Enterprise Risk Management Framework

1. INTRODUCTION

Catholic Family Life Limited and CFL Lumens Trust, collectively known as Catholic Family Life ("CFL") recognises that risk management is a key element of sound governance and management practice. This is particularly important in an increasingly volatile and uncertain world.

Enterprise Risk Management ("ERM") provides a standardised approach to assessing risks and providing management and the Board with enhanced information and oversight on the Charity's risk and control environment. The management of risk is a shared responsibility at all levels of CFL.

2. PURPOSE

CFL ERM is designed to identify potential events and trends (which are commonly defined as 'Risks') that may significantly affect CFL's ability to achieve its strategic goals or maintain its operations, either positively or negatively. Through the ERM process, identified potential risks and incidents are assessed against the CFL's level of risk tolerance to provide reasonable assurance regarding the achievement of CFL's objectives.

CFL's objectives in managing risk include:

- Establishing and maintaining good governance and a sound system of internal controls;
- Facilitating the achievements of the organisation's objectives and goals through better identification of opportunities, threats and managing them;
- Developing a common understanding of risk across multiple functions to manage risk cost-effectively on an enterprise-wide basis;
- Ensuring compliance with the relevant regulatory and legal requirements;
- Improving the organisation's preparedness and resilience to unexpected events.

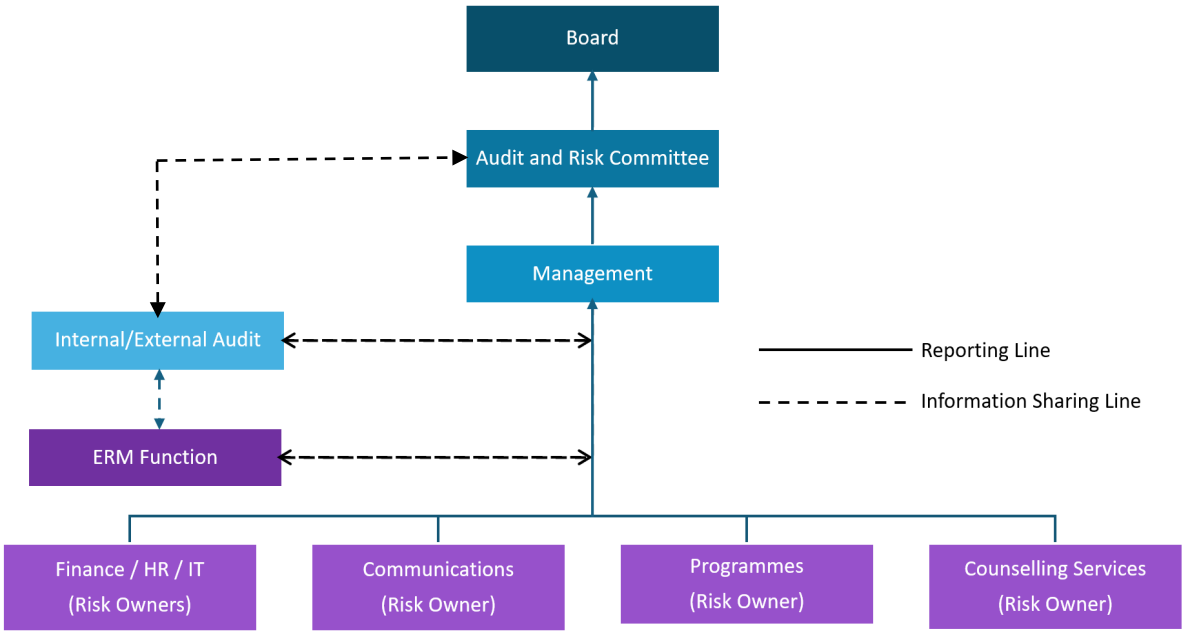
3. GOVERNANCE STRUCTURE

3.1. The Board has overall responsibility for the oversight of material risks in CFL. The Audit and Risk Committee (ARC) assists the Board in overseeing CFL's risk policies and ensuring the effectiveness of CFL's risk management system, including the identification and management of significant risks, and reports to the Board on material matters, findings and recommendations pertaining to risk management. It also oversees financial reporting risk and the adequacy and effectiveness of CFL's internal control and compliance systems.

3.2. Risk management programmes are administered through the ARC, which acts as a platform to review and discuss risk-related matters. (Refer to Appendix A for the Terms of Reference of the ARC.)

3.3. All CFL staff members and outsourced personnel with resonsibilities for risk management are responsible for the effective management of risks, including the identification of potential risks.

3.4. The following diagram presents an overview of the governance structure and the key components therein to ensure that there is proper segregation of duties and accountability:



Audience	Roles & Responsibilities
Board	• Provides the overall guidance and advice on ERM matters, assisted by the ARC ; and • Appoints and delegate the ERM oversight responsibility to the ARC.
Audit and Risk Committee ("ARC")	• Has overall responsibility in overseeing CFL's ERM framework, and reviewing and approving the appropriate risk management policies and procedures, and monitoring their implementation across the organisation; • Reviews the top risk profile and ensure the mitigation responses are consistent with the risk appetite • Refer to Appendix A for the Terms of Reference of the ARC.
Management	• Proposes the direction on ERM and is responsible for implementing the ERM policy and framework; • Sets and instils the right culture throughout CFL for effective risk governance; and • Ensures that the risks relevant to CFL are properly identified, assessed and monitored.
Internal / External Audit	• Provide independent assurance on the adequacy and effectiveness of the internal controls for the key risks; and • Share insights with the ERM Function and Management on significant issues and findings from the audits conducted to feed into the risk management process.
ERM Function	• Maintains the ERM policy framework in line with industry better practices and the CFL's operating environment; • Acts as internal 'ambassador' and knowledge resource for ERM; • Fosters a corporate risk culture through adequate training and communication sessions; • Coordinate with Risk Owners and Risk Champions on risk-related matters to obtain

	an enterprise-wide view of risks; and ● Prepares bi-annual risk reports to ARC.
Risk Owners	● Identify, assess, monitor and report potential risks in their areas of responsibility; ● Review and complete risk registers (risk assessment etc.) for all risks; and ● Monitor and report changes to existing risks or risk profiles to Management.

4. Enterprise Risk Management Process

CFL has developed an ERM Framework to manage change and uncertainty and is committed to establishing an organisation that ensures risk management is a core capability and an integral part of all CFL activities. This framework adopts a systematic approach to evaluating and improving the effectiveness of risk management and control.

4.1. Enterprise Risk Management Framework ("ERM Framework")

CFL adopts the following process in managing risk.

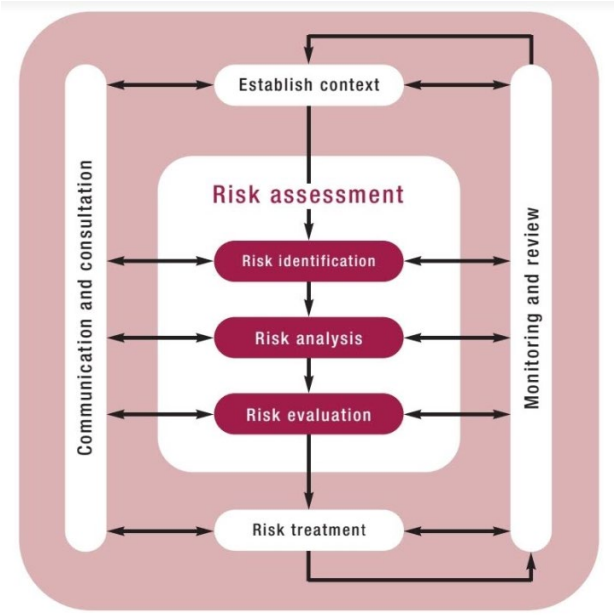


Figure 1 - ISO 3100 Risk Management Process Diagram

4.1.1. Establish the Context

This stage in the process articulates objectives, defines external and internal influences and sets the scope and risk criteria for the risk process.

- External context considers the social perception, regulatory, financial and other dimensions where CFL operates with limited influence over these macro-conditions.

- Internal context considers (or any changes to these elements) organisational objectives, people, systems and processes.

4.1.2. Risk Identification

Risk Identification describes the process of identifying risks in the form of threats and/or opportunities that will impact CFL's mission, values or set objectives. Risks may be identified through various channels, such as:

- Focus group
- Internal audit report
- Gap assessment by consultants
- Monthly departmental report
- SWOT analysis
- Interviews with key stakeholders

Examples of the Categories of Risks are listed in Appendix B as a guide to risk identification.

4.1.3. Risk Analysis

Risk Analysis involves prioritising and understanding the key risks to the Charity, including the likelihood and potential impact of the risk to the Charity. A catalogue of the full spectrum of risks, with impacts and likelihoods assessed, forms the CFL risk register (Appendix C). The Risk Register summarises the efforts undertaken by the organisation in a document that describes the risks, their severity, corresponding treatment and assigned ownership.

The Impact and Likelihood (of event) are used to calculate the risk score: Risk = Impact X Likelihood. The combined scores on a 5 x 5 Risk Assessment matrix will give scores ranging from 1 to 25, depending on the severity of the risk. The inherent and residual risk levels of the identified risks should be recorded in the Risk Register. Risk assessment can be done by using the following Risk Analysis Tools:

Table 1 - Definitions of Risk Impact levels

Score	1	2	3	4	5
Impact Descriptors	Insignificant	Minor	Moderate	Major	Critical

Table 2 - Definitions of Likelihood levels

Score	1	2	3	4	5
Likelihood Descriptors	Remote	Unlikely	Moderate	Likely	Almost Certain

Table 3 - Risk Assessment Matrix

Impact / Likelihood	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Critical (5)
Almost Certain (5)	Medium (5)	Medium (10)	High (15)	High (20)	High (25)
Likely (4)	Low (4)	Medium (6)	Medium (12)	High (16)	High (20)
Moderate (3)	Low (3)	Medium (6)	Medium (9)	Medium (12)	High (15)
Unlikely (2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium (10)
Remote (1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)

4.1.4. Risk Evaluation

Risk evaluation involves making a decision about what should be done about the risk. The scores will give the following Risk Level Ratings which will assist the Risk Owners to take appropriate actions. Some of the actions include:

- Determine approach – risk appetite (undertake or avoid)
- Determine treatment strategy – accept, avoid, reduce, transfer
- Set expected risk outcome – based on threshold of risk and cost benefit analysis
- Set priority and resource allocation – for risk treatment purposes
- Assign ownership of risk – define Risk Owner

Table 4 - Risk Level Rating

Risk Tier	Risk Score/Level	Action/ Response for Residual Risks
Tier 1	Red Zone High (15 – 25)	High-risk zone. A plan must be put in place to move to the Yellow Zone.
Tier 2	Yellow Zone Moderate (5 – 12)	State of active monitoring and progress. Risks are either partially or completely remediated and have achieved the targeted risk outcome. These risks will be subjected to periodic reviews as described under the risk management process.
Tier 3	Green Zone Low (1 – 4)	Managed state. Risks are at the default desirable and / or acceptable state. Risks are deemed well-remediated with comprehensive active controls in place.

4.1.5. Risk Treatment

Risk treatment involves modifying the risk in some way so that the positive outcomes are maximised, and negative outcomes are minimised. Based on the results of the Residual Risk Assessment, the following risk treatment can be used:

- Terminate - identifying actions to eliminate the risk, such as withdrawing from the activity.
- Accept - when the impact and likelihood are low, or when it would be too expensive to reduce/ mitigate a risk.
- Reduce - taking action to reduce/ mitigate either the impact or likelihood of the risk.
- Transfer - transferring the risk to a third party, e.g. insurance.

4.1.6. Monitor and Review

Risk monitoring focuses on the planned activities and processes for ongoing monitoring and surveillance of risk profile within the organisation. It communicates the approach for tracking, assessing, and reporting Risks to ensure that they remain within acceptable levels and that appropriate actions can be taken in a timely manner.

The risk universe, 'Tier 1' risk profile and risk register should be monitored and reviewed at least annually to ensure the continued relevance of ERM to the Charity.

4.1.7. Communication and Consultation

This stage of the process focuses on consolidating key information gathered throughout the risk profiling process and communicating to relevant persons, including the appropriate level of management and the Board. It would involve proper documentation to be put in place as part of the communication process.

It is important to ensure there is an appropriate level of awareness and appreciation for risk management throughout the organisation. Existing processes in the organisation should be refined by taking into consideration the outcome of the risk management process. In this respect, integrating the risk management process into planning, developing strategy and making decisions is encouraged.

4.2. Definitions

ISO 3100 Enterprise Risk Management Framework
ISO 31000 is an international standard that provides principles and guidelines for risk management. It outlines a comprehensive approach to identifying, analysing, evaluating, treating, monitoring and communicating risks across an organisation.

Risk
In the context of ISO 31000, risk is defined as the effect of uncertainty on objectives, whether positive or negative.

Impact / Consequence
The result or an effect of an event.

Likelihood / Probability
Factors that measure or indicate the frequency or probability of a risk event occurring.

Inherent Risk
Events or conditions that will prevent or impede the achievement of objectives before taking into consideration any controls that might alter the risk's impact or likelihood.

Residual Risk
The assessment of an event or condition after taking into consideration the effectiveness of controls and/or treatment plans.

Risk Register
A record of risks, risk assessments, risk mitigations, and action plans prepared by the responsible parties that help support the overall Enterprise Risk Management.

Risk Appetite
Is the amount of risk, on a broad level, CFL is willing to accept in the pursuit of its mission & vision.

Risk Tolerance
Is the acceptable level of variation relative to the achievement of objectives.

Treatments
Treatments are processes, systems, or any other measures in place to reduce the likelihood or impact of the risk, or detect indications of the risk occurring such that follow-up actions can be taken to reduce the likelihood or impact of the risk.

4.3. References

- A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000
- Enterprise Risk Management Toolkit for Charities and Institutions of a Public Character (IPCs)

Appendix A

CATHOLIC FAMILY LIFE
TERMS OF REFERENCE
AUDIT AND RISK COMMITTEE

This term of reference (TOR) is applicable to the Audit and Risk Committee (ARC) of the Board of Catholic Family Life (CFL) and is in addition to the TOR for all committees, which shall be deemed to form part of this TOR.

1. FUNCTIONS AND RESPONSIBILITIES
   A. Review the annual financial statements of CFL and recommend to the Board for adoption.
   B. Review the work of the external auditor, including the independence of the auditor, the (re)appointment of the auditor, audit fees, audit plan, and the findings and reports of the auditor.
   C. Monitor compliance with the Charity Code of Governance and prepare the Corporate Governance Checklist for submission to the Charity Commissioner for adoption by the Board.
   D. Oversee and review the adequacy and effectiveness of CFL's risk management framework and function. Review the findings of the internal auditor and ensure that the internal controls of CFL are adequate.
   E. Undertake other functions or responsibilities as may be directed by the Board

Appendix B

A Guide on Categories of Risk

Risk Category	Example of Risk
Financial	Funding risk
	Accounting and reporting risk
Compliance	Non-compliance with established laws and regulations risk
	Risk of violation of Personal Data Protection Act (PDPA)
	Conflict of interest risk (e.g. related party transactions not at arm's length)
	Professional liability risk
Technology	Risk of losing confidential data
	Risk of data corruption
Operational	Employee risk (e.g. retention, disgruntled employees)
	Adverse events risk (Internal and external)

Appendix C

Risk Register

Risk Ref	Risk Item	Risk Description	Risk Category	Risk Drivers	Risk Consequences	Date in Register	Inherent Risk Level	Mitigating Measures	Residual Risk Level	Risk Tier	Areas for Improvement	Risk Owner/Timeline

Risk Ref :	Unique Risk ID tagged to the identified Risk Item.
Risk Item :	Risk name or risk title.
Risk Description :	Concise description of the Risk
Risk Category:	Category of Risk e.g Financial, Compliance, Technology, Operational
Risk Drivers:	Circumstances or situations, which may arise internally or externally, that can potentially result in the risk occurring.
Risk Consequences:	Potential impact resulting from the occurrence of a risk, which may be expressed in several aspects (e.g. Financial, Operational, Reputational, etc.).
Inherent Risk :	Combined Risk Score of Inherent Impact X Inherent Likelihood.
Mitigating Measures	Existing and on-going Risk Treatment Plan / Response / Controls etc. *Concise Action Plan.
Residual Risk :	Combined Risk Score AFTER treatment. * Score must be smaller or equal to the Inherent Risk.
Risk Tier:	Risk Tier 1: Red Zone, Risk Tier 2: Yellow Zone, Risk Tier 3: Green Zone
Risk Owner/ TImeline	Risk Owner, Timeline of completion and Status (Open / Closed)

Appendix D

Risk Analysis Tools

Table 5 - Definitions of Likelihood levels

Likelihood Descriptors	(1) Remote	(2) Unlikely	(3) Moderate	(4) Likely	(5) Almost Certain
Prior risk incidents in industry	Did not happen in the industry	Has happened once in the industry	Happened several times in the industry	Happens regularly in the industry	Is a common occurrence in the industry
Probability	< 5%	Between 5% and 25%	Between 26% and 50%	Between 51% and 75%	> 75%

Table 6 - Definitions of Risk Impact levels

Impact Descriptors	(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Critical
Financial Impact Parameters					
Financial loss / impact	< X1% of income	X1% to X2% of income	X2% to X3% of income	X3% to X4% of income	> X4% of income
Operational Impact Parameters					
Unplanned outages for critical IT systems	Critical IT system outage for < 2 Hours	Critical IT system outage for 2 - 4 Hours	Critical IT system outage for 5 – 12 Hours	Critical l IT system outage for 13 - 24 Hours	Critical IT system outage for > 24 Hours
Reputational Impact Parameters					
Perceived damage to reputation	Adverse media coverage and / or internet activity resulting in minimal reputational damage amongst a selection of key stakeholders	Adverse media coverage and/or internet activity resulting in some damage to reputation amongst a selection of key stakeholders	Adverse media coverage and/or internet activity resulting in short-term (< 1 week) damage to reputation across all key stakeholders	Adverse media coverage and/or internet activity resulting in medium-term (1-2 weeks) damage to reputation across all key stakeholders	Adverse media coverage and/or internet activity resulting in prolonged (> 2 weeks) damage to reputation across all key stakeholders