TONGA NATIONAL QUALIFICATIONS AND ACCREDITATION BOARD

RISK MANAGEMENT FRAMEWORK

Overview

Tonga National Qualifications and Accreditation Board (TNQAB) was established in 2004, after the Tonga National Qualifications and Accreditation Board Act 2004, was approved by parliament. The actual operation and functioning of the Board as an organization, however, did not begin until 2009, when the initial staff members were recruited and inducted into their roles. Since then, TNQAB, has functioned as the national regulator for post compulsory education and training. Its primary objective is to ensure that quality education is attained and maintained through the effective monitoring and regulation of providers' registration and accreditation of courses of study.

A risk division was established last year with the recruitment of a risk analyst and this Risk Management Framework is the first attempt at 1) incorporating risk management into the organization's procedures and 2) creating a TNQAB Risk Management Framework in order to have an apparatus, a tool with which to measure and treat risks to the organization.

The TNQAB Risk Management Framework was adapted from the New Zealand Qualification Authority (NZQA) Risk Management procedure 2013, the Australian Skills and Qualification Authority (ASQA) Regulatory Risk Framework 2016 and the Tertiary Education Quality and Standards Authority (TEQSA) Risk Assessment Framework 2016. Various components from these risk frameworks were adopted and then adapted for TNQAB and the Higher Education context in Tonga. All three risk frameworks (NZQA, ASQA, and TEQSA) and the TNQAB Risk Management Framework, use the core elements of the ISO Standards for Risk Assessment (ISO 31000/2009).

The TNQAB Risk Management Framework will improve as time allows the capacity of the risk personnel(s) to develop and when more information is available about its implementation and impact on the Post Compulsory Education and Training (PCET) providers in Tonga.

Why is it important for TNQAB to have a Risk Management Framework?

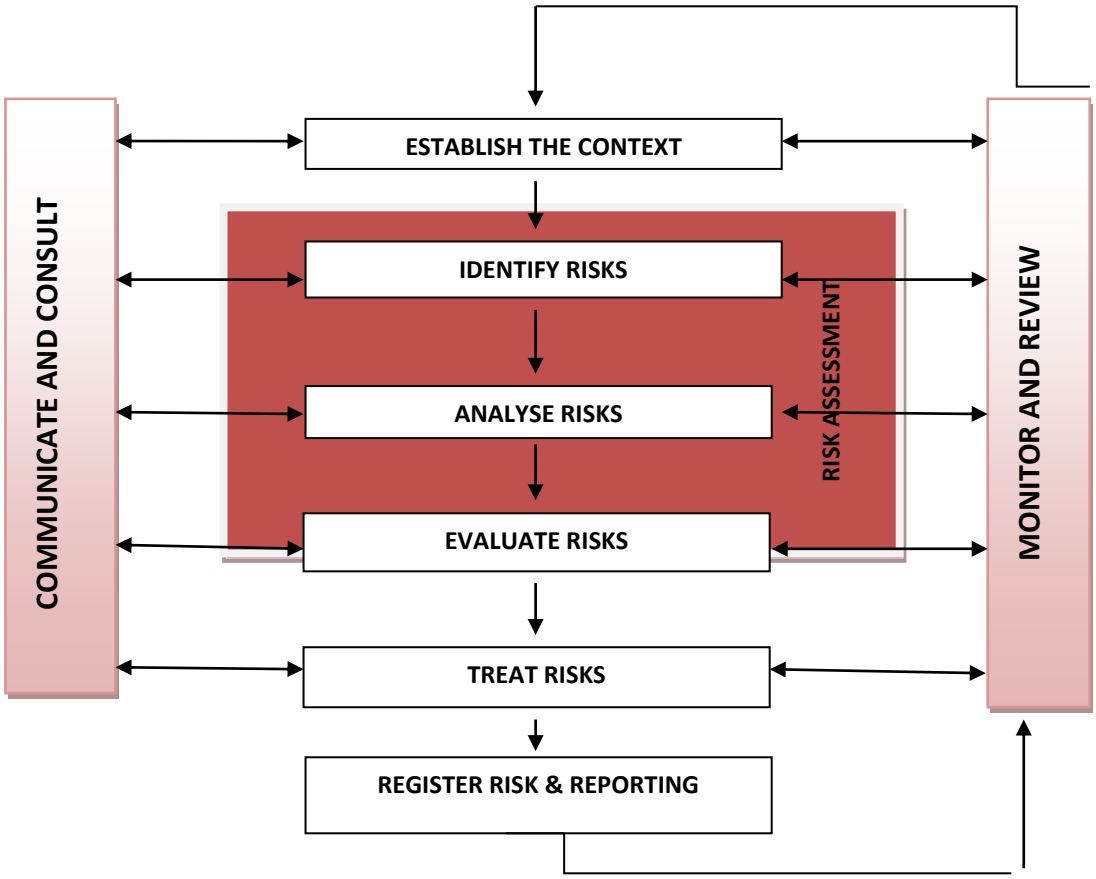
1) The fundamental purpose of having a Risk Management Framework is to ensure that the objectives an organization desires to achieve, are in fact achieved. Risk, as described in the ISO Standards for Risk Assessment (ISO 31000/2009), is the effect of *uncertainty* on objectives. Therefore, the primary reason for having a Risk Management Framework is to be able to mitigate and where possible, eliminate the uncertainties that affect an organization from achieving its objectives.
2) In order to have an apparatus to manage risk in a methodical way, therefore, enabling consistency in the handling and treatment of risk.
3) To have an apparatus to effectively monitor and regulate PCET providers and their registration and accreditation status.
4) To be able to detect risks and enforce compliance to the TNQAB Act, Regulation, policies and guidelines, thereby improving confidence in the organization.
5) To be able to identify the critical risks in order to prioritize the organization's time and resources to handling those risks first before addressing the risks that are less threatening.

6) As stated already, TNQAB's primary objective is to ensure that quality education is attained and maintained in tertiary vocational education and training and in university level education. It is therefore important for TNQAB to have a Risk Management Framework, in order to guarantee the achievement of this objective. We can then be confident that the individuals who graduate from PCET institutions and university institutions in Tonga, are fully equipped with the knowledge and skills to take on employment responsibilities.

What risk does TNQAB seek to manage?

1) Internal risk - The TNQAB Risk Management Framework will be used to manage *internal risks* from within the organization. For example – If the Quality Assurance officers do not comply with the policies delineated in the Quality Assurance Policy, this creates risk(s). The risk framework is used to identify, analyze and treat the risk.
2) External risk - The TNQAB Risk Management Framework will be used to manage *external risks* from without the organization. For example – When a PCET provider does not comply with the TNQAB Act 2004 or the TNQAB Regulation, this is an act of non-compliance and it causes risk(s). The risk framework is used to identify, analyze and treat the risk.
3) Systemic Risk - The TNQAB Risk Management Framework will be used to manage *systemic risks*, which is a risk that is likely to be prevalent amongst a significant number of PCET providers. If left untreated, it can have a grave impact on the quality of education and training of students. This in turn, will affect the industry and the wider community and lead to a loss of confidence in TNQAB as a regulator of quality education.

The TNQAB Risk Management Procedure



1 Stage 1: Establishing the Context

The aim of this stage is to express the objectives/goals and internal and external parameters of TNQAB. Furthermore, the scope and risk criteria of the risk management process are also determined in this stage.

When the risk management procedure is applied to TNQAB *internal risks*, it is the organization's objectives that are expressed. Furthermore, the external and internal parameters that are important to consider when implementing internal risk management, are drawn. In addition, the scope of the risk management process and the risk criteria, are established during this stage.

When the risk management procedure is applied to TNQAB *external risks*, it is the organization's objectives and goals that are expressed. Furthermore, the external and internal parameters that are important to consider when implementing external risk management, are drawn. In addition, the scope of the risk management process and the risk criteria, are established during this stage.

The external context can include, but is not limited to:

- The social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national and regional or local;
- Key drivers and trends having impact on the objectives of the organization; and
- Relationships with, perceptions and values of external shareholders.

The internal context can include, but is not limited to:

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- The relationships with and perceptions and values of internal stakeholders;
- The organization's culture;
- Information systems, information flows and decision making processes (both formal and informal);
- Standards, guidelines and models adopted by the organization; and
- Form and extent of contractual relationships.

(AS/NZS ISO 31000:2009)

NB: The 'Establish the Context' form is Appendix 1.

2 Stage 2: Risk Identification

The aim of this stage is to identify the sources of risk, areas of impact, events (including the changes in circumstances) and their causes and their potential consequences (AS/NZ ISO 31000:2009). When this is executed effectively, it will result in the production of a comprehensive list of risks, established from those events anticipated to affect (either positively or negatively) the achievement of objectives.

Risks are identified through a process called *profiling*. Profiling is essentially a complete and thorough analysis using a range of tools such as brainstorming, compiling results from audit reports (quality audit and financial audit), using professional judgement, analysis of historical events, SWOT/R Strengths Weaknesses Opportunities Threats/Risks analysis, scenario analysis, gap analysis, and trend analysis. Profiling is used as the procedure for identifying risk because it is a way of constructing a holistic overview of the situation. This, in turn, will foster a better understanding of the situation and therefore later assist the organization in making the appropriate decisions to best manage the risk(s).

The comprehensive list of risks identified during this stage, will be presented in the 'Risk Identification' forms included in the appendix.

The Risk Identification forms - Appendix 2: Provider Context, Appendix 3: Regulatory History and Standing, Appendix 4: Stakeholder needs.
Note: In order to determine financial viability and sustainability, the provider is expected to provide a current annual operating budget, a statement of financial position, a statement of financial performance and cash-flows and forecasts. If the

provider is getting outside funding, it should also provide a statement from the funding body.
The aforementioned financial information was submitted as a requirement for registration. However, in order to identify risk, an up-to-date version of the financial information required, will be needed for risk identification.

TNQAB has also established a complaint procedure for the general public to use. The complaint procedure includes the procedure that students use when lodging a complaint about a PCET provider, the procedure that individuals who are not students (a parent or guardian) use when lodging a complaint about a PCET provider and the procedure that individuals use when lodging a complaint about TNQAB. The complaint procedure is a means by which risk is detected because complaints may reveal non-compliance which then indicates that something or someone is at risk.

3 Stage 3: Risk Analysis

The aim of this stage is to better understand the risks identified in Stage 2 by determining their likelihood and consequence.

The likelihood of a risk is the possibility of that risk happening. The consequence of a risk is the impact that it will have on TNQAB objectives.

Likelihood and consequence are identified using the Likelihood and Consequence scales.

Consequence Scale:

Risk Impact Matrix					
RISK TYPE	**Critical/Catastrophic**	**Major**	**Moderate**	**Minor**	**Rare**
Core Function delivery	• Failure to deliver on Strategic Plan, or Statement of Intent; • Failure to deliver on an entire output; • Core processes unavailable or failing. Corporate Plans/ disaster recovery plans need to be triggered.	• Failure to deliver on a single output; • Significant processes affected or unavailable. Workarounds only partially available or will require time to implement. BCP's or disaster recovery can be triggered.	• Failure of internal systems or component of a high profile service; • Some effect on processes, workarounds available or to be implemented in acceptable timeframe.	• Internal quality standards fail; • Minimal effect on processes. Work-arounds available	No immediate effect on processes, workarounds available.
Financial	>$500,000	>$50,000 NZQA)	>$20,000	>$5000	>100
Organisational / structure	Significant change at Board, Senior Management Team (SMT) level and/or >30% turnover	>25% turnover and/or significant change in any one area.	Significant organisational change. Turnover of staff >20%.	Key person loss (any SMT and/or SMT defined person).	
Reputation	Loss of reputation that may take 3-5 years to recover from and/or Ministers loses confidence in TNQAB's outputs/deliverables.	Loss of reputation that may take 1-3 years to recover from.	Loss of reputation that may take 3-6 months to recover from.	Loss of reputation that may take 1-3 months to recover from.	Incidents over the course of 2-3 days maximum, which reflects negatively on TNQAB.

Security	Qualifications fraud by employee/contractor. Theft and use of Qualification material.	Monetary fraud by staff. Theft of TNQAB material.	System security breach.	Discovery of security weaknesses by third party.	
Technology	Technology failure or security breach resulting in irreversible loss or failure to deliver on Strategic Plan or Statement of Intent or an entire output class.	Failure of a high profile support system of significant output or process at a critical time.	• Failure of a high profile system at a non-critical time; • Failure of a lower profile system at a critical time.	Failure of a low profile system at a non-critical time.	

Consequence Criteria

The descriptions below are indicative only and provide a guide to relative consequence.

Rating	Score	Criteria/ Example
Catastrophic	**5**	• Government or external agency instigates an inquiry or legal action • Significant damage to the organization's reputation • Widespread, ongoing, negative media coverage • Legal action involving major criminal charges and/or civil suits with possible fines and costs exceeding $10,000 (>$500,000 NZQA) • Long term cessation of core activities (months) • Destruction or long-term unavailability of infrastructure, systems and resources directly impacting operations • Financial loss not covered by insurance (more than $10,000) (>$500,000 NZQA) • Major problem from which there is no recovery • Significant damage to the organisation's credibility or integrity • Complete loss of ability to deliver a critical program.
Major	**4**	• Widespread negative media coverage • Legal action involving criminal charges and/or civil suits with possible fines and costs exceeding $5,000 (>$50,000 NZQA) • Short term cessation of core activities (weeks) • Financial loss not covered by insurance ($10,000 – $5,000) (>$50,000 NZQA) • Event that requires a major realignment of how service is delivered. • Significant event which has a long recovery period. • Failure to deliver a major project commitment.
Moderate	**3**	• May generate unfavourable media attention/ coverage • Significant disruption to core activities (days) • Financial loss not covered by insurance ($5,000 - $1,000) (<$20,000 NZQA) • Recovery from the event requires cooperation across divisions.
Minor	**2**	• Limited unfavourable media coverage • Short-term disruption to core activities (days) • Long-term disruption to non-core activities (weeks) • Financial loss not covered by insurance ($1,000 - $500) (>$5000 NZQA) • Can be dealt with at a division level but requires Chief Executive notification. • Delay in funding or change in funding criteria • Stakeholder or client would take note or interest.
Rare	**1**	• Unlikely to have an impact on the Provider's public image • Minimal impact on operations • Minimal financial loss (less than $500) • Can be dealt with internally • No escalation of the issue required • No media attention.

		• No or manageable stakeholder or client interest.

Likelihood Criteria

Rating	Score	Description
Almost Certain	**5**	• High likelihood (>90% probability) of risk event happening several times within the next year or that it has occurred in the last 6 months
Probable / Likely	**4**	• A risk event that has a 50% - 90% probability likely to occur more than once in the next 12 months or it has occurred in the last 12 months
Possible/ Moderate	**3**	• Anticipated 25% - 50% probability of risk occurring in the next 12 months or more than once in a 5 year period. There may be a history of occurrence
Unlikely	**2**	• The risk event could occur at some time but is unlikely. That is, it has a 10% - 25% probability of occurring in the next 12 months
Rare	**1**	• Within the realms of possibility but extremely unlikely to occur. Occurs once in 10 years or Less than 10% probability of occurring in the next 12 months

4 Stage 4: Risk Evaluation

The aim of this stage is to evaluate risk by giving it a value, by quantifying it. Risk is an uncertainty, therefore, it is abstract. Yet, the aim of this stage is to assign a value to it so that it becomes something that we can work with – by assigning it a value, a quantity, it can then be determined how catastrophic or not, the risk is. This, in turn, informs Stage 5: Risk Treatment, on which risks to prioritize first, to dedicate the organization's resources to, whether human or financial and how much of it is dedicated to managing that particular risk. Furthermore, it also determines who can make decisions about the risk, to what extent a risk should be accepted or mitigated, and who the risk should be reported to (AS/NZ ISO 31000:2009).

Risk evaluation is established by multiplying the likelihood and consequence levels of a risk using the Risk Evaluation Matrix (Heat Map).

Risk Evaluation Matrix

Risk rating as a function of consequence and likelihood scores.

Consequence						
	5 Catastrophic	MEDIUM	HIGH	CRITICAL	CRITICAL	CRITICAL
	4 Major	LOW	MEDIUM	HIGH	CRITICAL	CRITICAL
	3 Moderate	LOW	LOW	MEDIUM	HIGH	CRITICAL
	2 Minor	MINOR	LOW	LOW	MEDIUM	HIGH
	1 Rare	MINOR	MINOR	LOW	LOW	MEDIUM
		1 Rare	2 Unlikely	3 Moderate	4 Likely	5 Almost Certain
		Likelihood				

For example, a risk deemed as having a "Minor (2)" consequence and be "Unlikely (2)" would have an evaluation rating of 4 (=2 x 2). A risk deemed to have a "Catastrophic" consequence and be "Almost certain" of occurring would have an evaluation rating of 25 (5 x 5). The level of risk/ risk ranking is entered into the Risk Assessment Guide (Appendix 4) along with details of the escalation requirements (if any) for the risk.

Actions/reporting escalations required

Level of risk	
Critical (20-25)	Advise Board, CEO and Senior Management Team. Immediate action required.
High (10-16)	Advise CEO and Senior Management Team. Senior Management Team to manage. Documented controls and mitigation strategies must be reported.
Medium (5-9)	Advise Senior Management Team. Managed by Senior Management Team Member, who may delegate to a Principal Qualification Officer. Controls and mitigation strategies are to be appropriate to the risk.
Low (2-4)	Managed by a Principal Qualification Officer. Controls and mitigation strategies are to be appropriate to the risk.
Minor (1)	Managed by staff or a Principal Qualification Officer. Controls and mitigation strategies are to be appropriate to the risk.

5 Stage 5: Risk Treatment

The aim of this stage is to choose the option(s) for managing risk in order to minimize its impact. Stages 1 to 4 established the foundation on which risk treatment is then determined. The key elements of risk treatment are as follows:

- It's a good idea to have a range of risk treatment options to then choose from
- Treatment plans can be an incorporation of a number of options combined together, tailored to suit the risk situation
- Treatment plans should be justified based on cost/benefit analysis
- Risk treatment plans should at best, not affect the effective and efficient operation of TNQAB
- Risk treatment plans should comply with TNQAB policies and regulations in addition to related Acts and laws and it should also be compatible with the objectives of TNQAB.

Treatment options include:

- Avoid the risk altogether, eliminate it by deciding not to continue with the activity that produces the risk or continue with the activity and seek ways to manage and maintain it
- Reduce the likelihood of a risk by reducing the likelihood of negative outcomes or increase the likelihood of beneficial outcomes
- Reduce the consequences to reduce the extent of losses or increase the extent of gains
- Transferring the risk or opportunity
- Retaining the risk or residual opportunity

6 Stage 6: Register Risk and Reporting

The aim of this stage is to record the risk and to forward it to the appropriate decision making level.

An electronic TNQAB Risk Register will be established in the organization's Intranet system so that staff members working in the different divisions of the organization can register both internal and external risks they discovered, perceive or anticipate to occur. The staff member who identified the risk, will complete the Risk Assessment Guidance and lodge it into the electronic Risk Register. Only the Senior Risk analyst will have access to the Risk Register and will analyze and report the risks during the monthly Senior Management Team meeting.

The Risk Assessment Guidance (Appendix 6) is included in the appendix.

The procedure for managing Systemic Risk

Risk Identification – Systemic risks are identified through *environmental scanning*. Environmental scanning is making an observation of a situation based on various sources of information such as regulatory site visit reports, audit visit reports, student complaints, registration visits, intelligence from internal and external sources, provider consultations and other external data.

Environmental scanning identifies the areas of concern that may cause a risk for TNQAB, towards which effort and resources can be assigned.

Risk analysis and evaluation – The areas of concern identified through environmental scanning are then analysed and evaluated against a range of 'likelihood' and 'impact' measures to produce a list of systemic risks. Likelihood and impact measures can include:

Likelihood	Impact
- Prevalence of the concern amongst PCET stakeholders - Prevalence of the concern in complaints, failure to comply with TNQAB Act, regulation, policies. - Prevalence of the concern detected during regulatory site visits.	- Impact on students (e.g. number of students enrolled for a particular qualification). - Impact on industry. - Impact on the reputation of the organization.

Risk treatment –TNQAB takes a project-based approach to analysing and treating the most serious systemic risks identified. The number of systemic risk projects approved for implementation is determined by the nature of treatment strategies recommended and TNQAB's capacity to undertake the work.

Treatment strategies will vary according to the nature and scale of the risk, but may include:

- Conducting information and awareness campaigns
- Collaborating with stakeholders during consultations and training workshops
- Focus audits or investigation of providers

References

1. ISO (2009). Risk Management – Principles and guidelines (AS/NZS ISO 31000)
2. Tertiary Education Quality and Standards Agency (2016). Risk Assessment Framework.
3. Australian Skills Quality Authority Regulatory (2016). Risk Framework.
4. New Zealand Qualification Authority (2013). Risk Management Procedure.

Appendix 1:

Establishing the Context

Objectives: *Goals/aims which the organization (TNQAB) desires to achieve.*
External parameters: *External environment in which the organization seeks to achieve its objectives.*
Internal parameters: *Internal environment in which the organization seeks to achieve its objectives.*
Scope: *The range or extent of an action.*
Risk criteria: *Terms of reference against which the significance of risk is evaluated.*

Appendix 2:

Provider Context

Provider Details		
Provider name: Registration status: First registered (dd/mm/yyyy): Registration expires (dd/mm/yyyy): Delivery mode:		
List of Higher Education Course Offerings	**Qualification Level**	**Accreditation status**
Provider Background		

Appendix 3:

Regulatory History and Standing

Regulatory event and findings	Date
Complaints received by TNQAB	Date

Appendix 4

Stakeholder Needs

Stakeholder need	How need will be addressed	Person(s) responsible	Need met (Date)
For e.g. Needs TNQAB training on standards for programme accreditation.			

Appendix 5:

Risk Assessment Guide

Name of Risk	
Nature of risk	*Eg – strategic, operational, financial, knowledge, compliance, etc*
Source of risk	
Event or incident	
A **cause**	
When and **Where** could the risk occur	
Who might be involved or impacted	
Controls and their **level of effectiveness**	
Consequence/Impact	
Likelihood	
Risk evaluation and Escalation requirements	
Treatment Options	
Best Treatment Option	
Risk owner	
Strategy and policy developments	

Appendix 6:

Risk Treatment Plan

<table>
<tr><td colspan="4">Division/Activity:</td></tr>
<tr><td colspan="3">Risk:</td><td>Ref:</td></tr>
<tr><td colspan="4">Summary: Recommended response and impact</td></tr>
<tr><td colspan="4">Action Plan
1. Proposed actions (including communications strategy)</td></tr>
<tr><td colspan="4">2. Resource requirement</td></tr>
<tr><td colspan="4">3. Cost vs. benefit analysis</td></tr>
<tr><td colspan="4">4. Responsibility
• Risk owner
• Senior Risk Analyst</td></tr>
<tr><td colspan="4">5. Timing</td></tr>
<tr><td colspan="4">6. Reporting and monitoring required</td></tr>
<tr><td>Compiled by:</td><td>Date:</td><td>Reviewed by:</td><td>Date:</td></tr>
</table>