POLICY

PPMF | TAFESA | 146

Title	Risk Management Policy & Framework

Contact Officer at version effective date

Position	Manager, Internal Audit and Risk
Phone	(08) 7210 3589

Table of Contents

TAFE SA Policies are issued under the TAFE SA Policy Management Framework. They are binding on all TAFE SA employees.

Policy Owner: Manager, Internal Audit and Risk

Version 6.0 Version effective date: 30/7/2019

1 Policy

TAFE SA is committed to effectively managing risks in order to protect itself and its employees, the government and Minister from situations or events that have the potential to prevent it from achieving its strategic and operational objectives. TAFE SA will achieve this by:

- applying consistent risk management principles and practices across the organisation;
- aligning risk identification activities with the strategies and objectives of TAFE SA;
- adopting a practical approach that carefully plans for and prioritises risks and balances the costs and benefits of action;
- ensuring all significant decisions are supported by effective risk management processes;
- encouraging all employees to report and take ownership of their own risks within their span of control;
- allocating responsibility and accountability for risk management at appropriate levels within the organisation;
- allocating adequate risk management resources;
- monitoring risk management performance; and
- continuing to improve risk management practices within TAFE SA.

2 Scope

The Risk Management Policy & Framework applies to all TAFE SA staff.

3 Definitions

Consequence	The outcomes of an event affecting objectives.
Control	An existing process, policy, practice or other action which reduces the likelihood and/or potential consequences of a risk.
Current level of risk	The estimated level of risk post consideration of existing controls.
Event	Occurrence or change of a particular set of circumstances.
Key risk	Those risks fitting the description of significant, relevant, pertinent and important.
Likelihood	The chance of something happening.
Level of risk	The magnitude of a risk expressed in terms of the combination of consequences and the likelihood of the risk occurring.
Retirement	Formal close-out of risks which are no longer relevant.
Risk	The effect of uncertainty on objectives.

	Risk can be described as something that may happen in the future that can have a negative or positive impact on the performance of an organisation or division.
Risk acceptance	An informed decision to accept the consequences of a particular risk without further treatment.
Risk appetite	A measurement of the tendency or inclination for risk taking or risk aversion, normally expressed with the Consequence Scale.
Risk assessment matrix	The tool used for assessing, ranking and prioritising the level of risk by defining the ranges for consequence and likelihood.
Risk management	Coordinated activities to direct and control and organisation with regard to risk.
Risk owner	The person with the most appropriate level of accountability and authority for managing a risk.
Risk profile	Refers to a collection of risks and describes the overall level of risk relating to that collection.
Risk rating	The risk rating is determined by cross-referencing the anticipated consequence of the risk with the likelihood (can also be referred to as Level of Risk). Risks are rated at two levels – post controls (Current Risk Rating) and post treatments (Treated Risk Rating).
Risk register	A tool for recording the details of identified risks and provides a picture of the risks impacting an organisation, division or unit. Includes Strategic Risk Registers and Operational Risk Registers.
Risk source	Element which alone or in combination has the potential to give rise to risk
Risk tolerance	The level of risk an organisation is prepared to take to achieve its objectives.
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Treated level of risk	The estimated level of risk post consideration of existing controls and (planned) treatments.
Treatment	Proposed mitigating actions designed to reduce the Current Risk Level of a risk. Once completed, treatments become controls as they reduce the level of risk.
Treatment owner	The officer responsible for actioning a treatment. (Note: The treatment owner may be different to the risk owner)

4 References

ISO 31000:2018	Risk Management –Guidelines
ASX Corporate Governance Principles	Principle 7 – Recognise and Manage Risk
SA Government	Risk Management Policy Statement
Treasurer’s Instructions	TI2: Financial Management

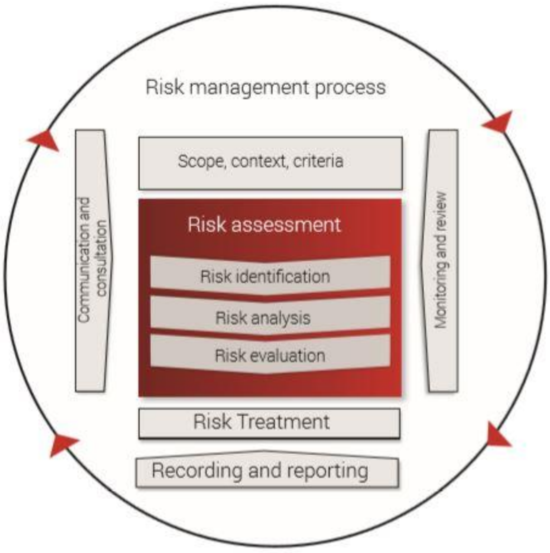
5 Framework

The framework below provides the necessary foundations and organisational arrangements for managing risk across TAFE SA. It describes the key principles, elements and processes to guide all staff in effectively managing risk, making it part of our day to day decision making and practices.

5.1 Risk Management Process

The process for managing risk (refer to diagram below) refers to the end to end process of risk management, including:

1. Effective **communication and consultation** with appropriate stakeholders
2. Establish the **scope, context and criteria** of the risk management process
3. **Risk identification** and documentation
4. **Risk analysis** and prioritisation
5. **Risk evaluation** and development of mitigation strategies
6. Development of **risk treatments** as appropriate
7. Ongoing **monitoring and review** of risks and the framework
8. **Recording and reporting** of risk management activities



5.2 Communication and Consultation

The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision making.

Communication and consultation with appropriate internal and external stakeholders should take place throughout all steps of the risk management process, and in particular when strategic plans and business plans are being formulated and when significant decisions need to be made.

Adequate communication and consultation should occur to ensure that existing risks are reviewed as part of the planning process to ensure that all risks are still relevant and match the business or strategic objectives and to ascertain that all risks are captured.

Regular communication is also required with any Treatment Owners to ensure that actions are completed in a timely manner.

5.3 Scope, context and criteria

The purpose of establishing the scope, the context and criteria is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment. Scope, context and criteria involve defining the scope of the process, and understanding the external and internal context.

As the risk management process may be applied at different levels (e.g. strategic, operational, project etc.) it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with organisational objectives.

Establishing the context defines the parameters within which risks should be identified and managed. Consideration should be made of the environment within which risks are to be identified. Some areas that can be considered in determining the context include:

- scope and structure of the organisation, unit, function or process;
- legal, financial, cultural, political, socio-economic and physical aspects;
- key drivers and trends impacting the objectives of the organisation;
- organisation's governance structure, culture, vision, goals, objectives and strategies (whether strategic or operational);
- relevant internal and external stakeholders and partners; and
- current key risks for the organisation.

Refer to Appendix 1 for the criteria to be considered when evaluating risks.

5.4 Risk Identification

This step seeks to identify the risks that the organisation should manage using a consultative process with key stakeholders and assumes effective context setting.

This process will usually involve:

- a workshop including all key stakeholders (i.e. those that are best equipped to identify and assess the risks and those who will be involved in risk mitigating processes/actions);

- identification of risks through a brainstorming process;
- documentation of risks in a Risk Profile/Register; and
- verification of the output by key stakeholders.

Risk management activities in TAFE SA are not about the identification and capture of all risks. Efforts should be directed towards the identification and capture of key risks, thereby ensuring that the benefit outweighs the potential cost and effort of capturing the information.

Risk identification is normally undertaken as part of strategic or business planning processes. This planning process involves setting the context and review of existing risks as well as identification and capture of new risks. The process would typically involve a workshop including key stakeholders.

Other methods of identifying risks include:

- policy and procedure analysis;
- audits and physical inspections;
- checklists, surveys and questionnaires;
- judgements based on experience;
- flow charts;
- systems analysis and scenario analysis;
- customer complaints;
- incidents;
- historical factors; and
- legislation or government policy changes.

Staff are encouraged to report any risks that are identified independently of the planning processes direct to their relevant Manager. (Note: Workplace safety risks should also be reported through the Hazard and Incident Reporting Module (HIRM)). Management have a key role in verifying the validity and relevance of risk information to the objectives of the business prior to the formal addition of a risk to the relevant Risk Register.

Management also have an important role in considering the broader impacts of any risk identified, particularly if a risk has the potential to impact more than their Division or Business Unit. Risks that are identified to have broader impacts should be escalated to the relevant Executive.

Risks are commonly captured in a cause and effect type statement, but most importantly they should be outcome focussed thereby reflecting the actual risk. A short summary title along with a detailed description of the risk should be documented. An example of a risk description is provided below:

"Loss and/or destruction of key TAFE SA assets due to a natural disaster or state of emergency, which results in the disruption of educational services and financial loss."

5.5 Risk Analysis

Risk analysis is the process of comprehending the nature of risk and its characteristics including, where appropriate, the level of risk. This involves analysing the cause, consequence and likelihood, identification of the effectiveness of existing controls and interdependence with other risks. The outcome of this process provides a basis for future management and development of potential treatment(s).

Whether it is a new risk, or a review of an existing risk, for risks to be effectively managed the following steps are required to be performed:

1. Identify the most appropriate risk owner.
2. Determine the cause of the risk.
3. Determine the best matched objective (strategic or operational).
4. Document the identified consequences.
5. Identify current controls and make an objective assessment of their effectiveness (if required).
6. Determine the **Current Risk Rating** by:
    a. Assessing the possible consequences/impact using the scale provided in Appendix 1.1 *(NB: the consequence of a risk does not normally change with the implementation of controls).*
    b. Estimating the likelihood of a risk eventuating *after* considering existing controls, using the scale provided in Appendix 1.2.
    c. Referring to the Risk Analysis Matrix in Appendix 1.3 to calculate the resulting rating and determine the resulting priority for treatment and monitoring.

5.6 Risk Evaluation

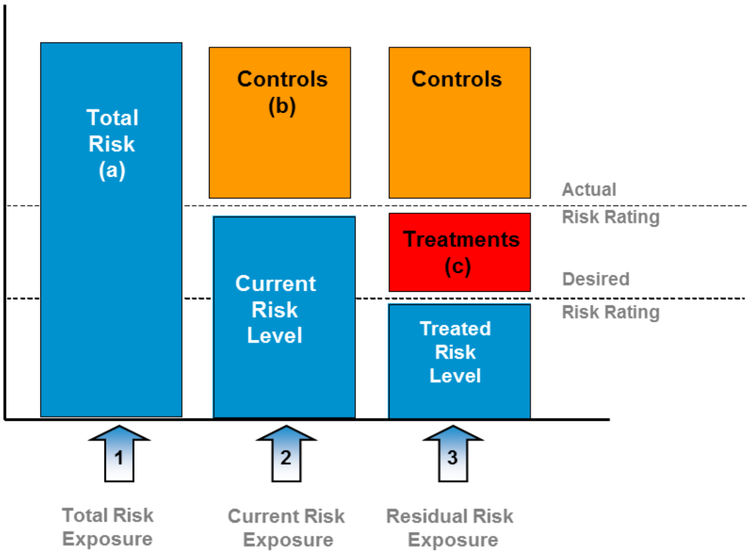
The risk evaluation step determines the priority for management of each risk. Each risk is evaluated against a range of different risk management strategies including:

- Risk Acceptance - the organisation takes a calculated risk and knowingly accepts responsibility for the consequences without any further action or alternatively accepts that there are no further actions to effectively mitigate the risk.
- Risk Reduction - the organisation implements measures that will reduce the level of risk to an acceptable level.
- Risk Avoidance - activities are changed or business activities are discontinued that generate the risk.
- Risk Sharing - the organisation shares the risk (e.g. through the purchase of insurance).

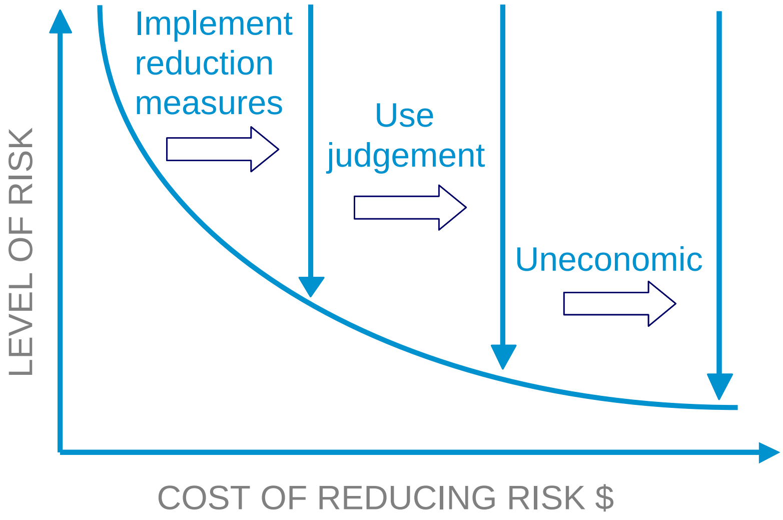
The chosen risk management strategy will determine the subsequent actions. Where the strategy is to accept or reduce the risk, TAFE SA prescribes certain actions based on predefined criteria (refer to Risk Assessment Process Steps and Action Required table in Appendix 2.1 and 2.2). Therefore, in some cases, the resulting decision will need to be modified to comply with the risk tolerance set by TAFE SA.

Some of the specific actions include the identification of treatments for all risks rated as Extreme or High post controls. For all other risks a cost/benefit analysis should be performed.

The following diagram illustrates an example decision making process for managing risk exposure. It assumes that there is an existing control and that the existing control does not achieve a desirable Residual Risk Rating. The desired rating is achieved by developing a Treatment Plan to create a future control.



It is important to recognise the need to balance the costs and benefits resulting from making the decision to mitigate a risk to a further level. This should be considered for each and every risk. The cost of mitigation should not outweigh the benefit of mitigating a risk. A cost/benefit assessment should also be applied to risks and existing controls to ensure the economic viability of the controls. This concept is illustrated in the following diagram.



5.7 Risk Treatment

This step is required only if the decision has been made to progress with development of treatments with the aim of reducing the residual risk exposure. The key steps in the process involve:

1. Identify relevant treatment options that addresses the root cause of the risk.
2. Prepare treatment plans that incorporate consideration of who will be responsible, what will be delivered and when the treatment will be complete.
3. Determine the **Treated Risk Rating** (estimated *future* Residual Risk Rating) by:
    a. Assessing the possible consequences/impact using the scale provided in Appendix 1.1

(NB: the consequence of a risk does not normally change with the implementation of controls and treatments).

b. Estimating the likelihood of a risk eventuating *after* considering existing controls and treatments, using the scale provided in Appendix 1.2.

c. Referring to the Risk Analysis Matrix in Appendix 1.3 to calculate the resulting rating and determine the resulting priority for monitoring.

Once a treatment is complete, the normal procedure is to close the treatment and add it to the list of controls relating to a particular risk. The Current Risk Rating should be reassessed in light of the new control, along with the Treated Risk Rating in light of the completed treatment.

In the situation where there is a decision to no longer proceed with a treatment, the normal process is to close the treatment.

5.8 Monitoring and Review

5.8.1 Monitor

An effective risk management process requires ongoing monitoring and review of all risks, controls and treatments. This should form part of normal management activities. Processes should be implemented to ensure that the Risk Register is monitored and reviewed regularly and risk, control and treatment owners are engaged in the process.

To ensure that risk information is current, formal risk assessments are generally required to be undertaken annually when business plans are being developed. This should take place using a risk assessment workshop involving all key stakeholders. Changing circumstances may warrant a more frequent formal risk assessment.

All aspects of existing risks, controls and treatments should be part of the review. The process should seek to validate the currency of all risks and the risk coverage to ensure that all key risks have been identified and included.

5.8.2 Risk Retirement

Risk retirement is the formal close-out of risks which are no longer relevant. This may be because a function is no longer performed, business processes have changed, due to a structural change within the organisation or simply a change in strategy.

Risk retirement is not something that is done when a risk has been mitigated to a satisfactory level, as such a risk is still relevant for the purpose of decision making. The controls in relation to such a risk may also become ineffective or stop operating over time, rendering the current risk level higher than originally expected. If such a risk has been retired then it will not be monitored.

Any retired risks should be reported as part of the next reporting cycle.

5.9 Reporting

Reporting is undertaken on a regular basis to ensure that key stakeholders have visibility of relevant risks, and that the implications of risks can be considered by management and in decision making.

6 Responsibilities

6.1 TAFE SA Board

The TAFE SA Board is responsible for reviewing and commenting on TAFE SA's Risk Management Policy and Framework and satisfying itself that management has developed and implemented a sound system of risk management and internal control. The TAFE SA Board may elect to receive regular risk reports, question TAFE SA Executive on key risk issues and provide comment as appropriate.

6.2 Chief Executive, TAFE SA

The Chief Executive is responsible for establishing and maintaining effective policies, procedures and systems for the identification, assessment, monitoring, management and review of key strategic and operational risks.

6.3 TAFE SA Executive

TAFE SA Executive are responsible for the effective application of the Risk Management Policy and Framework in their respective areas of responsibility.

6.4 TAFE SA Staff

It is the responsibility of all TAFE SA staff to familiarise themselves and apply the key principles of the Risk Management Policy and Framework in the conduct of their duties. All staff are required to contribute to the identification, management and reporting of risks.

7 Review of TAFE SA policy

TAFE SA policies must undertake a full review process, including staff consultation and TAFE SA Executive/Board approval, at least every three years, but may be actioned earlier according to strategic priorities, reforms or feedback received.

Appendix 1 – Risk Assessment Matrix

1.1 Consequence (Impact) Rating Guide

	Customer and Service Delivery	Financial	Legal, Compliance and Regulation	Human Resources	Reputation and Image
5 Critical	A significant business interruption event resulting in TAFE SA being unable to deliver (any) courses across multiple campuses for more than 30 days	Financial loss or damage in excess of $10 million	Sustained failure in TAFE SA's governance and control framework resulting in significant penalty, loss of registration and authority to deliver services	Death of one or more TAFE SA staff member(s) or student(s) SafeWork SA intervention leading to prosecution and disruption to service delivery Ongoing industrial issues causing widespread disruption to the delivery of services	Sustained adverse media coverage leading to the resignation of TAFE SA Board members and/or the Chief Executive Independent inquiry conducted into TAFE SA's operations
4. Major	A significant business interruption event resulting in TAFE SA being unable to deliver course(s) at one or more campuses for more than 7 days	Financial loss or damage between $2 million - $10 million	Systemic legal, compliance or regulatory failure requiring immediate and decisive action by the Board and/or Chief Executive to prevent significant disruption to TAFE SA's authority/ability to continue to deliver services	Serious injury to TAFE SA staff member(s) or student(s) requiring hospitalisation Multiple lost time injuries SafeWork SA intervention / possible prohibition notice Low employee engagement High staff turnover and inability to recruit appropriately skilled staff to deliver services Industrial dispute with penalty to TAFE SA	Ongoing adverse media coverage resulting in long-term reputational damage Loss of confidence in TAFE SA, including the Board and Chief Executive, by the Minister and general public
3. Moderate	A business interruption event resulting in TAFE SA being unable to deliver course(s) at multiple campuses for up to 2 days	Financial loss or damage between $500,000 – $2 million	Repeated legal, compliance or regulatory failures requiring prompt action to prevent any disruption to services	Lost time injuries to staff. Injury to student requiring medical treatment Ongoing widespread morale issues Turnover of key staff Industrial disputations with no major penalty SafeWork SA intervention / Improvement notice	Widespread negative reporting in the media Short term reputational damage Temporary breakdown in relationship between the Minister, TAFE SA Board and Chief Executive
2. Minor	A business interruption event which results in TAFE SA being unable to deliver a (single) course at a campus for up to 2 days	Financial loss or damage between $100,000 - $500,000	One-off minor legal, compliance or regulatory failure resolved without penalty or major disruption to service delivery	Minor first aid treatment to staff or student requiring treatment Incident resulting in improvement notice issued by SafeWork SA Industrial grievance resolved internally	Isolated adverse media exposure Temporary minor negative impact on the reputation of the organisation
1. Insignificant	A business interruption event which has negligible impact on TAFE SA's ability to deliver services	Financial loss or damage up to $100,000	Immaterial legal, compliance or regulatory failure without penalty and immediate correction action being required	No impact	One-off media coverage with no reputational impact

1.2 Likelihood of Rating Guide

Level	Category	Probability Description
1	**Rare**	Once in 10 YEARS (< 1% probability of occurrence) Event may only occur in exceptional circumstances in the long-term future
2	**Unlikely**	Once in 5 YEARS (1% - 20% probability of occurrence) Event could occur but not anticipated in the foreseeable future
3	**Possible**	Once a YEAR (20% - 50% probability of occurrence) Event could occur within short-term timeframe
4	**Likely**	Once a MONTH (50% - 99% probability of occurrence) Event could occur in most circumstances
5	**Almost Certain**	Once a WEEK or DAILY (> 99% probability of occurrence) Event is expected to occur in most circumstances, risk is occurring now

1.3 Risk Analysis Matrix

Likelihood

5 (Almost Certain)	Moderate	Moderate	High	Extreme	Extreme
4 (Likely)	Moderate	Moderate	High	High	Extreme
3 (Possible)	Low	Moderate	Moderate	High	High
2 (Unlikely)	Low	Low	Moderate	Moderate	High
1 (Rare)	Low	Low	Low	Moderate	High
	1 (Insignificant)	2 (Minor)	3 (Moderate)	4 (Major)	5 (Critical)

Consequence

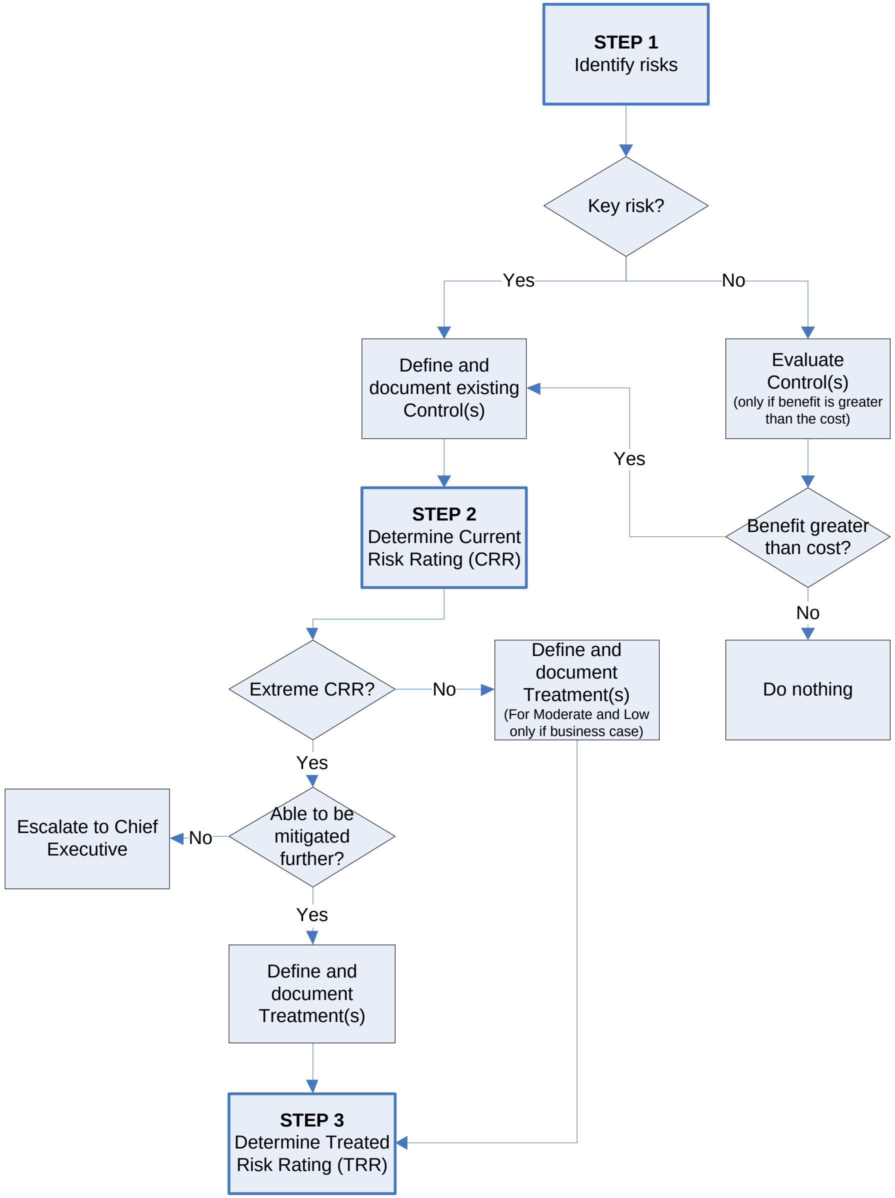
Appendix 2 - Risk Assessment Process

2.1 Process Steps

Step 1: Identify Risk and Document Controls
Document the risk description and the key controls currently in place to mitigate the risk.

Step 2: Complete Current Risk Rating
Make an objective assessment of the consequence and likelihood of the risk post controls and using the Risk Analysis Matrix determine the Current Risk Rating.

Step 3: Complete Treated Risk Rating
Define and document treatments (if required) and make an objective assessment of the consequence and likelihood of the risk post treatments and using the Risk Analysis Matrix determine the Treated Risk Rating.
NB: If a Moderate or Low Current Risk Rating, Treatment Plans are optional (refer to Action Required table below).


STEP 1
Identify risks
Key risk?
Yes
No
Define and document existing Control(s)
Evaluate Control(s) (only if benefit is greater than the cost)
Yes
STEP 2
Determine Current Risk Rating (CRR)
Benefit greater than cost?
No
Extreme CRR?
No
Define and document Treatment(s) (For Moderate and Low only if business case)
Do nothing
Yes
Escalate to Chief Executive
No
Able to be mitigated further?
Yes
Define and document Treatment(s)
STEP 3
Determine Treated Risk Rating (TRR)

2.2 Action Required

Current Level of Risk	Action Description
Extreme	Immediate action required and commitment of Executive, Treatment Plan prepared and documented in < 1 month (if applicable), escalate to TAFE SA Chief Executive via Executive if unable to be mitigated to a lower level and not already reported, active monitoring of controls.
High	Executive attention required, Treatment Plan documented in < 3 months, regular and ongoing monitoring of controls.
Moderate	Management responsibility must be specified and accountability defined, Treatment Plan optional based on benefit to business, periodic ongoing monitoring of controls.
Low	Responsibility must be specified, Treatment Plan optional based on benefit to business (NB: requires control evaluation to be completed), monitoring by Management, consider excess or redundant controls.

The Risk Assessment Process Steps and Action Required table above define the minimum requirements based on the Current Level of Risk rating.

Treatments are optional for risks with Moderate and Low Current Risk Ratings. Only define treatments for risks with Moderate and Low Current Risk Rating if benefit is greater than the cost.

Appendix 3 – Guide to Assessing Likelihood, Consequences and Controls

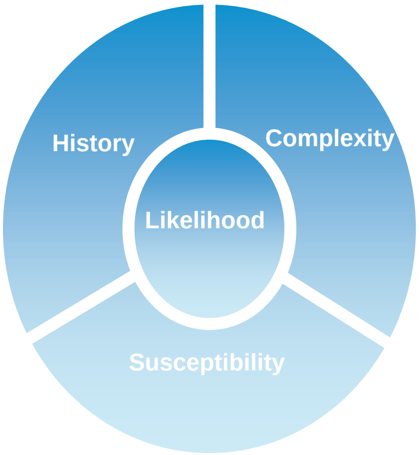
Consequence

Analysing risks also requires an assessment of the impact (consequence) of the outcomes of a risk event. This can be expressed qualitatively or quantitatively. A Consequence Rating Guide is provided (refer to Appendix 2.1) that defines TAFE SA's risk appetite to assist staff in assessing the impact of a risk. Staff would normally select a rating and category aligned with the greatest possible impact.

Likelihood

Analysing risks requires an assessment of their frequency of occurrence. Some useful factors to consider and assist in making an assessment of the likelihood or probability of a risk event occurring include:

Complexity – how complex is the risk or process? Consider the complexity of the underlying processes or environment in which the organisation operates.



Susceptibility – how vulnerable is the business to the risk? Consider the relative newness of people or processes, the number of stakeholders involved, level of change etc.

History – to what extent is the risk known to have occurred previously? Consider the history of error within the relevant environment or the industry.

The TAFE SA Likelihood Rating Guide is provided in Appendix 1.2 and is designed to assist staff in selecting an appropriate rating.

Controls

An assessment of controls is required to determine the Current Risk Rating for each risk. This provides an estimate of the Residual Risk Rating and decisions can then be made if additional controls are required.

Control activities occur throughout an organisation, at all levels and in all functions. Management should consider the following types of controls:

- Directive controls – including plans, policies and procedures that specify what has to happen.
- Preventative controls – including password controls, swipe cards etc implemented to minimise undesirable events such as mistakes and errors.
- Detective/corrective controls – including monitoring and follow up to highlight compliance or non-compliance.
- Behavioural controls – including leadership and other practices that create the right environment for things to happen.

It is important to note that while individual controls may be effective, a group of controls may not be effective in mitigating the overall level of risk. In such a case often treatments will be developed, thereby creating future controls. Individual control effectiveness and overall control effectiveness should be assessed in accordance with the following matrix:

Control Category	Effectiveness Description
Effective	Control is operating effectively
Requires Improvement	Control is operating mostly effectively, however some weaknesses identified (implies that a treatment is required)
Ineffective	Control is not operating effectively (implies that a treatment is required)