	Original Publication
Enterprise Risk Management (ERM) Manual	Manual	WDCSG17501	01/11/17

## Version Release

Date	Version	Key Changes	Author
1 Oct 2017	1.0	Draft for internal comment	Tony Harb
1 Nov 2017	1.1	Updated for feedback. First issue approved by COO	Tony Harb
24 Apr 2018	1.2	Minor changes endorsed by ELT in relation to: <ul style="list-style-type: none"> <li>▪ Risk register record keeping in HPCM</li> <li>▪ Risk Treatment Plans</li> <li>▪ Risk and control ownership</li> <li>▪ Control and action numbering</li> </ul>	Clare Kitcher
2 Aug 2019	1.3	Inclusion of revised risk categories and related risk consequence table and risk register template. Updated Risk Appetite Statement and associated changes to escalation procedures. Simplified the risk management process steps to improve useability. Amended MD message.	Clare Kitcher
30 April 2021	1.4	Update to TPP20-08 Internal Audit and Risk Management Policy for the General Government Sector References to Risk Appetite Statement updated to reflect October 2020 changes to risk appetite. Replace reference to Executive Leadership Team with FOCUS Team Update titles from Business Partners Risk Management to Principal Risk Advisors	Clare Kitcher

## Associated documents

This Manual should be read in conjunction with the following related documents:

- Enterprise Risk Management Policy
- Risk Appetite Statement
- Enterprise Risk Management Plan (annual)
- AS/NZS ISO 31000:2018 Risk Management - Principles and guidelines
- TPP20-08 - Internal Audit and Risk Management Policy for the General Government Sector

## FORWARD

### A MESSAGE FROM THE MANAGING DIRECTOR

“TAFE NSW’s vision is to provide learning for jobs and brighter futures, and to skill the workforce for the future. To achieve this vision, opportunities to become more competitive, agile and customer-centred must be taken in a managed way.

The Enterprise Risk Management framework is an important management tool in ensuring that our organisation looks for opportunities to be more innovative and creative and takes these opportunities in a carefully managed way.

We recognise that large, unmitigated risks can adversely impact our stakeholders, our reputation and our ability to achieve our vision and purpose.

It is critical that all risks be understood and managed at the most appropriate level within the organisation. Management will take a leadership role in creating an environment that promotes sound risk-taking behaviour and ensures risks are considered when making important strategic and operational decisions. Nevertheless, it is everyone's responsibility to help manage risk by proactively identifying, evaluating and escalating risks that could impact TAFE NSW.

This Enterprise Risk Management Manual is a Written Direction and key to the enterprise risk management framework. This Manual aims to ensure risk management practices are embedded into all activities, risk management thinking is deeply entrenched into the organisation’s norms and prudent risk taking is aligned to TAFE NSW’s Risk Appetite.

I am committed to fostering an organisational culture where risk management is seen as an enabler, embraced by our leaders and valued by all our employees and stakeholders.”

**Steffen Faurby**

Managing Director, TAFE NSW

# CONTENTS

- Document Control ..... 2
- Version Release ..... 2
- Associated documents ..... 2
- FORWARD..... 3
  - A message from the Managing Director ..... 3
- CONTENTS ..... 4
- 1. INTRODUCTION ..... 7
  - Purpose..... 7
  - Scope ..... 7
- 2. RISK MANAGEMENT FUNDAMENTALS..... 8
  - 2.1 THE BASICS ..... 8
    - What is risk? ..... 8
    - What is risk management?..... 8
    - When should we manage risk? ..... 8
    - How do we manage risk? ..... 9
    - Who is responsible for managing risks?..... 9
    - What are the benefits of managing risk? ..... 9
    - What happens with all the risk management information collected?..... 10
    - What can stop TAFE NSW managing risk effectively? ..... 11
  - 2.2 THREE LINES Model ..... 12
    - First Line – Management..... 12
    - Second Line – Risk Management Function..... 13
    - Third Line – Internal Audit..... 13
  - 2.3 RISK CULTURE ..... 13
- 3. ENTERPRISE RISK MANAGEMENT FRAMEWORK..... 14
  - 3.1 FRAMEWORK DESIGN..... 14
  - 3.2 FRAMEWORK ELEMENTS..... 14
    - Risk Management Framework ..... 14
    - Risk management resources and committees ..... 15
    - Risk management records..... 15
    - Other supporting policies, procedures and arrangements ..... 15
- 4. RISK MANAGEMENT PROCEDURE IMPLEMENTATION..... 16

4.1 APPROACH AND METHODOLOGY ..... 16

4.2 MANAGE RISKS AT ALL LEVELS ..... 16

    Strategic Level ..... 16

    Operational Level ..... 17

    Project Level ..... 17

4.3 MAINTAIN RISK REGISTERS..... 19

    Other risk assessments..... 19

4.4 MONITOR, ESCALATE AND REPORT RISKS..... 20

    Other incidents and issues ..... 20

5. RESPONSIBILITIES ..... 21

6. DEFINITIONS ..... 21

ANNEX A: RISK MANAGEMENT PROCEDURE ..... 25

    1 – COMMUNICATION AND CONSULTATION..... 26

    2 – ESTABLISH CONTEXT..... 27

    3 – RISK ASSESSMENT..... 27

        Risk Identification ..... 27

        Risk Analysis ..... 29

        Risk Evaluation ..... 31

    4 – RISK TREATMENT..... 33

        Implementing additional controls / treatment actions..... 33

        Other risk treatment options ..... 35

        Escalating risks..... 35

        When to escalate a risk ..... 35

        How to escalate a risk..... 36

        Completed treatment actions ..... 37

    5 – MONITORING AND REVIEW..... 37

        Monitoring and review of specific risks..... 37

        Monitoring risks outside appetite and Risk Treatment Plans ..... 37

        Monitoring and review of the risk management framework ..... 38

APPENDIX 1 – RISK REGISTER WORK INSTRUCTION..... 39

    STEP 1: RISK IDENTIFICATION ..... 39

        Risk Assessment - Inherent ..... 39

    STEP 2: RISK ASSESSMENT..... 40

        Risk Control ..... 40

Risk Assessment - Current ..... 40

STEP 3: RISK TREATMENT ..... 41

    Develop action plan..... 41

    Risk Assessment – After Treatment ..... 41

STEP 4: ESCALATION ..... 42

APPENDIX 2: RISK REGISTER TEMPLATE..... 43

APPENDIX 3: LIKELIHOOD RATING TABLE..... 44

APPENDIX 4: CONSEQUENCE RATING TABLE ..... 45

APPENDIX 5: RISK LEVEL RATING TABLE..... 49

# 1. INTRODUCTION

In accordance with the TAFE NSW Enterprise Risk Management Policy, TAFE NSW is committed to maintaining an effective and efficient enterprise risk management framework to help promote a positive risk culture and proactively manage enterprise wide risks at all levels to support the achievement of TAFE NSW’s objectives. This is achieved through the enterprise risk management framework and Written Direction that ensure risk management practices are embedded into all activities, risk management thinking is deeply entrenched into the organisation’s norms and prudent risk taking is aligned to risk appetite.

## PURPOSE

The purpose of this Enterprise Risk Management Manual is to outline TAFE NSW’s enterprise risk management framework to ensure a consistent approach for identifying, analysing, evaluating, treating, reporting and escalating risks. This Manual will help risk owners develop and maintain their risk register in a manner that is uniform with the TAFE NSW enterprise risk management framework.

## SCOPE

This Enterprise Risk Management Manual applies to all employees, in particular to senior managers and risk owners, who are responsible for identifying risks, designing, implementing and monitoring internal controls and maintaining a risk register for their functions, activities and projects.

## 2. RISK MANAGEMENT FUNDAMENTALS

### 2.1 THE BASICS

Before we provide an outline of the TAFE NSW Enterprise Risk Management framework, it is important to understand some risk management basics. There are many terms used in this Manual. Definitions for key terms are in Section 6 of the Manual.

#### ***What is risk?***

Risks are inherent in our day-to-day activities, operational procedures, strategic and operational planning processes and decision-making structures.

Risk is defined as the 'effect of uncertainty on objectives'. Risks arise due to uncertainty about future outcomes or events. Of course, some of that uncertainty may be positive i.e. achieving more than we planned, as well as uncertainty threatening the achievement of our objectives.

Risk is often measured in terms of its consequence (how bad an event will be?) and likelihood (how likely is the event to occur?). The combination of consequence and likelihood will indicate the level of risk.

Enterprise Risk Management (ERM) covers risks across the organisation and is strongly linked to the TAFE NSW strategy, goals, objectives and governance. It focusses on making good decisions and prioritising work on a risk basis.

#### ***What is risk management?***

Risk management includes all the coordinated activities to direct and control an organisation with regard to risk. TAFE NSW has established a rigorous Enterprise Risk Management framework consisting of a formal Policy, Manual and Risk Appetite Statement to direct and control risk management activities along with an annual Enterprise Risk Management Plan to ensure continuous improvement. Refer to Section 3 of this Manual for an overview of TAFE NSW's Enterprise Risk Management framework.

In terms of process, risk management starts by anticipating, identifying and analysing possible risks and then implementing internal controls to remove uncertainty by minimising negative impacts and locking in positive consequences. The output of the risk management process is good decisions, allocating resources where they will have the biggest impact, innovating where TAFE NSW has an appetite for taking a bit more risk and reducing negative outcomes to the level defined in the TAFE NSW Risk Appetite Statement.

A risk register will record the risks being managed, how big they are, and the way they are being managed.

#### ***When should we manage risk?***

We must manage risks at all levels of the organisation. This includes all functions, activities and projects. Refer to Section 4.2 of this Manual for the levels within TAFE NSW we consider risk.

Some think that risk management only occurs when you undertake a risk assessment or complete a risk register. This is not correct. Risk management happens every minute, every hour and every day. By simply following this Manual and other Written Direction (policies and procedures), we are managing many of our day-to-day operational risks.

Risk management is not an isolated function that exists within TAFE NSW with responsibility limited to a few people. Rather, it is an integral part of strategic, operational and project management. Risk management should be embedded in all our procedures and activities.



## ***How do we manage risk?***

We manage day-to-day risks by implementing a range of effective internal controls designed to minimise or negate potential negative outcomes and enhance opportunities. Internal controls are often documented in Written Directions and reflected in our business processes.

Risks that arise from our strategic initiatives and programs are more complex, transient and subject to more uncertainty and risk. These risks will require more rigorous analysis and formal risk assessment when pursuing new strategies or establishing new programs.

## ***Who is responsible for managing risks?***

Risk management is everyone's responsibility, but it is primarily the responsibility of managers in our business. Refer to the Three Lines model in Section 2.2 on the range of responsibilities.

The Enterprise Risk Management Policy contains a brief overview of the roles and responsibilities of key positions.

At TAFE NSW, risk owners are responsible for managing risk in a structured and consistent manner and maintaining a risk register for their project, region, group, branch, or unit that covers all current and future activities.

Risk owners will allocate control owners for each risk control. These control owners will make sure the control is put in place and maintained. They will also report to the risk owner on their controls.

Risk owners will also allocate an action owner for each risk treatment action. These action owners will make sure the treatment is implemented within the timeframe set. They will also report to the risk owner on the status of their treatment actions, flagging any delays or changes in the effectiveness of actions.

All employees are responsible for identifying risks and reporting those risks to their managers. Employees are often the first to identify emerging risks so escalating them to managers for evaluation is really important. All employees are responsible for following TAFE NSW policies, guidelines and manuals that have controls to manage risk already embedded into them.

## ***What are the benefits of managing risk?***

Managing risk has considerable tangible and intangible benefits.

The combination of proficient risk management capabilities by all senior managers and risk owners and a proactive, structured, systematic and integrated approach to risk management will help ensure a positive risk-aware culture that will deliver a range of benefits to TAFE NSW, including:

- Increased likelihood of TAFE NSW achieving its short and long term objectives;
- Achieving a balanced approach to taking risk(s) to reduce uncertainty;
- Better and consistent decision-making and planning;
- Better identification of opportunities and threats;
- Mitigating the likelihood and impact of undesirable events;
- Pro-active rather than re-active management;
- More effective allocation and use of resources (human, financial, intellectual);
- Improving stakeholder confidence and trust;
- Improving compliance with key regulatory requirements;
- Better corporate governance; and
- Protecting and enhancing reputation.

***What happens with all the risk management information collected?***

The outputs of formal risk management and risk assessment activities will provide risk owners, management and stakeholders with important information about the organisation’s risk profile and control environment. For example:

- Risk owners will have a better understanding of the risks in their area or project to enable them to make decisions with more confidence and prioritise work more effectively.
- The FOCUS Team and management will use risk information to support risk owners in managing risks within the risk appetite.
- Internal Audit may rely on information from various risk registers to prepare a strategic audit plan and help prioritise and resource internal audit activities.
- When conducting an audit, internal audit may use the controls identified in the risk register to validate the effective operation of controls.
- The Audit and Risk Committee will have visibility over key risks and controls to help them provide effective oversight and independent advice on risk management activities.
- The Managing Director will use information and reports provided to support the annual Attestation Statement published in the Annual Report.

### What can stop TAFE NSW managing risk effectively?

A risk management framework is only as strong as its weakest link. TAFE NSW has identified and addressed the key barriers that inhibit effective risk management in Table 1 below.

Risk Management Inhibitors	TAFE NSW Strategies to Mitigate Inhibitors
<p><b>A lack of support from senior management</b></p>	<ul style="list-style-type: none"> <li>▪ Managing Director has committed to risk management.</li> <li>▪ Enterprise Risk Management Policy outlines clear responsibilities for ownership and oversight.</li> <li>▪ FOCUS Team actively discuss risk management and the risks within the organisation.</li> <li>▪ Oversight by TAFE Commission Board and Audit and Risk Committee (ARC).</li> </ul>
<p><b>A lack of time and resources allocated to risk management</b></p>	<ul style="list-style-type: none"> <li>▪ Risk management function comprising of Head of Risk and Principal Risk Advisors.</li> <li>▪ Enterprise Risk Management Plan outlines timing of key activities and strategies to build capabilities.</li> <li>▪ Enterprise Risk Management Policy outlines responsibilities.</li> </ul>
<p><b>A lack of clarity over risk ownership/responsibility for risk management</b></p>	<ul style="list-style-type: none"> <li>▪ Enterprise Risk Management Manual, Plan and Policy outline responsibilities.</li> <li>▪ Initial and ongoing risk management awareness training.</li> </ul>
<p><b>Over- or under-treatment of risks</b></p>	<ul style="list-style-type: none"> <li>▪ The Risk Appetite Statement sets expectations on the level of risk control required.</li> <li>▪ Enterprise Risk Management Manual requires regular review and monitoring of risks.</li> <li>▪ Escalation processes are in place.</li> <li>▪ FOCUS Team and Audit and Risk Committee monitor the treatment of risks within the appetite set.</li> </ul>
<p><b>Unnecessarily complex risk documentation</b></p>	<ul style="list-style-type: none"> <li>▪ Clear risk management framework documents and templates.</li> <li>▪ Extensive engagement and coaching available to risk and control owners from Principal Risk Advisors.</li> </ul>
<p><b>A lack of independent assurance over the effectiveness of the risk management framework</b></p>	<ul style="list-style-type: none"> <li>▪ Oversight by FOCUS Team and Audit and Risk Committee.</li> <li>▪ Annual reporting against TPP20-08 risk management requirements.</li> </ul>
<p><b>Difficulty in identifying and assessing emerging risks, especially cross-agency risks</b></p>	<ul style="list-style-type: none"> <li>▪ Oversight by risk management function and Audit and Risk Committee.</li> <li>▪ Risk reports containing information on changes to the risk environment and emerging/changing risks</li> </ul>

Table 1: Risk management inhibitors

## 2.2 THREE LINES MODEL

The Three Lines Model of governance recognises that three key groups need to work together at different stages to protect the organisation against an ever-widening array of risks. In simple terms, the three lines have different roles and reporting lines to protect TAFE NSW from a range of risks as highlighted in Figure 1 below.

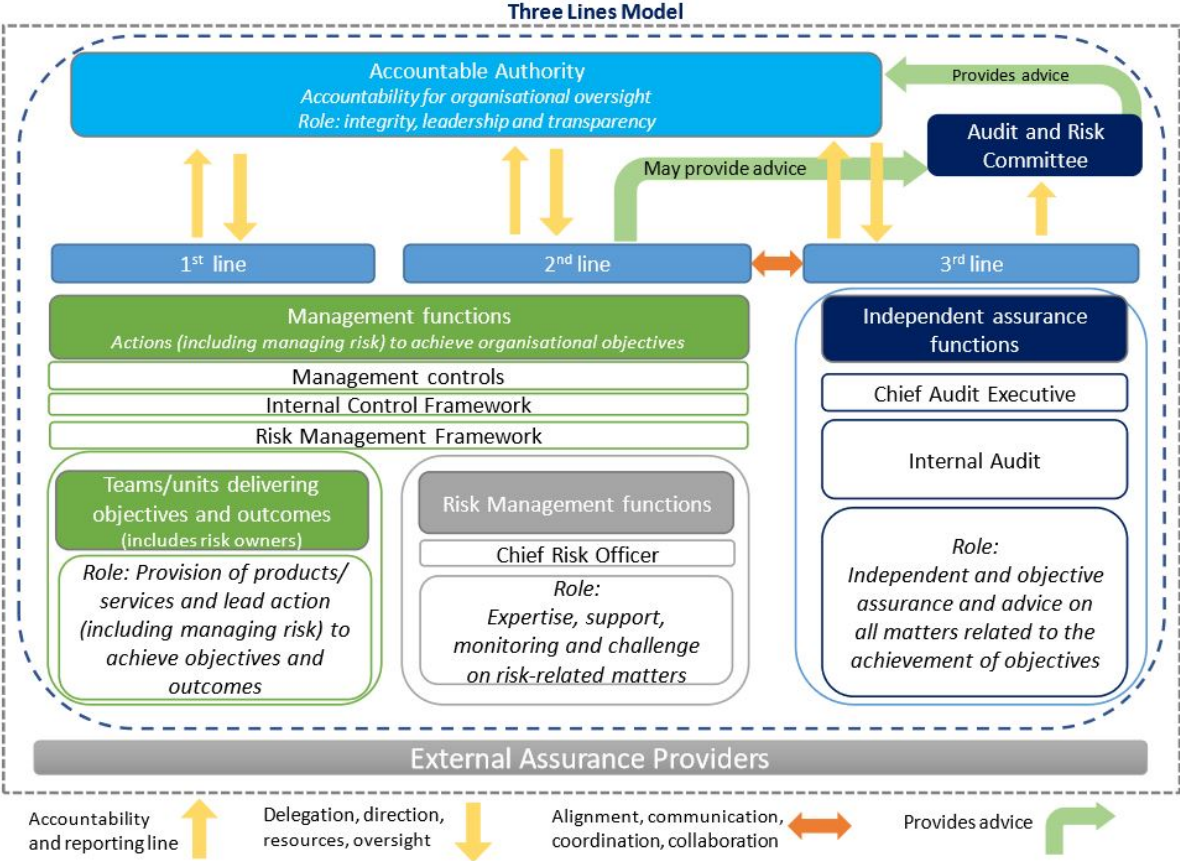


Figure 1: Three Lines Model

The Three Lines Model provides a simple and effective way to enhance communications on risk management and control by clarifying essential roles and duties within an organisation. The model promotes risk ownership and a stronger risk culture while eliminating inefficiencies, gaps and overlaps that occur in the management of risk and compliance by multiple functions.

### First Line – Management

The first line is the key to success because invariably it is the quality of internal controls and written directions (people, policies, procedures and systems) at the coalface that is the main determinant of success to managing risk. The first line is performed by operational managers (including risk owners, control owners and risk treatment action owners) and employees. The first line comprises of all the actions, behaviours and internal controls that are designed and enforced by front line managers to help manage risk. This line includes for example our teachers, our staff in student services, our administration staff processing financial transactions and educational related records e.g. enrolments.

**Second Line – Risk Management Function**

The second line provides a support role to the first line and is performed by the risk management function and the various compliance management functions. TAFE NSW has a designated risk management function that includes a Head of Risk and Principal Risk Advisors to support front line managers. In addition, other compliance functions specific for TAFE NSW are Standards and Compliance, whose role includes developing frameworks to support and monitor compliance with ASQA and TESQA and the Work Health and Safety function who develop frameworks and monitor compliance relating to high risk activities that impact people’s physical and psychological safety and health.

**Third Line – Internal Audit**

The third line provides more independent assurance that risks are being managed and controlled effectively. This includes the role of the internal audit function. Through the development of the three-year Internal Audit Plan and its annual refresh, TAFE NSW’s risks are considered and key areas of risk are identified and key controls frequently audited.

**2.3 RISK CULTURE**

Risk culture is a term describing the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people.

An effective risk culture is one that enables and rewards individuals and groups for behaviours and actions that are in line with risk management objectives of risk awareness, effective risk control and taking the right risks in an informed manner. A good risk culture can be achieved in several ways:

- FOCUS Team and senior managers championing risk management and leading by example;
- Promoting the view that all employees are managers of risk;
- Encouraging all managers and staff to develop knowledge and skills in risk management; and
- Supporting and encouraging staff to incorporate risk management into their everyday roles and responsibilities.

The TAFE NSW Enterprise Risk Management Plan outlines the strategies in respect to management resources, training and awareness programs for building an effective organisational culture.

### 3. ENTERPRISE RISK MANAGEMENT FRAMEWORK

#### 3.1 FRAMEWORK DESIGN

TAFE NSW’s Enterprise Risk Management framework is modelled on Australian/New Zealand Standard (AS/NZS) ISO 31000:2018 Risk Management – Principles and guidelines, tailored to meet the needs of TAFE NSW. The framework is also aligned with the Internal Audit and Risk Management Policy for the General Government Sector (TPP 20-08). TPP 20-08 also advocates the use of AS/NZS ISO 31000:2018 risk management approach to ensure common and generally accepted risk management terminology and processes are applied across Government.

The Enterprise Risk Management framework has been designed in consultation with key stakeholders including Managing Director, FOCUS Team, TAFE Commission Board, Audit and Risk Committee and managers from across TAFE NSW. Many of the changes to the framework have been generated by the front line and escalated through the extensive engagement activities of the Principal Risk Advisors.

A prescribed risk management framework helps establish the foundations and organisational arrangements for mandating risk management, designing the framework, implementing risk management processes, monitoring and reviewing the framework and continually improving the risk management framework.

Specific details about how these key elements of the risk management framework are implemented at TAFE NSW are outlined in the annual Enterprise Risk Management Plan.

#### 3.2 FRAMEWORK ELEMENTS

The TAFE NSW Enterprise Risk Management framework consists of a number of elements to provide a structure for a consistent risk management approach and for embedding risk management across all operations.

##### *Risk Management Framework*

- **Enterprise Risk Management Policy:** clearly communicates TAFE NSW commitment to maintaining an effective and efficient risk management framework to support the management of enterprise-wide risks at all levels and embed risk management into day-to-day activities.
- **Risk Appetite Statement:** a document that defines how much risk to take to achieve our objectives. The Risk Appetite Statement (RAS) is used to assist manage our risks and guide our decision-making.
- **Enterprise Risk Management Manual:** provides a reference point for all employees and risk owners to improve their risk management capabilities on how risk management can be practically applied in day-to-day activities, projects and strategic planning, resulting in better management of their risks.
- **Enterprise Risk Management Plan:** provides an annual plan of initiatives that will foster a positive risk-aware culture and mechanisms for implementing, resourcing, communicating and improving risk management as well as measuring and reporting risk management performance.
- **Risk Management Procedure and Risk Register Work Instruction:** part of the Enterprise Risk Management Manual to help risk owners maintain their risk register in a manner that is consistent with the TAFE NSW Enterprise Risk Management framework by providing step-by-step instructions for identifying, analysing, evaluating, treating and escalating risks.

### ***Risk management resources and committees***

A dedicated risk management function is available to support TAFE NSW employees in managing their risks. The team includes a Head of Risk and Principal Risk Advisors based across the state.

Various Board and management committees provide oversight of risk management. Key committees include TAFE NSW Commission Board, Audit and Risk Committee, FOCUS Team, regional and senior leadership teams (RLT and SLT).

Clearly defined responsibilities for risk ownership and oversight are detailed in the TAFE NSW Enterprise Risk Management Policy.

### ***Risk management records***

Risk registers and other risk assessment records are kept to formally document the risk evaluation process. Risk reports are produced to communicate important risk and control information to stakeholders.

Note: Content Manager is the repository for TAFE NSW records. Folders have been established within Content Manager to retain operational risk registers and the Strategic Risk Register along with ERM Framework documents, reports etc. These can be viewed by all staff who have been given access permission.

### ***Other supporting policies, procedures and arrangements***

Other supporting policies, procedures, processes, frameworks and arrangements exist that complement risk management including written direction framework, internal audit, business resilience, insurance arrangements, fraud and corruption control plans, incident, emergency and crisis management plans, compliance plans and workplace health and safety management systems.

## 4. RISK MANAGEMENT PROCEDURE IMPLEMENTATION

### 4.1 APPROACH AND METHODOLOGY

TAFE NSW utilises the Australian and New Zealand Risk Management Standard AS/NZS ISO 31000:2018 Risk Management - Principles and guidelines to support the design and implementation of an effective and efficient risk management processes.

This standard provides a proactive and structured, step-by-step risk management approach that can be applied across TAFE NSW to manage risks at all levels including strategic level risks, project level risks and operational level risks.

TAFE NSW will maintain risk management processes that are also aligned with the Internal Audit and Risk Management Policy for the General Government Sector (TPP 20-08) and NSW Treasury’s risk management toolkit (TPP12-03).

It is important that risk management be embedded into planning processes, decision-making structures, projects, daily operational procedures and organisational culture...that is to say, “it’s the way we do things around here”.

### 4.2 MANAGE RISKS AT ALL LEVELS

Integrated risk management requires an ongoing assessment of potential risks at every level. At minimum, risk management must be integrated and considered in all activities at strategic, project and operational level.

#### *Strategic Level*

A strategy involves an informed, measurable decision about the direction an organisation chooses to take. Strategic risks arise during strategy formulation and strategy implementation or from factors in the external environment that could impact strategy.

Strategic level risks are often very hard to manage as they involve greater uncertainty, complex assumptions, complex activities and overall high inherent risk when compared to day to day, operational activities. The risks that are associated with strategies may be transient or relatively short term in nature but often have long lasting consequences.

Failure to manage strategic level risks could have significant negative financial, reputational and operational consequences on TAFE NSW and stakeholders. Therefore, a risk register is maintained for strategic level risks.

Strategic risks cannot always be managed through a rules-based control model. Instead, controls need to be dynamic and flexible. Strategic risks and their controls are often helped or hindered by the organisation’s culture and norms of behaviour within and across organisational boundaries.

It is important to understand that strategic risks are different from preventable operational risks because activities that give rise to strategic risks are not inherently undesirable.

Whilst managing strategic level risks is good management practice, TPP20-08 specifically requires that “risk management is integrated into strategic and business planning, budgeting and reporting processes”.

Risk and strategy are linked. Whenever there is a change to the strategy, the risks will also change. In addition, strategic plans will not remain static due to changing priorities, environmental changes, and government decisions and therefore will need re-assessment regularly.



Maintaining an eye on changes in the risk environment is critical to identifying, escalating and managing strategic risks.

Strategic level risks are identified and assessed by the FOCUS Team and Managing Director and given formal consideration by the Audit and Risk Committee.

If the Managing Director cannot reduce a strategic risk to within risk appetite, the risk must be escalated to the TAFE Commission Board through the Audit and Risk Committee. The Managing Director may also escalate a risk to the Minister for immediate consultation.

### ***Operational Level***

Operational structures, systems and processes that follow strategy will give rise to operational risks. Operational level risks typically exist within the day-to-day activities and decisions at different levels across TAFE NSW.

Operational level risks are often easier to manage than strategic level risks and project level risks as the risks are often more predictable, involve less uncertainty and can be adequately controlled through well designed and executed policies and procedures. High impact, low probability risks can also be mitigated with appropriate business continuity and disaster recovery planning.

Whilst managing operational level risks is good management practice, there are a number of stakeholder requirements to proactively manage risk. Examples include:

- TPP20-08 specifically requires that “risks are formally considered when developing and implementing policies or programs, projects and other activities including procurement” and “risk management covers all relevant risk categories including strategic, operational, project, compliance, reputational, financial, legal and reporting risks”.
- The Standards for Registered Training Organisations (RTOs) 2015 require “the RTO to implement a comprehensive plan of systematic validation of its assessment practices and results, based on risk” and take into account “the relative risks of all of the training products”.
- The VET Quality Framework contains “Financial Viability Risk Assessment Requirements”.
- Tertiary Education Quality and Standards Agency (TEQSA) utilises a risk-based approach to assuring higher education standards and consider if the significant risks of the provider have been identified and controlled.
- The Work Health and Safety Act 2011 and Regulations require persons who have a duty to ensure health and safety to ‘manage risks’.

Operational level risks at TAFE NSW are very broad and would cover (but is not limited to) the risks associated with service delivery, employee management, quality products and teaching, work health and safety, financial management and budgeting, financial and management reporting, legal and business compliance, internal and external fraud, business processes, outsourcing, procurement, business continuity, information technology, security, and the introduction of new products.

Any operational risk that cannot be brought within the defined risk appetite must be escalated for formal consideration by the FOCUS Team, Managing Director, and Audit and Risk Committee.

### ***Project Level***

A project is planned work or an activity that is finished over a period of time and intended to achieve a particular purpose. Projects can be related to strategic plans or operational activities.

Project risk considerations need to include the inherent risks associated with the project(s), the type of project activity and the impact the project will have on the risk environment.

All projects have risks. If the potential risks are not identified and managed early, then the project is exposed to risk of delays, cost over-runs and/or result in below quality outcomes.

Managing project risks is considered good management practice and an integral element of leading project management methodologies such as PMBoK and PRINCE2. In addition, TPP20-08 specifically requires that “risks are formally considered when developing and implementing policies or programs, projects and other activities” and “the risk management process used to manage project risks is consistent with and linked to the agency’s risk management framework, to ensure project risks are visible, rather than being managed as a discrete activity”.

Typical project risks are.

<b>Schedule</b>	Events or trends potentially impacting on the delivery of project/program deliverables or outcomes within agreed timeframes
<b>Budget</b>	Events or trends potentially impacting on the agreed expenditure of the project/program
<b>Scope</b>	Events or trends potentially impacting the delivery of the stated scope of the program/project or portfolio
<b>Quality</b>	Risks that relate to events or trends that could impact on delivery of quality of deliverables and outcomes, such that they satisfy expectations
<b>Resourcing</b>	Events or trends potentially impacting the availability of resources in alignment with program/project needs
<b>Governance</b>	Risks that relate to events or trends that could impact on the way the Portfolio is structured, operated, directed and controlled
<b>Stakeholders</b>	Risks that relate to events or trends that could impede availability of stakeholders or buy-in to the stated program/project objectives
<b>Business Impacts</b>	Events or trends potentially impeding business continuity, resilience, or organisation acceptance of change
<b>Vendor</b>	Risks that relate to events or trends that could impact on Portfolio performance because of vendor management/non-performance
<b>Benefits</b>	Risks that relate to events or trends potentially impacting on the ability of the programs/projects delivery of approved benefits quantum or benefits profile
<b>Delivered Risk</b>	Adverse post-implementation risk of the delivered project on ongoing day-to-day activities

Table 2: Types of project risks

Project and Program Managers are responsible for keeping their Work Stream Sponsor and relevant Steering Committee advised of their project/program risk profile and managing it on their behalf. The relevant General Manager is responsible for keeping the FOCUS Team, Managing Director, and Audit and Risk Committee advised of the risk profile and managing it on their behalf.

Any project risk that cannot be brought within the defined risk appetite must be escalated for formal consideration by the FOCUS Team, Managing Director, and Audit and Risk Committee.

### 4.3 MAINTAIN RISK REGISTERS

The risk register is an important element of the risk management framework because it is a formal record of the risks identified, evaluated and managed by the risk owner.

A risk register can be established for a region, group, branch, unit, project and strategic initiatives and cover all current and future activities.

At minimum a risk register should be maintained for key risks at strategic, operational and project level.

Emerging risks should be incorporated in the appropriate risk register as they are identified.

All risk owners are required to maintain a risk register which provides a current, accurate and complete record of risk assessment and management activities. The risk register is to be a “living document”, remain current and subject to regular review and update as risks are addressed and new risks identified, and controls and risk treatments for current risks updated.

Risk registers are maintained in electronic format using the TAFE NSW risk register template (Excel) and stored in Content Manager at folder PRGM17/9226. It is the responsibility of the Risk Owner to ensure the latest version of the Risk Register is in Content Manager.

The Risk Register Work Instructions for risk register maintenance are in the later appendices to this manual. These include steps for identifying, analysing, evaluating, treating and escalating risks. The work instructions aim to help risk owners maintain their risk register in a manner that is consistent with the TAFE NSW risk management framework.

The risk registers and Risk Register Work Instruction are to be applied consistently for all strategic, operational and project risks.

The Head of Risk reports risk performance to the FOCUS Team, and information used in that reporting is sourced from completed Risk Registers that are in Content Manager.

#### ***Other risk assessments***

In some instances, using this Manual, the Risk Register Work Instruction and the risk ratings may not be suitable for some risk assessments and more context specific risks assessments are needed e.g. Onsite Safety Risk Assessment. These risk assessment activities are often identified as controls on the risk register for a region, group, branch or unit.

Risk owners may use other more suitable risk assessment tools to manage specific and more dynamic risks, however, in all cases these risk assessments should:

- Be modelled on Australian/New Zealand Standard (AS/NZS) ISO 31000: 2018 Risk management – Principles and guidelines or the relevant standard, this Manual or best practice risk assessment methods; and
- Risk ratings and risk evaluation criteria used should always reflect TAFE NSW Risk Appetite Statement.

## 4.4 MONITOR, ESCALATE AND REPORT RISKS

All employees are responsible for identifying risks and reporting those risks to their manager for consideration of the impact and level of risk.

Once a risk has been identified, managers and/or risk owners are responsible for assessing and managing the risk in accordance with the TAFE NSW risk management framework.

For the purpose of formal risk assessments, risk reporting is a shared responsibility between the risk owner, Head of Risk and Principal Risk Advisors.

Risk reporting supports decision making for major risks identified during the risk assessment process and when balancing between threat and opportunity. Reporting arrangements can include:

- Any risk management initiatives undertaken during the period;
- Any moderate level or higher incidents or issues that have occurred during the previous quarter;
- The key inherent and residual risks facing the area/activity/project and the controls in place to manage those risks;
- Progress in implementing key risk treatment plans; and
- Any other issues that have arisen over a period or likely to arise in the future, relevant to the risk management framework that should be brought to the attention of the Head of Risk, FOCUS Team and/or Managing Director.
- Where a risk has been identified that is likely to impact other agencies, the risk should be formally communicated to the affected agency or agencies by the Managing Director via the TAFE NSW Executive and Ministerial Liaison Unit.

Formal reporting will also be required as part of TAFE NSW's regulatory reporting requirements.

### ***Other incidents and issues***

Incidents, complaints, issues, near misses or near incidents may be leading risk indicators to an emerging risk. All employees are responsible for reporting incidents, complaints, issues, near misses or near incidents to their managers in a way consistent with the appropriate TAFE NSW policy and procedure.

## 5. RESPONSIBILITIES

Managing risk is everyone’s responsibility. The Enterprise Risk Management Policy contains a brief overview of the roles and responsibilities of key positions.

## 6. DEFINITIONS

The following terms are used in this Manual.

TERM	DEFINITION
<b>ALARP</b>	As Low As Reasonably Practicable (used in WHS risk context where risks are inherently undesirable)
<b>Audit and Risk Committee (ARC)</b>	A committee established to monitor, review and provide advice about governance processes, risk management and internal control frameworks, and external accountability obligations.
<b>Communication and consultation</b>	Continual and iterative processes within the risk management process to provide, share or obtain information and to engage in dialogue with stakeholders and others regarding the management of risk.
<b>Consequence</b>	The outcome of an event affecting objectives e.g. safety, customer experience, financial, reputation, regulatory. Note - consequences may be positive or negative.
<b>Control</b>	A measure that modifies risk. Includes existing processes, procedures, policies, devices, practices or other actions that act to change the likelihood of the risk occurring or the consequences should the risk event happen or both.
<b>Control Owner</b>	The position with accountability and authority to deliver and maintain the control. Control owners will be a team leader or above. The control owner is a position rather than an individual, e.g. Head Teacher rather than Jane Smith.
<b>Current risk</b>	The risk today. Level of risk remaining after considering existing controls but before any future treatment actions are in place.
<b>Enterprise Risk Management (ERM)</b>	Coordinated activities to direct and control the organisation with regard to risk. Providing a framework for addressing risk in methodical, consistent ways, creating an environment where informed decisions about TAFE NSW’s risks are made in an open and transparent way, and giving confidence that we can reduce uncertainty in achieving our objectives by: <ul style="list-style-type: none"> <li>effectively managing threats to an acceptable/tolerable level</li> <li>making informed decisions about exploiting opportunities, where they exist</li> </ul>
<b>Enterprise Risk Management Manual</b>	A document within the risk management framework that aims to ensure a consistent approach for the management and monitoring of risks.

<b>Enterprise Risk Management Plan</b>	A document produced annually to set the risk management direction and priorities for the organisation for that (financial) year.
<b>Enterprise Risk Management Policy</b>	A document within the risk management framework mandating the overall intentions and direction of an organisation related to risk management.
<b>Establishing context</b>	A step in the risk management process that involves setting the parameters within which risks are identified, assessed and managed.
<b>External context</b>	Considering the external environment in which the organisation seeks to achieve its objectives e.g. competitors, government policy, economic conditions.
<b>Inherent risk</b>	Level of risk before considering existing controls or risk treatment.
<b>Internal audit</b>	An independent, objective assurance and consulting activity designed to add value and improve an organisation’s operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
<b>Internal context</b>	Considering the internal environment in which the organisation seeks to achieve its objectives e.g. internal resources, internal processes.
<b>Level of risk</b>	The risk rating calculated by applying the likelihood rating and consequence rating criteria. The level of risk may be determined before considering controls (inherent risk), after considering controls (current risk) and after delivery of future treatment actions (after treatment risk).
<b>Likelihood</b>	Chance of something happening.
<b>Monitoring</b>	Continual checking, supervising, critically observing or determining the status of the risk and control in order to identify changes e.g. new or emerging risks, recent incidents, weakened controls, new controls.
<b>Operational risk</b>	A source of uncertainty or events that may arise during the normal course of day-to-day activities and decisions. Operational risks may arise from inadequate or failed internal processes, people and systems, or from external events. They are managed by risk owners and escalated to the FOCUS Team/Managing Director when the level of risk is outside risk appetite.
<b>Project risk</b>	A source of uncertainty that may arise from taking on projects that can hamper the project’s overall objectives and success resulting in a range of adverse consequences. They are managed by the Program Manager who is the risk owner and escalated to the FOCUS Team/Managing Director when the level of risk is outside risk appetite.
<b>Residual risk</b>	See Current risk

<b>Review</b>	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.
<b>Risk</b>	Effect of uncertainty on objectives. (Note: effect is a deviation from the expected and may be positive or negative).
<b>Risk analysis</b>	A systematic process to comprehend the nature of risk and to determine the level of risk.
<b>Risk appetite</b>	The amount of risk that the organisations is prepared to accept or be exposed to in the pursuit of its objectives.
<b>Risk assessment</b>	The overall process of risk identification, risk analysis and risk evaluation.
<b>Risk attitude</b>	Organisation's approach to assess and eventually pursue, retain, take or turn away from risk.
<b>Risk aversion</b>	Attitude to turn away from risk
<b>Risk avoidance</b>	An informed decision not to become involved in, or to withdraw from, a risk activity, decision, situation or event.
<b>Risk evaluation</b>	The process used to determine risk management priorities by comparing the level of risk against predetermined appetite, tolerance, target risk levels or other criteria.
<b>Risk identification</b>	Process of finding, recognising and describing risks
<b>Risk management</b>	The coordinated activities to direct and control an organisation with regard to risk
<b>Risk management framework</b>	The set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation
<b>Risk management process</b>	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.
<b>Risk owner</b>	The position with the accountability and authority to manage the risk. Risk owners will be a Head of or above. The Risk Owner will ensure the risk is assessed and treated, assign risk control owners and assign risk treatment action owners.
<b>Risk culture</b>	A term describing the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people.
<b>Risk profile</b>	The documented and prioritised overall assessment of a range of specific risks or set of risks faced.

<b>Risk rating criteria</b>	A reference against which the significance or level of a risk is evaluated. The risk rating resulting from the application of the risk assessment ratings on the likelihood of the risk and consequence of a risk.
<b>Risk register</b>	A formal record or repository (system or file) of the risks identified, evaluated and managed by the risk owner.
<b>Risk Register Work Instruction</b>	A document within the Enterprise Risk Management Manual to provide risk owners with step-by-step instructions for identifying, analysing, evaluating, treating and escalating risks to complete a risk register. See Appendix A.
<b>Risk retention</b>	The level of risk ultimately accepted.
<b>Risk sharing</b>	Sharing with another party the burden of loss or consequence from a particular risk.
<b>Risk source</b>	Element which alone or in combination has the intrinsic potential to give rise to risk event. Considered during the risk assessment step.
<b>Risk transfer</b>	Shifting the responsibility or burden for loss to another party usually through contract, insurance or other means.
<b>Risk treatment</b>	Selection and implementation of an action or process identified to address or mitigate a risk. Risk treatments should have a clear deliverable, an owner and a due date. The expected impact of risk treatments on the risk is shown in the after treatment risk rating.
<b>Stakeholder</b>	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
<b>Strategic risk</b>	A source of uncertainty that may arise in pursuit of strategic objectives. The risks and uncertainties associated with carrying out of the strategic objectives as articulated in high level plans; strategic programs/initiatives. Strategic risks arise during strategy formulation and implementation or factors from the external environment that could impact strategy. They are managed by the FOCUS Team/Managing Director.

Table 3 Definitions



## ANNEX A: RISK MANAGEMENT PROCEDURE

The purpose of the Risk Management Procedure is to describe the risk management process adopted by TAFE NSW and mandated in the Enterprise Risk Management Policy in more detail.

This Risk Management Procedure reflects the Australian/New Zealand Standard (AS/NZS) ISO 31000:2018 Risk Management – Principles and guidelines and is aligned with the Internal Audit and Risk Management Policy for the General Government Sector (TPP 20-08). Refer to Figure 2 below for an illustration of the AS/NZS ISO 31000:2018 risk management approach and the five key stages to the risk management process that applies at TAFE NSW.

Following this Procedure will help risk owners manage their risks and maintain their risk register in a manner that is consistent with the TAFE NSW risk management framework.

This Risk Management Procedure should be read in conjunction with:

- Appendix 1 - Risk Register Work Instruction
- Appendix 2 - Risk Register Template
- Appendix 3 - Likelihood Rating Table
- Appendix 4 - Consequence Rating Table
- Appendix 5 - Risk Level Rating Table
- TAFE NSW Risk Appetite Statement

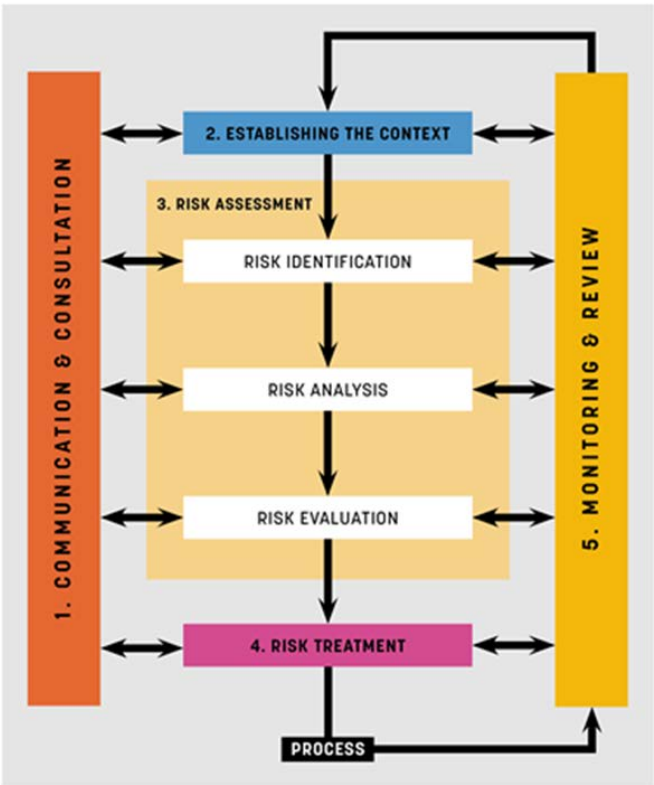


Figure 2: Risk management approach using AS/NZS ISO 31000 Risk Management – Principles and guidelines

## 1 – COMMUNICATION AND CONSULTATION

Effective ongoing communication and consultation with key stakeholders regarding risks and their management is critical to the success of TAFE NSW's enterprise risk management framework.

### Communication

Clear and effective communication is necessary to ensure that the right people receive the right information at the right time, so they can make the best decisions and carry out their risk management responsibilities.

Different people within TAFE NSW have different information needs. For example, staff who are accountable for carrying out actions to deal with risks will need to understand their accountability, the rationale for decisions and why these actions are required.

Other internal stakeholders such as the Managing Director, Chiefs, the TAFE NSW Commission Board and the Audit and Risk Committee will have their own unique information needs, such as an understanding of how risks are managed and reported.

TPP20-08 requires that where a risk has been identified that is likely to impact another agency, the risk should be formally communicated to the affected agency/agencies.

### Consultation

Consulting with internal and external stakeholders can deliver the following benefits:

- The context in which you are operating is fully understood;
- The interests of stakeholders are understood and considered;
- All risks are identified;
- Different areas of expertise are drawn on when analysing and evaluating risks;
- Different views are considered; and
- You can secure endorsement and support for risk treatment plans.

Consultation can be formal or informal. Formal consultation processes may include strategic and business planning sessions, quarterly risk reviews, presentations to FOCUS Team, RLT or SLT meetings, and risk evaluation meeting.

Informal consultation may include less formal meetings, workshops, e-mails, briefings and focus groups.

Communication and consultation with stakeholders is important as they make judgements about risk based on their perceptions. These perceptions can vary due to differences in values, experience, assumptions and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders perceptions should be identified, recorded and taken into account in the decision making process.

Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.

Plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequence (if known) and the measures being taken to treat it.

## 2 – ESTABLISH CONTEXT

The purpose of establishing context is to understand the business environment your risk management process operates in. In turn, this understanding informs the scope and structure for the remaining components of the risk management process including determining what types of risk will be considered and deciding if a risk is tolerable or not.

In establishing the context, we consider a number of factors:

- For strategic risks, TAFE NSW objectives – considering strategy, mission and purpose etc.;
- For operational and project risks, business plans and other specific objectives of the branch, unit, activity or project;
- Performance metrics;
- Internal and external stakeholders;
- Internal factors – organisational size, design and structure, activities (day-to-day and project), experience, capabilities, values, management style, policies, communication, financial position, internal strengths and weaknesses.
- External environment – trends, social, cultural, financial, legal, technological, competitor, political and regulatory influences.

The context of the risk assessment is not recorded on the risk register. It is simply used to help set the scene and parameters of the risk assessment to complete the risk register.

## 3 – RISK ASSESSMENT

Having established the context, you can now begin the process of assessing and treating the potential risks.

Risk assessment is a structured approach to identify and analyse the uncertainties that exist in meeting your objectives. The risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

### *Risk Identification*

Risk identification is the process of finding, describing and recognising uncertainties that might enhance or inhibit your ability to achieve your objectives. Identified risks form the basis of further analysis, evaluation and treatment. Risk identification is therefore a critical aspect of the risk management process.

In identifying risks, you must consider not only threats, but also the risks associated with not pursuing an opportunity, for example, increasing student job readiness by offering courses in remote communities or high migrant areas. Once the risk is identified, any existing controls should be identified at the same time.

The risk identification stage involves thinking through the sources of risks, the potential threats and opportunities, the possible causes and the potential exposure within the context of the objective or strategy being assessed. The next step is documenting the identified risks in a risk register.

The aim of this stage is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

Depending on the context of the risk assessment, there are a number of risk identification techniques to use:

- Brainstorming - Using the personal experiences, skills and knowledge of people to help identify and assess risks;
- Quarterly Risk Reviews – Calling on the skills of internal risk management specialists to assist in identifying emerging or changing risks;
- Business process reviews and work breakdowns – Breaking down areas into smaller processes, activities or sub-processes for a more granular identification of risks;
- Scenario analysis and what-if analysis;
- Risk categories – Identifying risks based on the TAFE NSW risk categories.
- Checklist – Identifying risks via a checklist of standard risks;
- SWOT analysis (Strength, Weaknesses, Opportunity, Threats);
- Environmental scanning – Using PESTEL analysis (Political, Economic, Social, Technological, Environmental, Legal) to consider risks from different perspectives and emerging risks;
- Review of actual incidents and issues identified - Incidents, breaches and issues including ‘near misses’ may be leading indicators to a major problem or potential risk; and
- Commissioned risk review – Calling on external specialists to support risk identification.

The key questions and considerations when identifying risks are:

- What can happen?
- How can it happen?
- Where can it happen?
- When can it happen?
- Why can it happen?
- What is the impact?
- Who is responsible for managing the risk?

**Risk Description**

Once the risk has been identified, describe the risk event and consequence. What can happen? What is its impact?

HINT: Often trying to find the right words to describe the actual risk can be a tricky. As a guide:

- Describe the risk event and the objective affected. E.g. “failure to meet contract obligations resulting in loss of contract and revenue.”
- A ‘broken control’ is not a risk. E.g. “bank reconciliation not done” is a broken control or a control that is not working or performing as desired. Whilst broken controls can be a source of risk, management are responsible for ensuring all internal controls are working effectively.
- Refer to the bow-tie diagram in Figure 3 below and how it can help clearly display the links between the potential causes, preventative and mitigating controls and consequences of a risk.

REMEMBER - risks that are not identified at this stage will not be included in further analysis.

### Risk Analysis

Once risks have been identified, they are then examined in more detail. Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur.

#### Sources of risk

Sources of risk are factors that can cause the risk. It is important to consider the potential causes and sources of a risk to help address and control the risk in the next stage of the risk assessment. Documenting sources of risk will help when it comes to risk control and treatment actions. It is often easier to think of controls for individual sources of risk than a high-level risk description.

Some sources of risk can include:

- Organisational capabilities
- Staff knowledge and expertise
- Conduct/human behaviour
- Processes and systems
- Data
- Priorities
- Commercial/legal relationships
- Political/legal influences
- Management activities
- Technology/technical issues
- Interface or shared responsibilities
- Local or specific variables

The bow-tie diagram is a useful tool in risk analysis. The diagram clearly displays the links between the potential causes, preventative and mitigating controls and consequences of a major risk. See Figure 3 for a simple bow-tie diagram.



Figure 3: Bow-tie diagram

### Risk Category

To determine the most suitable risk category, think about the most likely consequence of the risk description. For example, poor maintenance of electrical equipment may have 'Regulatory' consequence to TAFE NSW, but the most likely consequences are 'Safety' and therefore the most appropriate risk category to use is 'Safety'.

TAFE NSW has adopted the following seven risk categories:

Risk Category	Consequences to be covered
<b>Safety</b>	Employee, contractor, student and visitor health and safety; wellbeing; mental and physical health; work health and safety systems; injury management and prevention
<b>Regulatory</b>	Compliance regime; legislation; RTO accreditation; regulator relationship; standards compliance; contractual compliance; insurance and risk management; preparation for new and/or amended legislation; lobbying of regulators; governance
<b>Probity</b>	Values development and implementation; fraud and corruption; ethical/unethical behaviour; public interest disclosures; gifts and benefits; misuse of resources; maladministration; cyber security
<b>Customer</b>	Student and industry/employer customer experience; delivery of education and training program; design, development and implementation of business policies, processes, procedures, and technologies to support the administrative and customer experience and student-centred services; student safety; business continuity planning; disruption to service delivery; student completions
<b>Financial</b>	Revenue (sources, mix of sources, amount); cost/expenditure (amount, type), budget and financial performance reporting, grant management
<b>Reputation</b>	Stakeholder management; community engagement; community awareness; government relations; image of TAFE NSW; media management; brand management
<b>Workforce</b>	People; staff wellbeing; internal capability; external contractors; organisational culture; staff morale; change management; employee expectations; unplanned employee departures; loss of key staff; succession planning; workforce planning and capability development

Table 4 TAFE NSW Risk Categories

**Risk Appetite**

Risk appetite is the amount of risk that TAFE NSW is prepared to accept or be exposed to in the pursuit of its objectives. Risk appetite for a particular risk category is predetermined by the Managing Director and FOCUS Team and presented in the Risk Appetite Statement. This cannot be changed by risk owners.

**Inherent risk**

Inherent risk is the baseline level risk that is inherent in the activity before considering the existence of, or quality of controls. It is determined by combining the likelihood and consequence ratings together.

**Likelihood**

The **likelihood** of occurrence is the chance or probability of an event occurring. When considering the likelihood of a risk occurring, you should consider a number of things:

- Anticipated frequency of activity i.e. how often is the activity performed
- Duration of activity.

- The external environment.
- History of previous events within TAFE NSW or other similar type organisations, e.g. other Registered Training Organisations (RTOs).

Refer to Appendix 3 for the Likelihood Rating Table.

**Consequence**

The **consequence** is the impact of the risk event. Evaluation of the consequence of the risk event is based on the risk category selected.

Refer to Appendix 4 for the Consequence Rating Table.

**Risk Evaluation**

Once you have determined the inherent risk, you need to identify controls that currently exist to modify risk by:

- Preventing or reducing the likelihood of an undesirable risk event,
- Mitigating the consequences of such a negative risk event,
- Increasing the likelihood of realising an opportunity, or
- Increasing the expected gain from such a positive event.

A **control** will include any policy, procedure, system or action that is effective at changing the level of risk by changing the likelihood, consequence or both. Sample controls are shown in table 2 below.

Strong **controls** have a bigger impact on the risk. You obviously need fewer strong controls than weak controls to get the same risk control benefit.

Controls that reduce likelihood for negative risks	Controls that reduce consequences for negative risks
Policies and procedures	Oversight, monitoring and corrective actions
Adequate resourcing including provision of subject matter expertise	Personal Protective Equipment (PPE)
Structured training e.g. induction, on-the-job	Contract conditions
Supervision e.g. observation	Disaster planning
Delegations, separation of duties e.g. reviewer and authoriser and system controls e.g. user access limits	Stakeholder engagement and communications including public relations
Preventative maintenance	Insurance

Controls that increase likelihood for positive risks	Controls that increase consequences for positive risks
Clear strategy and accountabilities	Structured and active change management
Project management and project governance	Investment in new technology
Testing of a new product	Allocation of resources

Table 5: Example of how controls impact on likelihood and consequences

Once you have identified these controls, you need to assess the control’s effectiveness to determine the current risk rating. Control effectiveness is determined by considering:

- Whether the controls are well designed – for example, are they capable of managing the risk and maintaining it at an acceptable or tolerable level?
- Whether the controls are operating as intended. Have they been, or can they be, proven to work in practice? Are they cost-effective?

To determine control effectiveness, think about the quality of documented policies and procedures, adequacy of training, staff turnover, and recent issues - see Table 3 below as a guide on control effectiveness.

Level	Description and further action	Design effectiveness	Operational effectiveness
<b>Substantially effective</b>	Existing controls address risk, are in operation and are applied consistently. Management is confident that the controls are effective and reliable. Ongoing monitoring is required	Y	Y
<b>Partially effective</b>	Controls are only partially effective, require ongoing monitoring and may need to be redesigned, improved or supplemented.	N Y	Y N
<b>Largely ineffective</b>	Management cannot be confident that any degree of risk modification is being achieved. Controls need to be redesigned.	N	N

Table 6: Guide to control effectiveness



**Current risk** is the level of risk after considering the effectiveness of existing controls. As most controls should be reasonably effective, the level of current risk will in almost all cases be lower than inherent risk.

**Within Risk Appetite?**

Ultimately, the level of current risk is compared to TAFE NSW’s risk appetite to determine if the level of risk is acceptable i.e. within risk appetite.

Where current risk is **within** risk appetite, no further or immediate action is required other than simply ensuring the risk assessment has been performed diligently and the risk is continually monitored.

Where the current risk level is **outside** risk appetite, the risk owner must:

- a. Develop an appropriate Risk Treatment Plan to implement additional actions to control the risk – refer to 4 - Risk Treatment
- b. Communicate and consult with key stakeholders (Principal Risk Advisors, TAFE NSW Head of Risk, other managers) to provide technical guidance; and
- c. Assess the expected future risk rating and record in the after-treatment risk register columns. This should be your best estimate of where the risk will be once the proposed treatment actions have been fully delivered.

Where a risk is likely to impact another agency, the risk should be formally communicated to the affected agencies. Refer to 4 - Risk Treatment for more information.

REMEMBER: No one, including a risk owner can accept a risk outside TAFE NSW’s risk appetite.

**4 – RISK TREATMENT**

When a risk is currently outside TAFE NSW’s risk appetite, further action is required. This part of the risk management process seeks to control these risks by developing a treatment action plan that addresses underlying causes, assesses the treatment’s effectiveness and, if the after treatment risk is still considered unacceptable or intolerable, generates an escalation to more senior management.

These actions typically involve implementing additional controls or strengthening the controls already in place.

It is also important to ensure the residual risk level is not too low, as this may result in an opportunity being missed, or may mean that too stringent controls have been applied. If the residual risk is more than one level below the Risk Appetite, more controlled risk can be taken in this area to achieve objectives.

***Implementing additional controls/treatment actions***

Implementing additional treatment actions aims to modify or enhance the existing controls to change the likelihood and/or consequences to within risk appetite.

The purpose of risk treatment is to identify the most appropriate and cost-effective strategies within the risk owner’s delegations and implement them.

Risk owners need to weigh the costs of implementing a treatment against the benefits it is likely to deliver. Issues to consider include:

- The financial and other resources required to implement the treatment;
- The feasibility (including timing) of implementing the treatment;
- How effective the treatment is likely to be in impacting the risk rating;
- The potential impact of the treatment on stakeholders' values, perceptions and interests – as some risk treatments may be more acceptable to some stakeholders than others;
- Whether the treatment will compromise internal policies or be in conflict with any legal, regulatory or other obligations;
- Possible unintended consequences of the treatment – risk treatments themselves may affect other existing risks, or may introduce new risks (known as secondary risks);
- Your ability (including resources and delegations) to effectively implement the risk treatment.

When choosing risk treatments the risk owner should consider whether:

- Risk treatments can be implemented effectively and in a timely manner; and
- Performance and success measures can be assigned to the risk treatment so that delivery can be monitored and reviewed for ongoing control effectiveness.

Information documented in risk treatment plans should include:

- The expected outcome of the treatment i.e. what control will be delivered;
- The action(s) to be undertaken to practically implement the selected treatment;
- Accountabilities and responsibilities for delivering the action;
- Performance measures – measures to evaluate the effectiveness of the controls and evaluation criteria
- The due date for delivery of the enhanced level of risk control.

Once a risk treatment plan is developed the risk owner must evaluate the expected after treatment risk level. This third round of risk rating will evaluate the expected likelihood and expected consequence after completion of all actions within the risk treatment plan.

**After treatment risk** is the level of risk after considering the effectiveness of all actions within the risk treatment plan. As most treatment actions should be reasonably effective, the level of after treatment risk will in almost all cases be lower than current risk.

## ALARP

When considering the most appropriate risk treatment options for threats and undesirable risk events, risk owners may consider the concept of “As Low as Reasonably Practicable” (ALARP).

ALARP as illustrated in Figure 5 is the point where the risk is negligible, or at least at a level where it can be managed by routine procedures. ALARP is the level of risk that is tolerable and cannot be reduced further without expenditure of resources, time and effort being disproportionate to the benefit gained or where the solution is impractical to implement.

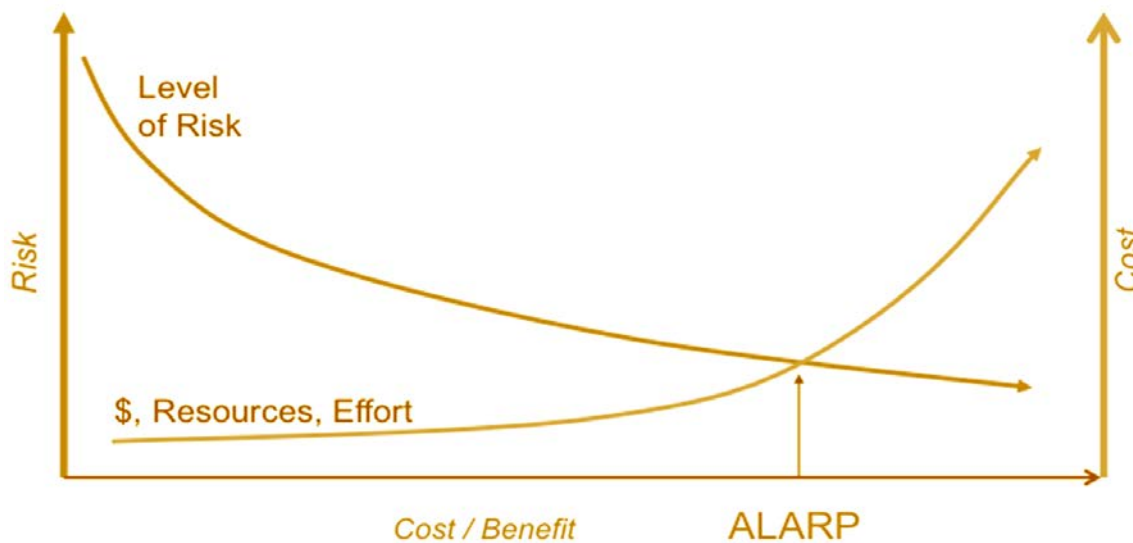


Figure 5: The ALARP concept

### Other risk treatment options

#### Avoiding the risk

Applicable to negative consequence risks. This option involves deciding not to start or continue with the activity that gives rise to the risk. This will eliminate the risk. However, this is not always possible and may adversely impact stakeholders. Other risk treatment options should be considered.

#### Transferring the risk

This option involves transferring part or all the risk to another party or parties (through contracts, insurance and risk financing arrangement). For example, an activity can be outsourced to another party who have greater capabilities in mitigating the risk.

**Warning:** Outsourcing the activity will NOT always eliminate the risk to TAFE NSW. All activities and associated risks transferred should be carefully considered and only undertaken within the delegated authority of the risk owner and in accordance with TAFE NSW Written Direction.

### Escalating risks

Risk owners MUST escalate risks to FOCUS Team/Managing Director when:

- The after-treatment rating for a risk is outside risk appetite.
- A risk owner does not have sufficient delegation/resources to treat a risk.
- A risk is impacting or likely to impact another NSW Government agency or cause substantial reputational harm to TAFE NSW.

#### When to escalate a risk

##### 1. Risk is outside risk appetite after treatment

Where the **after-treatment** risk level is judged to be outside risk appetite, the risk owner must:

- a. Develop an appropriate Risk Treatment Plan to implement additional actions to control the risk;
- b. Communicate and consult with key stakeholders (Principal Risk Advisor, TAFE NSW Head of Risk, other managers) to provide technical guidance; and
- c. Assess the expected future risk rating and record in the after-treatment risk register columns. This should be your best estimate of where the risk will be once the proposed treatment actions have been fully delivered.

## 2. Risk owner does not have sufficient delegation/resources to treat a risk

Risks are also escalated when a risk owner does not have sufficient delegation or resources to implement a Risk Treatment Plan to mitigate a risk. Escalation of the risk to FOCUS Team/Managing Director will ensure the risk is considered by the Managing Director and risk mitigations actions considered and approved by the Managing Director where appropriate.

## 3. Risk impacting another agency

Where a risk has been identified that is likely to impact other agencies, the risk should be formally communicated to the affected agency or agencies by the Managing Director or Chief Officer via the TAFE NSW Executive and Ministerial Liaison Unit.

### *How to escalate a risk*

The advice of the Head of Risk or Principal Risk Advisor should be sought before escalating a risk to the FOCUS Team.

Where a risk is escalated to FOCUS/Managing Director, a FOCUS Briefing Paper should be prepared and a copy of the risk register for the risks outside risk appetite included.

The paper should explain why the risk owner cannot develop additional treatment actions to bring the risk within appetite. The paper should also make clear what action is requested from the FOCUS Team. The Head of Risk will usually provide FOCUS with an expert opinion and recommendation to support the escalation consideration.

The risk will be considered by FOCUS/Managing Director and may be rejected and returned to the risk owner for further work. If accepted the following outcomes are possible:

1. The activity giving rise to the risk may be avoided.
2. The Risk Treatment Plan proposed by the risk owner is within their delegations and is accepted by the Managing Director.
3. The Risk Treatment Plan proposed by the risk owner is outside their delegations and is refined and approved by the Managing Director.
4. No Risk Treatment Plan will reduce risk to within risk appetite and the Managing Director accepts the risk as outside risk appetite. However, where a risk outside risk appetite is accepted:
  - a. The Managing Director must inform the TAFE Commission Board through the Audit and Risk Committee of the risk;
  - b. The Managing Director may also escalate the risk to the Minister for immediate consultation.

The FOCUS Team or Managing Director decision will be recorded in the relevant meeting minutes.

### ***Completed treatment actions***

Once the risk treatment action is completed, the risk treatment can be:

- Transferred to the 'current control' column in the risk register;
- Level of current risk should be re-rated again to reflect the new control; and
- Risk Treatment Plan actions can be deleted.

## **5 – MONITORING AND REVIEW**

### ***Monitoring and review of specific risks***

In the changing environment in which TAFE NSW operates in, few risks identified on the risk register will remain static and new risks will emerge.

Risk monitoring and review is an integral step in the risk management process. It enables risk owners to proactively identify changes on the risk register.

Risk monitoring and review is a continuous process and can be undertaken either ad-hoc or as part of a formal scheduled review process. At minimum:

- Strategic risks are reviewed monthly by the FOCUS Team
- Project risks are reviewed monthly by the designated Program Manager
- Operational risks are reviewed quarterly by the nominated risk owner

All risk registers with outstanding Risk Treatment Plans should be monitored at least monthly by the risk owner and progress reported to the FOCUS Team – refer to 4 Risk Treatment.

When monitoring and reviewing risks and updating the risks register, risk owners should consider:

- Existence of current risks
- Whether the likelihood or impact of current risks have changed
- Consideration of new and emerging risk
- Consider any recent incidents that should be identified and formally assessed in the risk register
- Reevaluate effectiveness of existing controls
- Consider the need for new controls
- Review the progress of risk treatment plans and reassess priorities
- Need to alert or escalate new or emerging risks to FOCUS

By monitoring risks, controls and Risk Treatment Plans, we can ensure that the risk register is reflective of the risk profile and risks are being managed in accordance with the TAFE NSW risk management framework.

### ***Monitoring risks outside appetite and Risk Treatment Plans***

Risks outside risk appetite and Risk Treatment Plan are monitored regularly, usually monthly. The risk treatment action owner has the responsibility to report progress on the action to the risk owner. The risk owner has the responsibility to oversee the delivery of risk controls (existing and new).

FOCUS Team members must report the status of risk treatment actions within their group or branches to the Managing Director. This report should include the number of actions that are overdue and the number that are at risk of non-delivery i.e. are likely to go overdue or will not deliver the level of risk control expected. The relevant General Manager will comment on all overdue and at risk treatment actions.

***Monitoring and review of the risk management framework***

Ongoing monitoring of the risk management framework is part of the continual improvement process. The TAFE NSW Enterprise Risk Management Plan will outline all the risk management activities including monitoring and review.

## APPENDIX 1 – RISK REGISTER WORK INSTRUCTION

The purpose of this Risk Register Work Instruction is to provide step-by-step instructions for completing the risk register to help risk owners maintain their risk register in a manner that is consistent with the TAFE NSW Risk Management Procedure. To complete the risk register, you will need:

- Annex A - Risk Management Procedure
- Appendix 2 - Risk Register Template (available in Content Manager)
- Appendix 3 - Likelihood Rating Table
- Appendix 4 - Consequence Rating Table
- Appendix 5 - Risk Level Rating Table

### STEP 1: RISK IDENTIFICATION

Risk identification is the process of identifying risks in the context you have established. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

**Risk Number (#)** – For reference purposes.

**Risk Description** – Describe the risk and its impact. In the format “The <source of risk> may cause the < risk event> which positively/negatively impacts the < objective affected>”. For example, highly competitive labour market causes and inability to attract and retain skilled staff which negatively impacts service delivery.

**Risk Owner** – The position with the accountability and authority to manage the risk. Risk owners will be a *Head of or above*.

**Sources of Risk** – Describe factors that can cause the risk. How can the risk occur? This could be a list including both likely and improbably causes.

**Risk Category** – Consider the most likely consequence of the risk and select the risk category impacted. The risk categories are predetermined and cannot be changed as they are aligned to the categories used in the TAFE NSW Risk Appetite Statement and the risk consequence table.

**Risk Appetite** - The amount of risk that TAFE NSW is prepared to accept in the pursuit of its objectives. Risk appetite for each risk category is predetermined by the Managing Director and FOCUS Team and documented in the TAFE NSW Risk Appetite Statement. Risk appetite for a category cannot be changed. The risk appetite will be filled automatically in the template risk register once a risk category is selected.

#### ***Risk Assessment - Inherent***

**Likelihood** - The probability of the risk event occurring before considering any current controls.

Refer to Appendix 3 for the Likelihood Rating Table

**Consequence** - The impact of the risk event before considering any current controls. Based on the risk category selected.

Refer to Appendix 4 for the Consequence Rating Table

**Rating** - Inherent Risk is the level of risk before considering any current controls. The level of inherent risk is based on your selection of 'likelihood' and 'consequence' ratings.

The rating will be filled automatically in the template risk register once the likelihood and consequence are selected. Refer to Appendix 5 for the Risk Level Rating Table.

## STEP 2: RISK ASSESSMENT

This step involves identifying and considering the current controls that are working effectively to mitigate the risk and rerating the risk again.

### **Risk Control**

**Current Controls** – List the current and most effective controls that are already embedded within TAFE NSW current business processes which contribute to mitigating the risk and causes identified.

**Control Owner** – The position with accountability and authority to deliver and maintain the control. Control owners will be a *team leader* or above.

### **Risk Assessment - Current**

**Likelihood** - The probability of an event occurring after considering 'current controls'.

Refer to Appendix 3 for the Likelihood Rating Table

**Consequence** - The impact of the risk event after considering 'current controls'.

Refer to Appendix 4 for the Consequence Rating Table

**Rating** - Current Risk is the level of risk after considering the effectiveness of 'current controls'. The level of residual risk is based on your selection of revised 'likelihood' and revised 'consequence' ratings.

The rating will be filled automatically in the template risk register once the likelihood and consequence are selected. Refer to Appendix 5 for the Risk Level Rating Table.

**Within Risk Appetite?** – Compare the rating of current risk to TAFE NSW's risk appetite to determine if the current risk level is within risk appetite.

Where current risk is within risk appetite, no further or immediate action is required other than simply ensuring the risk assessment has been performed diligently.

Where current risk is not within risk appetite, further action is required by the risk owner. These actions can include:

- Risk treatment actions that will deliver new or strengthened controls;
- Avoiding the risk - deciding not to start or continue with the activity that gives rise to the risk. This will eliminate the risk.
- Transferring the risk.



**Please Note:**

- No-one, including a risk owner can accept a risk outside the TAFE NSW risk appetite.
- Where a risk has been identified that is likely to impact other agencies, the risk should be formally communicated to the affected agency or agencies by the Managing Director via the TAFE NSW Executive and Ministerial Liaison Unit.

**STEP 3: RISK TREATMENT**

The purpose of risk treatment is to identify the most appropriate risk modification strategies and implement them.

***Develop action plan***

- **Action** - Identify the specific risk treatment or risk transfer actions.
- **Owner** - The name of the person responsible who has the delegated authority to implement the action.
- **Due Date** - Set the due date to implement the action.

***Risk Assessment – After Treatment***

**Likelihood** - The expected probability of an event occurring after considering ‘current controls’ and delivery of all ‘actions’.

Refer to Appendix 3 for the Likelihood Rating Table

**Consequence** - The expected impact of the risk event after considering ‘current controls’ and delivery of all ‘actions’.

Refer to Appendix 4 for the Consequence Rating Table

**Rating** – After Treatment Risk is the level of risk expected after considering the effectiveness of ‘current controls’ and delivery of all ‘actions’. The after-treatment risk is based on your selection of revised ‘likelihood’ and revised ‘consequence’ ratings.

The rating will be filled automatically in the template risk register once the likelihood and consequence are selected. Refer to Appendix 5 for the Risk Level Rating Table.

**Within Risk Appetite?** – Compare the level of after treatment risk to TAFE NSW’s risk appetite level to determine if the expected level of risk is within risk appetite.

Where after treatment risk is within risk appetite, no further or immediate action is required other than ensuring the risk assessment has been performed regularly and diligently.

Where after treatment risk is not within risk appetite the risk must be escalated to FOCUS Team.

**STEP 4: ESCALATION**

The purpose of escalation is for the risk owners to communicate risks that are outside TAFE NSW’s risk appetite to the Managing Director. Ultimately, it is the Managing Director who accepts risks outside risk appetite in consultation with the TAFE Commission Board, the Audit and Risk Committee and the Minister. This is done through the FOCUS Team governance arrangements.

## APPENDIX 2: RISK REGISTER TEMPLATE

The template risk register is an excel spreadsheet and is available on the TAFE NSW Intranet. The template contains protected cells and autofill cells. Assistance with using the template is available from the Risk Unit.

The risk register contains the following sections:

STEP 1: RISK IDENTIFICATION						STEP 2: RISK ASSESSMENT						STEP 3: RISK TREATMENT						STEP 4: ESCALATION			
						RISK ASSESSMENT - INHERENT		RISK MITIGATION		RISK ASSESSMENT - CURRENT				TREATMENT ACTION PLAN			RISK ASSESSMENT – AFTER TREATMENT				
#	Risk Description	Risk Owner	Sources of risk	Risk Category	Risk Appetite	Likelihood	Consequence	Rating	Current Controls	Control Owner	Likelihood	Consequence	Rating	Within Risk Appetite?	Action	Action Owner	Due Date	Likelihood	Consequence	Rating	Within Risk Appetite?
1									1.1 1.2 ...	1.1 1.2 ...					1.1 1.2 ...	1.1 1.2 ...	1.1 1.2 ...				
2									2.1 2.2 ...	2.1 2.2 ...					2.1 2.2 ...	2.1 2.2 ...	2.1 2.2 ...				
3									3.1 3.2 ...	3.1 3.2 ...					3.1 3.2 ...	3.1 3.2 ...	3.1 3.2 ...				
4									4.1 4.2 ...	4.1 4.2 ...					4.1 4.2 ...	4.1 4.2 ...	4.1 4.2 ...				
5									5.1 5.2 ...	5.1 5.2 ...					5.1 5.2 ...	5.1 5.2 ...	5.1 5.2 ...				
6									6.1 6.2 ...	6.1 6.2 ...					6.1 6.2 ...	6.1 6.2 ...	6.1 6.2 ...				
7									7.1 7.2 ...	7.1 7.2 ...					7.1 7.2 ...	7.1 7.2 ...	7.1 7.2 ...				

## APPENDIX 3: LIKELIHOOD RATING TABLE

Rating	Likelihood	Description	Qualification
5	Almost Certain	The event is expected to occur in normal circumstances. There has been frequent past history.	Several times a year. Greater than 90% chance of occurring.
4	Likely	The event will probably occur. Some recurring past event history.	Once a year. Between 70% and 90% chance of occurring.
3	Possible	The event may occur sometime. Some past warning signs or previous event history.	Once every 5 years. Between 30% and 70% chance of occurring.
2	Unlikely	The event could occur in some circumstances. No past event history.	Once every 20 years. Between 5% and 30% chance of occurring.
1	Rare	The event may occur but only in exceptional circumstances. No past event history.	Once every 50 years or more. Less than 5% chance of occurring.

## APPENDIX 4: CONSEQUENCE RATING TABLE

Risk Categories	Risk Consequence				
	Negligible	Minor	Medium	Major	Severe
Safety	Minor concerns raised. Very minor incident or near miss.	Minor illness or injury from normal activities treated by first aid.	Customer medical treatment injury. Near miss that identifies weakness of current controls.	Customer hospitalisation. Employee or contractor lost time injuries or hospitalisation.	Customer, employee or contractor death. Near miss that identifies significant failures or weaknesses in current controls.
	Negligible improvement in lead indicators or safety programs.	Minor improvement in lead indicators or safety programs.	Significant improvement in lead indicators or safety programs.	Major innovation delivering improvement in safety outcomes for employees, students and/or contractors.	Significant innovation delivering improvement in safety outcomes for employees, students and/or contractors. Greatly exceed stakeholders' expectations.
Regulatory	Minor complaint or compliance issue. Resolved locally. Little or no effect on operations.	Isolated regulatory breach, incident or legal issue. Resolved at (R)GM/General Counsel level.	Major regulatory breach. Significant incident, complaint or legal action. Formal crisis management instigated.	Systemic regulatory breaches. Shutdown of a service or loss of RTO scope. One-off large fine. Ministerial inquiry.	Shutdown of multiple services or loss of RTO registration. Substantial fines. Prosecution of organisation or individual. Parliamentary scrutiny.
	Response submitted to correspondence from regulator, little or no expected effect.	Process improvement identified and notified to regulator, may result in some action.	Significant process improvement identified and discussed with regulator, agreement on some level of action	TAFE NSW is a key stakeholder in consultation around legislative review, and feedback incorporated into changes	Minister influences parliament to resolve changes to regulatory framework

Positive Outcomes	Negative Outcomes
-------------------	-------------------

Risk Categories	Risk Consequence				
	Negligible	Minor	Medium	Major	Severe
Probity	Negligible non-compliance with internal controls, little or no effect on operations.	Minor non-compliance with internal controls, problem investigated and solved at local level	Systemic non-compliance with internal controls or a minor non-compliance in multiple branches, resulting in Internal Audit or Legal investigation.	Significant systemic non-compliance with internal controls resulting in external investigation e.g. Police or ICAC	Finding of corruption or wrongdoing by external agency, Ministerial enquiry, staff misconduct resulting in termination
	Negligible improvement in internal controls, example of ethical behaviour, demonstration of TAFE NSW values	Minor improvement in internal controls, ethical behaviour that is starting to exceed TAFE NSW standards and values	Moderate improvement in internal controls, ethical behaviour that exceeds TAFE NSW standards and values.	Major, significant improvement in internal controls, ethical behaviour that greatly exceeds TAFE NSW standards and values.	Best practice improvement in internal controls, ethical behaviour that significantly exceeds TAFE NSW standards and values and is recognised by the Executive.
Customer	Education and training program outcome affected and resolved by routine operations.	Education and training program outcome compromised with minor impact and managed internally. Customer first aid injury.	Delivery of academic or community/program outcomes compromised. Significant review or changes to programs required. Customer medical treatment injury.	Outcome of a major program not achieved resulting in decline of enrolments/funding. Significant review of programs required. Customer hospitalisation.	Programs cannot be delivered resulting in significant decline in academic/community outcomes. Significant damage to reputation of vocational education. Ministerial enquiry. Customer death.
	Negligible improvement in programs, customer outcomes or industry engagement, changes implemented by routine operations. <1% increase in student completion rates	Minor improvement in programs, customer outcomes or industry engagement, minor improvement in efficiency or effectiveness. 1% - 5% increase in student completion rates.	Significant improvement in programs, customer outcomes or industry engagement, significant improvements to delivery or process efficiencies. 5% - 10% increase in student completion rates.	Major innovation delivering improvement in customer outcomes, industry engagement or major increase in customer satisfaction and participation rates.	Significant innovation delivering improvement in customer outcomes, industry engagement or major increase in customer satisfaction and participation rates. Greatly exceed customer expectations.

Positive Outcomes	Negative Outcomes
-------------------	-------------------

Risk Categories	Risk Consequence				
	Negligible	Minor	Medium	Major	Severe
Financial	Loss, error or omission <1% of annual budget. No financial forecasting required.	Loss, error or omission of 1% – 5% of annual budget. Financial reforecasting required.	Loss, error or omission of 5% - 10% of annual budget. Urgent and material financial re-forecasting required.	Loss, error or omission of 10% - 15% of annual budget. Delayed payment to staff and creditors.	Loss, error or omission >15% of annual budget.
	Saving or benefit <1% of appropriate baseline amount e.g. program or annual budget or projected revenue	Saving or benefit of 1% – 5% of appropriate baseline amount e.g. program or annual budget or projected revenue	Saving or benefit of 5% - 10% of appropriate baseline amount e.g. program or annual budget or projected revenue	Saving or benefit of 10% - 15% of appropriate baseline amount e.g. program or annual budget or projected revenue	Saving or benefit >15% of appropriate baseline amount e.g. program or annual budget or projected revenue
Reputation	Attention from minor stakeholder with little or no publicity. Resolved locally. Little or no effect on operations.	Local adverse publicity. Visible dissatisfaction from public or key stakeholder. Limited localised media or local member interest. Specific internal reporting.	State wide adverse publicity. Short term damage, public embarrassment, restricted negative publicity from local media. Internal inquiry. Formal crisis management instigated.	Sustained state wide adverse publicity. Regular mainstream media reports. Community dissatisfaction. Ministerial inquiries, questions in Parliament.	Resignation and or removal of Minister, Board member(s) or senior staff. Broad public concern/outrage. Continuous media coverage. Parliamentary Inquiry/Independent Review
	Modest positive publicity in local area	Local positive publicity with visible satisfaction expressed by the public and key stakeholders	State wide positive publicity with visible recognition from stakeholders.	Sustained state wide positive publicity and subsequent increase in level of enquiry/ enrolments.	Recognised by multiple stakeholders as the leader in education. Continuous state wide positive publicity, sustained increases in level of enquiry and subsequent enrolments

Positive Outcomes	Negative Outcomes
-------------------	-------------------

Risk Categories	Risk Consequence				
	Negligible	Minor	Medium	Major	Severe
Workforce	Localised minor wellbeing concerns. Resolved locally. Little or no effect on operations.	Short term, minor localised impact on employee workload, engagement or morale.	Loss of a key local staff, major localised impact on employee workload, engagement or morale. Local industrial action.	Loss of multiple staff or key management. People morale issues in multiple locations. State-wide industrial action.	Organisation wide impact on employee workload, engagement or morale. Industrial action affecting state-wide service delivery.
	Variable cultures and quality of workforce incident reporting. Organisational health survey indicates 50% or above satisfaction rate.	Most areas with a good culture; most staff reporting incidents; many staff engaged, organisational health survey indicates 60% or above satisfaction rate.	Good culture across a Region/Branch; leaders setting clear expectations, staff proactively reporting incidents. Organisational health survey indicates 70% or above satisfaction rate	Strong culture and leaders deal proactively with non-compliance and poor behaviours. Organisational health survey indicates 80% or above satisfaction rate	Very strong culture, leadership and staff engagement. Focus on organisational continuous improvement. Organisational health survey indicates 90% or above satisfaction rate.



## APPENDIX 5: RISK LEVEL RATING TABLE

Likelihood	Consequence				
	1 Negligible	2 Minor	3 Medium	4 Major	5 Severe
5 Almost Certain	Moderate	High	High	Very High	Very High
4 Likely	Low	Moderate	High	High	Very High
3 Possible	Low	Moderate	Moderate	High	High
2 Unlikely	Very Low	Low	Moderate	Moderate	High
1 Rare	Very Low	Very Low	Low	Low	Moderate

NOTE: The 2020 Risk Appetite amended the terminology to be used in the Risk Appetite, see below for the updated wordings for each level:

Previous terminology	New terminology
Very High	Seek
High	Encouraging
Moderate	Open
Low	Cautious
Very Low	Avoid



**TAFE**<sup>NSW</sup>