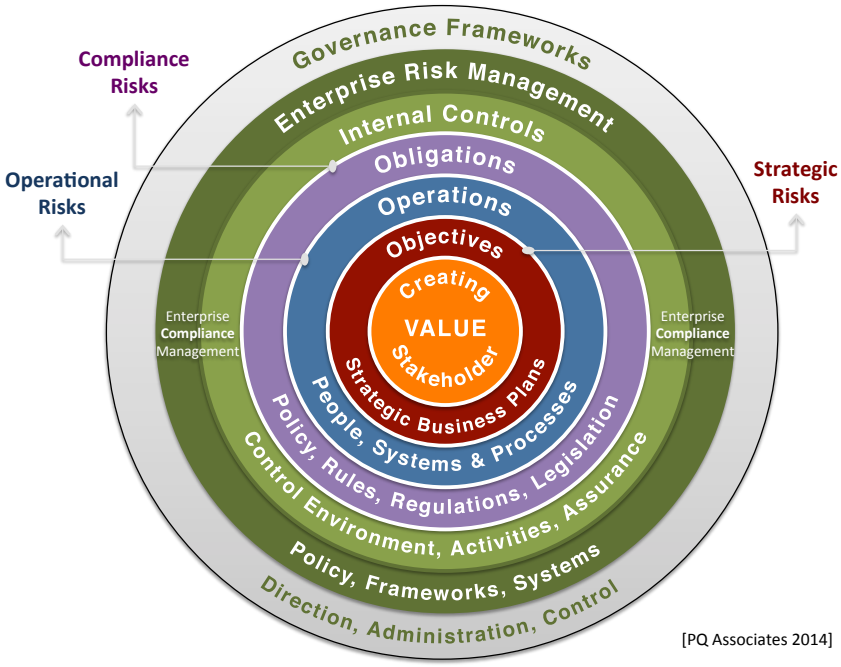
POLICY: Risk Management



1. CONTEXT

1.1 Scope

1.1.1 This policy applies to the Male Survivors of Sexual Abuse Trust of Aotearoa, New Zealand (MSSAT|ANZ) Board, Board Committees and staff members

1.2 Purpose

1.2.1 The objective of this policy is to ensure that risk management principles and practice are understood and consistently applied across the organisation and that individual and collective accountabilities are clearly understood

1.3 Principles

1.3.1 Risk management across the organisation is performed on a consistent basis and in accordance with:

- AS/NZ ISO 31000:2009 International Standard for Risk Management
- The management and reporting responsibilities and obligations outlined in this policy
- The risk appetite and tolerance of the organisation as defined by the Board using the approved risk evaluations and assessment criteria

1.4 Definitions

1.4.1 **Risk management** is the process of establishing stakeholder confidence that the organisation's culture, policies, procedures, systems and practices enable and support the effective management of risk to reduce uncertainty, exploit opportunities to enhance service quality, and provide reasonable assurance that the organisation's goals and objectives will be met.

- For further definitions refer to Appendix A

2. POLICY

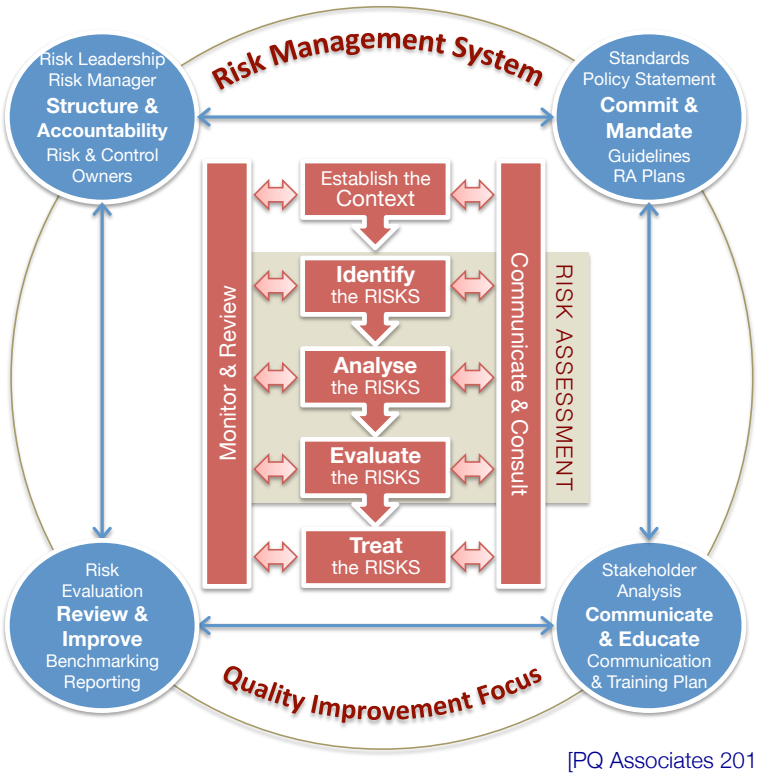
2.1 Risk Management Processes

2.1.1 Risk management reduces uncertainty and identifies opportunities to improve the quality of service.

2.1.2 Risk management is performed in accordance with the international standard for risk management [AS/NZ ISO 31000:2009]. All risk management processes must be performed in accordance with this standard [refer diagram below].

2.1.3 Risks are analysed and evaluated in accordance with the risk analysis and evaluation criteria approved by the Board. These criteria are detailed in Appendix C.

2.1.4 A quality improvement focus is applied to the definition and implementation of risk treatment or management plans.



[PQ Associates 2011]

2.2 Responsibility and Accountability

2.2.1 The **Board** is ultimately responsible for establishing and maintaining the risk management framework, maintaining an adequate risk management capability and ensuring that all 'Medium' to 'Very High' risks associated with the organisation's goals and objectives are effectively managed.

2.2.2 A primary objective of the **Governance Committee** of the Board is to assist the Board in discharging its risk management obligations. This committee, on behalf of the Board should:

- Ensure that an effective risk management framework is in place;
- Ensure that this framework is operating effectively to identify, assess and manage risks in accordance with this policy;
- Report to the Board all significant risk exposures identified by the framework and ensuring that the appropriate risk oversight responsibilities are effectively assigned to the Board, the Risk Committee or the Executive Director; and
- Ensure that any risks assigned to the Risk Committee are effectively managed.

2.2.3 The **Governance Committee** is primarily responsible for effective management of all risks associated with the achievement of the organisation's goals and objectives that are not specifically assigned to another Board Committee, Trustee or a member of staff.

2.2.4 All **staff** are responsible for reporting on any risks identified within the activities of their position. If their position is assigned responsibility for managing risks, they are responsible for ensuring that those risks are managed in accordance with the risk management framework.

2.2.5 **Risk owners** are responsible for ensuring that the likelihood and consequence of risks assigned to them, or for which they are otherwise responsible, are reduced. This includes responsibility for ensuring the timely implementation of effective quality focussed risk management processes [including controls and procedures] and monitoring systems. Risk owners are also responsible for reporting the status of their assigned risks and for monitoring any environmental changes that could impact on the risk status.

2.2.6 **Control owners** are responsible for ensuring that any control activity assigned to them is fully operating. Where a control is not yet fully operating, they are responsible for ensuring the completion of the necessary tasks and management plans to fully implement the control in a timely manner. A control owner is responsible for ensuring the status of the control is reported to the risk owner and for ensuring that all required documentation for the control is in place.

2.3 Risk Assessment

2.3.1 **Strategic risks** should be identified and assessed on an annual basis as part of the strategic planning process.

2.3.2 **Compliance risks** should be identified and assessed on an annual basis as part of an annual compliance review process.

2.3.3 **Operational risks** should be identified and assessed on a progressive basis across a three-year cycle with the proviso that the implementation of any new systems and processes should be subject to an operational risk assessment process.

2.3.4 The **risk management framework** should be formally reviewed by the Board on a three yearly basis or as otherwise required as a result of significant changes in risks management standards or practices.

2.3.5 The risk **assessment and evaluation criteria**, including the risk appetite and tolerance of the organisation should be reviewed by the General Manager and endorsed by the Board on an annual basis.

2.4 Risk Treatment

2.4.1 All risks must be assessed using the organisation's assessment criteria. Refer Appendix B

2.4.2 Decision on whether the risk requires treatment or not should be determined by the organisation's risk evaluation criteria. Refer Appendix B

2.4.3 Where the assessment and evaluation criteria have determined that a risk requires treatment, appropriate quality focussed management plans [including controls and procedures] must be enacted to reduce the likelihood or consequences of the risk.

2.4.4 Management [treatment] plans must exist for all 'High' or 'Very High' risks where adequate risk management controls or procedures are not in place. These plans should focus on opportunities to enhance service quality.

2.5 Reporting

2.5.1 The status and treatment plans for all 'High' and 'Very High' risks must be reported to the Board by the Governance Committee on a quarterly basis

2.5.2 The complete risk profile of the organisation is to be reported to the Board by the Governance Committee on an annual basis

2.5.3 The Board should ensure that the annual audit plan is appropriately informed by the risk profile of the organisation

Appendix A: Definitions

Term	Definition
Cause	An occurrence which individually or in conjunction with other 'causes', could lead to a risk incident happening
[Risk] Category	Strategic, Compliance or Operational depending on the nature of the objective which is subject to the risk
Compliance Risk	Risks associated with complying with the obligations of the organisation being legal, regulatory or internal policy
Consequence	The outcome of a risk incident happening. Consequence categories can include financial, service interruption, operational effectiveness, reputational or political, people and safety, or legal and compliance
Control Activity	An activity that either reduces the likelihood or consequence of the risk
Control Environment	Means the overall attitude, awareness and actions of the organisation regarding the internal control systems. It consists of the organisational level control activities, which reduce the risk of failure of specific control activities across the organisation.
Control Owner	An individual or group of individuals assigned with the responsibility for ensuring a control is fully operational.
Financial Risk	The risk associated with the achievement of the financial objectives of the organisation
Governance	The manner in which the Board directs, administer and controls the organisation. It includes the structures, processes, customs and policies applying to that direction administration and control
Incident	An occurrence that would have adverse consequence on the achievement of organisational goals or objectives
Internal Control Framework	The processes and structures that ensure control activities are implemented and effectively operating to manage risk
Likelihood	Probability [of a risk incident occurring]
Obligations	Legislative, regulatory, Government or internal policies with which the organisation must comply
Operational Risk	Risk associated with delivery of system, process and resource management objectives
Organisational Level Controls	Control activities that are performed at an organisational level which reduce the risk of failure of all other control activities performed within the organization. These include; governance, policies, reporting structures, codes of conduct, organisational structure, delegation of authorities and HR Practices.

Term	Definition
Risk	The likelihood of something occurring which has adverse consequences on the achievement of organisational goals and objectives
Risk Analysis	The process of determining the likelihood and consequence of a risk incident, and thus the risk rating
Risk Assessment	The combined process of identifying, analysing and evaluating risk
Risk Evaluation	The process of evaluating the level and type of treatment to be applied to a risk depending on its nature, severity and cost-benefit of treating the risk
Risk Management	The culture, processes and tools affected by the organisation's governance, management and staff, that supports the reduction of uncertainty and the exploitation of opportunities by identifying and managing risk to provide reasonable management that the organisation's goals and objectives will be met.
Risk Management [Treatment] Plan	A series of tasks which are required to be completed to ensure that controls rare fully operating to reduce the likelihood or consequence of the risk occurring
Risk Owner	Individual or group of individuals assigned the responsibility for managing the risk
Risk Rating	The level of overall severity assigned to a risk based on the severity of the consequences and the likelihood of the risk incident occurring
Risk Treatment	The method or process of dealing with an identified potential risk incident
Risk Universe	The total portfolio of risks and potential risks to which the organisation is exposed
Strategic Risks	Risks associated with achievement of objectives in the organisation's strategic business plan
Types [of causes]	The common themes of the causes of risk incidents

Appendix B: Assessment Criteria

RISK RATING

Consequences	Likelihood				
	Rare	Unlikely	Possible	Likely	Almost Certain
Severe	Medium	Medium	High	Very High	Very High
Major	Low	Medium	High	High	Very High
Moderate	Low	Low	Medium	High	High
Minor	Very Low	Low	Low	Medium	Medium
Insignificant	Very Low	Very Low	Low	Low	Low
	Incidents of this type have not occurred and are not expected to occur	Incidents of this type could occur but have not occurred before	Incidents of this type occur and have occurred infrequently before	Incidents of this type have occurred several times before and are likely to occur again in the future	Incidents of this type will occur frequently on an annual basis

RISK TREATMENT

Risk Rating	Evaluation	Treatment
Very Low	Inconsequential	No risk reduction action required
Low	Acceptable	No risk reduction action required
Medium	Tolerable	Risk reduction action is required but the risk may be acceptable if high costs or action impractical
High	Intolerable	Some risk reduction action MUST be implemented – scope of action subject to cost-benefit
Very High	Unacceptable	Risk reduction action MUST be implemented irrespective of costs

STATUS

Control Setting	Evidence shows that:	Indicator Setting	Evidence shows that:
Operating	Cause controls are fully operational	Increasing	Control (mitigation) activities are not yet effective
Partial	Only some of the cause controls are operating	Reducing	Control activities are working and reducing risk
No Control	There is no control in place for this cause	No Change	Control activities are maintaining risk status

CONSEQUENCES

Risk Type / Severity	Financial	Service Continuity	Operational Effectiveness	Political & Reputational	People & Safety	Legal & Compliance
Severe	Organisational revenue or cost impacts > 10% of annual budget;	Loss or non delivery of substantial member service for > 20 days;	Loss of an essential organisational service for > 20 days; all major outcomes of significant projects not realised; major projects abandoned	Severe relationship difficulties with Government; public enquiry; concentrated local or national media interest; severe member impacts.	Significant IR disruption and/or significant loss of key people; Single death or serious lifetime disability	Significant regulatory breach with serious litigation and/or major cost impacts;
Major	Organisational , revenue or cost impacts > 5% of annual budget;	Loss or non delivery of substantial major member service for > 10 days	Loss of an essential organisational service for > 10 days; most major outcomes of significant projects not realised; major projects significantly delayed or deferred	Government embarrassment and/or internal Govt. enquiry; major story in national or local media; major member impacts	Very low staff morale; multiple IR disruptions and/or very high staff turnover; injury involving long term hospital & rehabilitation	Major breach of regulation with major litigation and/or significant cost impacts
Moderate	Organisational revenue or cost impacts > 3% of annual budget;	Loss of a substantial member service for > 5 day	Loss of an essential organisational service for >5 day; some major outcomes of significant projects not realised; major project delayed	Issue requiring involvement of Minister or other Parliamentary member; significant coverage in local media; some significant member impacts.	Low staff morale; some IR disruptions and/or high staff turnover; injury involving hospital & rehabilitation	Serious breach of regulation with investigation or potential for prosecution and/or moderate cost impacts
Minor	Organisational revenue or cost impacts < 3% of annual budget;	Loss of a substantial member service for < 5 days	Loss of an essential organisational service for < 5 days: Some major outcomes of significant projects deferred; minor delays for major projects	Questions from external parties, low-level mention and interest in local media; no significant member impacts.	Some staff morale issues; injury involving medical treatment and some lost employment time	Some significant legal issues, non compliance or breaches of regulation and/or low cost impacts;
Insignificant	Organisational revenue or cost impacts < 1% of annual budget;	Loss of a substantial member service for < 1 day	Loss of an essential organisational service for < 1 day; Some major benefits of significant projects delayed	Issues resolved as part of internal management processes, no media interest or member concerns	Isolated staff morale issues; acceptable staff turnover	Minor legal issues, non compliance or breaches of regulation and/or no cost impacts;