Uniting Church in Australia
Synod of Victoria and Tasmania

RISK MANAGEMENT STRATEGY AND FRAMEWORK

Prepared by: Synod Risk Management Committee

Date Prepared and Issued: February 2010

TABLE OF CONTENTS

RISK MANAGEMENT STRATEGY AND FRAMEWORK
SYNOD of VICTORIA and TASMANIA

1. INTRODUCTION

Theological Basis and Strategic Objectives

The theological basis of risk management is central to the Synod's Risk Management Strategy and Framework. The theological basis is set out in Appendix 1.

The strategic objective is to apply systematic and consistent risk management methodologies across the Synod. This will enable identification of critical risk exposures as well as and improving capabilities for predicting and managing uncertainties. The strategy seeks to maximise positive benefits and to minimise any potential negative impact on the achievement of objectives.

The Synod Standing Committee's (SSC) key objective in risk management is to seek to align strategy, processes, people, technology and knowledge with the evaluation and management of uncertainties.

The SSC also seeks to develop an effective risk management culture that is consistent with the Church's values and to engage, as well as to encourage, managers across the Synod to foster the development of this culture.

Responsibility

Responsibility for the sound management of the Synod of Victoria and Tasmania (Synod) ultimately rests with SSC. As such, the SSC has recognised that it is necessary to further enhance risk management across the Synod and, as such, has appointed the Synod Risk Management Committee (RMC).

The objective of the RMC is to ensure that appropriate risk management is occurring throughout the Synod. The RMC's overriding responsibility is to ensure the establishment, maintenance and promotion of an appropriate Risk Management Framework (RMF) throughout the Synod. In undertaking its role the RMC will provide advice and assistance, including submitting reports and recommendations, to the SSC on risk management matters.

In accordance with the RMC's charter, the RMC has authority to request that all bodies within the Synod, Presbyteries, Congregations and Agencies comply with the RMF requirements.

The responsibility for the daily management of risk is a shared activity, and details of specific responsibilities for Synod Bodies are provided below in Section 4.

Document Overview and Applicability

The RMF detailed below, which has been endorsed by the SSC, sets out sound risk management practices and is based on the International Risk Management Standards (ISO/FDIS 31000: 2009 and IEC/FDIS 31010).

These International Standards are intended to meet the needs of a wide range of stakeholders, including:

- those responsible for developing risk management policy within their organisation;
- those accountable for ensuring that risk is effectively managed within an organisation as a whole or within a specific area, project or activity;

- those who need to evaluate an organisation's effectiveness in managing risk; and
- developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed.

It is intended that these practices outlined in the RMF will be the minimum standards to be initially adopted by certain key Synod Bodies (as defined in Appendices 7 & 8) and, in due course, by all key Synod Bodies.

The RMC assumes responsibility for the scheduling of a staged rollout of the RMF within the Synod and, at the appropriate time, will initiate contact with the relevant Synod Bodies. *The rollout strategy will allow for the recently implemented Presbytery structure to become fully established across the Synod.*

It is recognised that this RMF may need to be simplified for smaller Synod Bodies to ensure there is commonality in the approach to risk management across the Synod.

The following sections of the RMF describe:

1. What is risk management;
2. Principles for managing risk;
3. Synod's risk appetite;
4. Risk management policy;
5. Risk management strategy and framework;
6. Specific responsibilities and roles for risk management;
7. Risk management processes and controls.

What is Risk Management?

Risk management refers to the coordinated activities that direct and control an organisation with regard to risk. It includes the architecture (principles, framework and process) for managing risks effectively and the application of that architecture to particular risks.

The management of risk should be directed towards realising potential opportunities whilst managing adverse effects. This involves proactively managing activities to achieve an appropriate balance between realising opportunities for gains while minimising losses.

Risk management is not an isolated process, rather it is an integral part of sound management as well as an important means of improving decision making and operational activities.

The risk management process involves the systematic application of management policies, procedures and practices to the tasks of identifying, analysing, evaluating, treating, monitoring and reviewing risks.

Risk management develops the control environment and enhances governance, all of which should provide reasonable assurance to senior managers and governing bodies that the objectives of the Synod will be achieved within a tolerable degree of residual risk. Such governance processes across the Synod are vital to ensure that the interests of all stakeholders are protected.

Effective risk management will allow Synod Bodies to respond quickly and efficiently to unexpected threats and to take advantage of unexpected opportunities.

Principles for Managing Risk

The ISO/FDIS 31000:2009 standard states that for risk management to be effective, an organisation should at all levels comply with the principles below.

a) **Risk management creates and protects value**

Risk management contributes to the achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

b) **Risk management is an integral part of all organisational processes**

Risk management is not a stand-alone activity that is separate from the main activities and processes of the organisation. Risk management is part of the responsibilities of management and an integral part of all organisational processes, including strategic planning and all project and change management processes.

c) **Risk management is part of decision making**

Risk management helps decision makers make informed choices, prioritise actions and distinguish among alternative courses of action.

d) **Risk management explicitly addresses uncertainty**

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

e) **Risk management is systematic, structured and timely**

A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

f) **Risk management is based on the best available information**

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement.

g) **Risk management is tailored**

Risk management is aligned with the organisation's external and internal context and risk profile.

h) **Risk management takes human and cultural factors into account**

Risk management recognises the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organisation's objectives.

i) **Risk management is transparent and inclusive**

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organisation, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

j) **Risk management is dynamic, iterative and responsive to change**

As external and internal events occur, context and knowledge change, monitoring and review take place, new risks emerge, some change, and others disappear. Therefore, risk management continually senses and responds to change.

k) **Risk management facilitates continual improvement of the organisation**

Organisations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organisation.

Generally, across the Synod, key principles in establishing a dynamic approach to risk management will include:

- Recognition that risk management is an integral part of good management practice and that it should be integrated into all aspects of Synod's culture, decision making, programs, practice, planning and communication strategies;

- A strong and sustained Synod wide commitment to risk management by senior management levels and governing bodies (including adequate resourcing);

- Recognition that all members including staff, clergy and volunteers engaged in activities of agencies, schools, presbyteries and congregations have a role to play in risk management;

- Implementation of the ISO/FDIS 31000:2009 and IEC/FDIS 31010 standards as the preferred model for risk management across the Synod;

- Adoption of consistent standards by key Synod Bodies for analysing, evaluating and reporting (to appropriate bodies) on risk management;

- Pro-active promotion of a culture of risk awareness, which is supported by training in risk management;

- Establishment of governance arrangements, and clear delegation of responsibilities (and accountability) to appropriate personnel, to ensure the effective implementation of the Synod's approach to risk management and the maintenance of an ongoing focus on risk management;

- The existence of explicit risk management performance goals against which the key Synod bodies and individual manager's performance is measured;

- An effective communication plan that ensures ongoing consultation with internal and external stakeholders.

Synod's Risk Appetite

It is recognised that certain risks can never be completely eliminated and as such, the overall risk management objective is to manage risks to achieve a low to moderate risk significance (as detailed in Appendix 3). That is where no risk, or combination of risks, will result in a loss event that would generate a material adverse financial or other adverse impact upon the Synod.
Synod has a conservative risk appetite and requires a risk averse culture, as outlined in Appendix 1. This is fundamental to an effective risk management strategy.

2. RISK MANAGEMENT POLICY

In order to meet strategic objectives, the objective of the risk management policy is to apply systematic and consistent risk management methodologies across the Synod in order to identify critical risk exposures as well as to focus on improving capabilities for predicting and managing uncertainties. The policy seeks to maximise positive benefits and to minimise any potential negative impact on the achievement of objectives.

The policy also seeks to engender an effective risk management culture, which is consistent with the Church's values, by engaging and encouraging managers across the Synod to foster the development of this culture.

3. RISK MANAGEMENT STRATEGY AND FRAMEWORK

The RMC has adopted the overall philosophy of the International standards (ISO/FDIS 31000:2009 and IEC/FDIS 31010), which provides a holistic management process incorporating comprehensive detail for the management of risk.

The adoption of this standard will provide an important tool for boards, senior management, church officers, other employees and volunteers to understand the Synod's approach to risk management.

It is intended that the identification and management of risk occur at the relevant levels across the Synod, by utilising both the bottom up and top down processes.

Note that the RMF is the totality of systems, structures, processes and people across the Synod involved in identifying, analysing, evaluating, treating, monitoring, and reviewing all internal and external sources of risk that could have a material adverse impact on the Synod.

Risk Management Strategy includes the following:

- Implementation of proactive risk management strategies to protect the Synod, now and in the future;
- Adoption of appropriate governance structures/bodies;
- Crisis management and disaster recovery plans;
- Continuous identification, assessment and management of risks, incorporating the use of ISO/FDIS 31000:2009 and IEC/FDIS 31010;
- Clearly defined managerial responsibilities including assignment of particular risk management responsibilities to appropriate personnel;
- Efficient management of information and records;
- Timely and accurate management reporting, monitoring and actions to address significant issues adversely affecting areas across the Synod;
- Timely and accurate reporting to governing bodies (including the RMC);
- Training and guidance of relevant personnel in the management of risk.

Once the RMF has been implemented, the framework itself must continue to be managed (monitored, reviewed and improved) so as to ensure that the desired risk management objectives are being achieved.

Further information relating to the management of the framework is provided on Appendix 2.

Some Synod Bodies may already have a risk management process in place. This is acceptable if such processes meet the requirements of this RMF.

4. SPECIFIC RESPONSIBILITIES AND ROLES FOR RISK MANAGEMENT

Synod Standing Committee (SSC)

The SSC is responsible for charting direction and determining strategy for the Synod, including the risk management strategy. This responsibility includes the reviewing of risks and ensuring that risks are appropriately managed as well as ensuring that compliance with regulatory requirements and ethical standards occurs.

The SSC's key objective in risk management is to seek to align strategy, processes, people, technology and knowledge with the evaluation and management of uncertainties.

The SSC recognises that it is centrally responsible for oversight of risk management. However the SSC expects boards, committees, the General Secretary, management and various other personnel within Synod Bodies, all operating within the control systems that are currently in place, to undertake the daily management of risks. Further, in discharging its responsibility for overall risk management, the SSC delegates a number of key functions to the RMC and the Synod Audit Committee (SAC), which assist and report to the SSC.

The SSC, through the budgetary process, makes decisions and allocates resources regarding the oversighting of risk management.

In order to ensure that key risks are identified, appropriately managed and reported, the SSC established the RMC. The SSC required that the RMC develop and, subsequently ensure that, an appropriate RMF is implemented and maintained across the Synod. As such, the SSC has adopted and endorses the RMF, which is detailed below.

Risk Management Committee (RMC)

The RMC was inaugurated in December 2007 and is governed by the SSC approved RMC Charter. The RMC meets regularly, reports to the SSC and Synod, and interfaces with key Synod Bodies.

In undertaking its role the RMC will provide advice and assistance, including submitting reports and recommendations, to the SSC on risk management matters.

RMC's responsibilities include:

- Ensuring that the RMF is developed, maintained and promoted across the Synod;
- Review key risks and how they are changing;
- Identify emerging risks and their implications;
- Oversee how major risks are managed across Synod, and within those bodies with greater risks;
- Prepares and maintains the overall Synod risk register in respect of significant risks for key bodies;
- Reports to the General Secretary or SSC on hot issues, and proposes action plans;
- Provide recommendations and advice to the SSC in relation to risk management;
- Maintain its awareness of legal and other relevant performance standards;
- Will not, and should not, be expected to manage major problems;
- Promote the development of performance management objectives in relation to risk.

Synod Audit Committee (SAC)

The role of the SAC is to provide an objective independent non-executive review and oversight of internal financial reports as well as to identify and ensure appropriate management of financial risks in accordance with this Risk Management Framework.

The SAC also continues to provide advice and assistance to the SSC. In order to achieve these objectives, the SAC carries out RMC functions in respect of financial risks, specifically by:

  - identifying key financial risks and how these are changing;
  - identifying emerging financial risks and their implications;
  - overseeing how major financial risks are managed across Synod, and within those bodies with greater risks;

- recording key Synod-wide financial risks through maintenance of a Risk Register (based on information provided by Synod Bodies);
- regularly reporting financial risks and risk monitoring activities to the RMC;
- reporting to the RMC on hot financial issues, and formulating an action plan;
- maintaining its awareness of legal and other relevant performance standards;
- providing input to RMC in relation to SAC's overall risk management role;
- approves appointment of an internal auditor;
- monitors outcomes of the internal audit process;
- receives and reviews reports from the external auditors.

The risk management activities undertaken by the SAC do not override the authority, independence or responsibility of SAC in relation to the Standing Committee or Synod.

The SAC usually meets monthly and is accountable to the SSC. The SAC's Charter sets out its roles and responsibilities.

Synod Head Office Operations

- The Synod General Secretary has management responsibility for development and implementation of Synod strategic initiatives, senior management selection and development of budgets and oversight of Synod Operations.

- The General Secretary is supported by the Senior Leadership Team (SLT), which includes Executive Directors from the key Synod Bodies within Head Office of the Synod. From a risk management perspective, these key Synod Bodies manage both operational risk and compliance frameworks as well as related action plans.

- The Executive Director Administration and Finance (EDAF) is responsible for management, monitoring and controlling of financial risks across the Synod. The EDAF is a member of the SSC, RMC, SAC and the SLT.

- In order to enhance risk management, the appointment of an Internal Auditor and/or a Compliance Manager is being investigated.

- The Legal Reference Committee ensures that legal, regulatory and other guidelines are consistently applied.

Managers and Officers of Key Synod Bodies

Managers and Officers of key Synod Bodies, as part of their position descriptions, are accountable for the management of risk and should ensure that sufficient resources are applied to the management of risk.

Management utilises resources to undertake specific responsibilities including:

- Implementing and maintaining the RMF;
- Promotion of risk awareness and training of relevant personnel;
- Understanding the organisation and its internal and context;
- Ensuring that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls;
- Ensuring that culture and risk management policy are aligned;
- Determining risk management performance indicators that align with performance indicators;
- Aligning risk management objectives with the objectives and strategies;
- Embedded risk management within all of the organisation's practices and processes;

- Establishing internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk;
- Arranging independent audit, testing or peer review of key bodies on a rolling basis;
- Ensuring that legal, regulatory and other guidelines are consistently applied;
- Maintaining risk management records and manuals;
- Identifying and quantifying any new risk within their responsibility;
- Initiating and implementing improvement strategies until the level of risk(s) becomes acceptable;
- Ensuring that any required new controls are implemented;
- Reporting to management and to the RMC.

External Auditors

The Uniting Church Regulations specify the extent to which external auditors must be appointed. The role of these auditors is to provide independent and objective view as to the truth and fairness of the financial statements.

5. RISK MANAGEMENT PROCESSES AND CONTROLS

Process Overview

The proposed process for managing risks is consistent with International Risk Management Standards ISO/FDIS 31000: 2009 and IEC/FDIS 31010. Overall, this is a structured process processes that must be undertaken in conjunction with key stakeholders. Appropriate communication and consultation is essential. Additionally, it is absolutely imperative that key personnel have accountability for focusing on the identification and management of risks within in their units of responsibility.

Specifically, the process involves the following key steps:

- Establishing the context;
- Risk Assessment:
  - Risk Identification;
  - Risk analysis;
  - Risk evaluation;
- Risk treatment;
- Monitoring and reviewing.

These processes are described in Appendix 3.

Appendix 4 details the main risk categories to be adopted in the above process.

Communication and Escalation

As part of any risk management process, information processes must be established, maintained and utilised to assist in the management, communication, reporting and monitoring of risk issues and outcomes.

Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

A consultative team approach may:

- help establish the context appropriately;
- ensure that the interests of stakeholders are understood and considered;

- help ensure that risks are adequately identified;
- bring different areas of expertise together for analysing risks;
- ensure that different views are appropriately considered when defining risk criteria and in evaluating risks;
- secure endorsement and support for a treatment plan;
- enhance appropriate change management during the risk management process;
- develop an appropriate external and internal communication and consultation plan.

Communication and consultation with stakeholders is important as they make judgements about risk based on their perceptions of risk. These perceptions can vary due to differences in values, needs, assumptions, concepts 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. This should be developed at an early stage.

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

It will be critical that relevant, accurate and timely information is appropriately provided to risk managers as well as governing bodies in order to identify, analyse, evaluate, treat, monitor and review activities so as to effectively manage exposure to risk.

Such processes must ultimately lead to the RMC (and SSC through the RMC) being informed of Synod wide risks.

It is imperative that tools such as a Risk Register (refer to Appendices 9 and 5) and the Extreme Risk Report (refer to Appendix 6) are prepared, maintained and provided to management as well as to relevant governing bodies.

- ***Risk Register***

The identification of all possible sources of risk is an essential component of risk management. This is particularly important, as unidentified risks may pose a major threat to the Synod. In order to ensure that risks are systematically and appropriately identified, analysed, evaluated, reported, monitored and reviewed, a risk register should be maintained for all key Synod Bodies. Refer to Appendix 4 for the risk categories that are applicable for the Synod.

Specifically, a Risk Register, which should be generated as an output from the risk assessment process, is an effective tool that succinctly captures critical factors relating to all key risks. For each risk, the causes, potential effects, risk rating and actions are documented. These actions can then become the basis for a treatment plan Appendix 5 provides an example of a simplistic Risk Register.

In order to assist Synod Bodies in the management of risks, the RMC has acquired a web-based risk management system from WSP Risk Management Solutions. The **WSP system** enables the online recording and reporting of risks as well as facilitating the monitoring of risks. A standardised Risk Register is a key output of the system. Appendix 9 provides an overview of the WSP system.

It is intended that the WSP system will be available to those UCA bodies which require a sophisticated system to assist in the management, monitoring and reporting of risks. During the early part of 2010, the RMC will, in consultation with appropriate key Synod Bodies, schedule the rollout of this system. Subsequently, other interested bodies requiring the implementation of the WSP system should contact either the Synod Project Manager, Risk

Management System or the Executive Director Administration and Finance, who are located at 130 Little Collins St, Melbourne.

- ***Extreme Risk Report***

This is to be completed for new and emerging risks. The Extreme Risk Report (Refer to Appendix 6) must be completed by the responsible officer within a key Synod Body.

Extreme risks are those risks with an assessed inherent risk rating of 7 or more (on the 10 point scale – refer Appendix 3, Table 5).

Upon recognition of such risks, the Extreme Risk Report must be forwarded to the Synod Executive Director Administration & Finance, 130 Little Collins St, Melbourne, within 48 hours of the risk occurring.

Proactive Risk Mitigation

To enhance the effectiveness of the risk management strategy, key Synod Bodies should not only focus on identifying and managing known risks, but must also proactively manage operations so as to minimise the likelihood of certain risks occurring.

As part of a proactive and effective risk management process, various controls should be put into place as preventative measures. Control mechanisms should be utilised to ensure that the policies and procedures established for risk management are adhered to.

- ***Controls***

The process for mitigation and control will include:

- Risk Management Framework;
- Effective Synod wide governance structures;
- RMC and SAC establishing and maintaining control processes;
- Clearly defined managerial responsibilities/ and reporting lines;
- Crisis Management team;
- In-house legal counsel;
- Reviews by external and internal audit;
- Adoption (by key Synod Bodies) of risk management strategies;
- Business Continuity and Disaster Recovery Plans.
- Risk management policies and procedure manuals;
- Risk registers;
- Board policies, policies and procedural manuals for key activities such as Accounting, Legal, OH&S and Human Resources;
- Compliance policies and procedures;
- Budgetary, periodic reporting and other financial controls;
- Delegated authorities' policies;
- Efficient management of information and records;
- Communication (up and down) of risk management strategies and processes;
- In-house Insurance / Risk Manager;
- External Risk Management Consultants;
- Insurance Brokers;
- Synod Property Officer;
- Code of Conduct;
- Standard Conditions of Employment;
- Succession planning;
- Documented performance objectives / Performance Appraisals including Key Performance Indicators and responsibility for risk management;

- Training programs (including risk management);
- Accreditation programs;
- Computer Virus Management/ Antivirus software.

Risk Awareness and Culture

All personnel are recognised as having a role in risk management, from vigilance in the identification of risks through to treatment. In addition to personnel with specific risk management responsibilities, all other personnel should be actively encouraged to participate in the risk management process.

It is essential that education of personnel in relation to specific risks occur. However, further consideration should be given to overall training requirements in order that an appropriate culture and responsibility are nurtured across the Synod.

As the Synod seeks to develop an effective risk management culture, all managers are regarded as being responsible for fostering the development of a risk management culture.

Fundamental to this culture is:

- Acceptance by staff of the need to manage risk;
- Management support and responsiveness to pro-active risk management approaches by staff;
- Open communication with all stakeholders.

Review of Risk Management Framework

This version of the RMF has been reviewed by WSP Risk Solutions.

In order to ensure the ongoing relevance and effectiveness of the RMF, the RMF is required to be reviewed by the RMC and by independent external consultants on a periodical basis.

`

APPENDIX 1

RISK MANAGEMENT AND THE SYNOD OF VICTORIA AND TASMANIA

1.1 Our Theological Basis

Risk management within the Synod is a problematic area as it is often perceived as a process made in deference to secular values and corporate structures. The reality is that the Church exists within a society that has quite specific expectations in these areas. However, it is important to acknowledge at the outset that the Synod's involvement in risk management is primarily undertaken out of theological awareness and necessity rather than out of any societal expectation.

In the first instance, our awareness of risk management and our commitment to the processes set out in this document relate to our historical and traditional understanding of STEWARDSHIP. The Church acts as steward of its resources which are to be used for the mission of God and the continuation of the Church into future generations (in whatever shape or form). Caring for those resources is a duty that we accept as the Synod and as individual members of the Church.

Secondly, however, risk management is part of the ongoing conversation within the Church about "rendering to Caesar that which is Caesar's". As Church we operate in a society that has certain legal expectations that we must uphold if we wish to continue to operate within that society. We may choose to withdraw from certain areas of the life of our society but until we make that deliberate choice it is incumbent upon us to live within the legal rules and guidelines of our 21st century society.

1.2 Risk Management within the Church

Risk management is part of our life as Church in two important ways.
First, since its very beginnings, the Church as the community of followers of Jesus has been called to take risks. In the Uniting Church, for many years part of our public face (our branding, it would be said today) was the slogan: "Risking the Way of Jesus". Under that slogan we were called to radical discipleship that ultimately put all we are as Church "at risk" as we sought to be faithful to God's call and the directions for our life that were necessitated by that call. Whilst the slogan is not as prominent as it once was, the implications are just as real for us in 2007.

Within that context, risk management is undertaken in various ways as different bodies within the Church seek to live a lifestyle that reflects such a call to radical discipleship. Decisions are made and directions are followed that result in a cost to the Church and to the individuals involved. The planning around those decisions is part of the risk management that is undertaken on behalf of the Church. In that context, risk management does not mean that new directions should not be followed. Rather it is decided that the risks to be confronted are worthwhile confronting for the ultimate good of the gospel or the life of the Church or individual disciple. The weighing up and ultimate acceptance of those risks is part of the Church's understanding of risk management at the broadest level.

Secondly, risk management has a more specific meaning within the Church. As the Uniting Church has increasingly found itself making decisions with implications in areas of finance, employment, insurance and property, a more formal process of risk management has developed along the lines of risk management procedures that have been followed by other organisations within our society. Whilst this aspect of risk management is a more "business-oriented task" it is not dissimilar to what has been described above. The decisions that the Church has sought to make in these areas of its life have always been in the context of discipleship. Finance and property in the Church, for example, are not ends in themselves. They are merely tools that enable us to be the followers of Jesus within our society. They

are there to support mission and to enable discipleship to be lived out in a broad sense. Again, risk management does not imply that risks ought not to be taken but it provides procedures that ensure that the risks that are taken are taken intentionally because the missional goal is deemed to be worth the risk.

Within that broad context, risk management has three components:

- Giving the Church and its bodies confidence to identify and pursue new opportunities for strategy and mission.

- the management of risk at a very general level that may have an impact on the life of the Church because of the financial cost that has to be paid, or the reputational risk to the good name of the Church, which arises in situations where decisions incur a pastoral cost or where situations of abuse arise;

and, more specifically,

- the very specific necessity that is incurred by the legal compliance that we are to work within as an organisation that deals in areas of finance, property, insurance, human resources etc.

Whilst these components are separate, these have major impacts on the life of the Church. Unless they are managed appropriately the Church faces the very real risk of wasting the resources for which we are responsible for no missional benefit, of breaching pastoral responsibilities or of breaching legal and ethical expectations that could result in serious financial and structural penalties. In some cases, not only would hefty fines need to be paid for non-compliance but we could quickly be stripped of the authority to act in areas of mission, finance and property or as an employer.

1.3 The Synod's role in Risk management

Risk management rightly belongs within the oversight of each area of the Church. Presbyteries, Congregations and all other bodies that are part of the Church necessarily must undertake appropriate risk management as part of their stewardship of the resources to which they have access.
However, the Synod has a particular role over and beyond that of other bodies. This comes about for three reasons:

(a) Clause 32 of the Constitution of the Uniting Church states that the Synod "shall exercise executive, administrative, pastoral and disciplinary functions over the Presbyteries within its bounds….". This statement is repeated in Reg 3.5.11 (although the word "over" there becomes the phrase "in relation to"). The implication of this is that there are some "executive, administrative, pastoral and disciplinary" functions that can best be handled centrally by the Synod. I would argue, that whilst there is clearly a local responsibility for risk management, the overarching responsibility is one of those executive and administrative functions that belong to the Synod.

(b) All Church property is vested in the name of the Synod's Property Trust and the Trust is the legal body that ultimately bears the brunt of any property or legal action taken in the name of Church. Whatever body has the more specific stewardship oversight of resources, the Property Trust has an ultimate responsibility. Again, there is an argument here for central oversight.

(c) Even in the case of those bodies within the Uniting Church that are separately incorporated, these bodies operate under the name and our logo of the UCA. Whilst they may have very effective oversight of the risks that are relevant to their function,

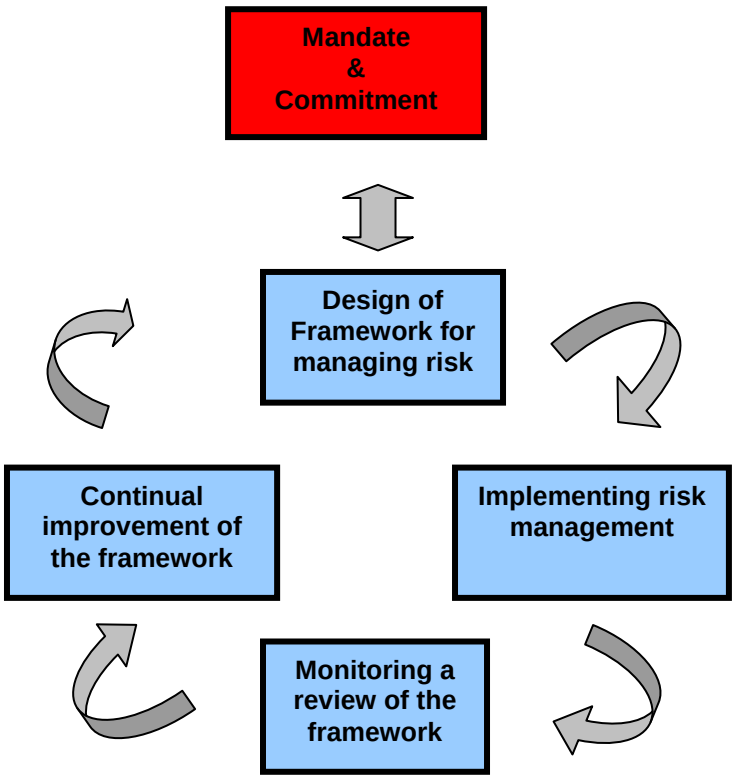
the good name of the Church requires that the risk management processes of these bodies feeds into the overall risk management structure of the Synod.

For these reasons, the Synod itself needs to have oversight of risk management at the broadest level. Each body shares the responsibility and some of those bodies will undertake their own, very rigorous risk management procedures but ultimately it is the Synod that bears the responsibility. Cooperation is needed from all Church bodies to ensure that even where appropriate procedures are followed by a particular church organisation, the Synod is aware of the processes undertaken and any risks that are evident.

APPENDIX 2

FRAMEWORK FOR MANAGING RISK

The management of the framework is depicted diagrammatically below.



The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organisation at all levels. The framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of the organisation. The framework ensures that information about risk derived from these processes is adequately reported and used as a basis for decision making and accountability at all relevant organisational levels.

The information below describes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner, as shown in the diagram above.

If existing management practices and processes include components of risk management or a formal risk management process, then these should be critically reviewed and assessed against the ISO/FDIS 31000: 2009 International Standard, in order to determine their adequacy and effectiveness.

Mandate and commitment

The introduction of risk management and ensuring its on-going effectiveness require strong and sustained commitment by management, as well as strategic and rigorous planning to achieve commitment at all levels.
Management should:

- define and endorse the risk management policy;

- ensure that the organisation's culture and risk management policy are aligned;
- determine risk management performance indicators that align with performance indicators of the organisation;
- align risk management objectives with the objectives and strategies of the organisation;
- ensure legal and regulatory compliance;
- assign accountabilities and responsibilities at appropriate levels within the organisation;
- ensure that the necessary resources are allocated to risk management;
- communicate the benefits of risk management to all stakeholders;
- ensure that the framework for managing risk continues to remain appropriate.

Design of framework for managing risk

1. Understanding of the organisation and its context

Before starting the design and implementation of the framework for managing risk, it is important to evaluate and understand both the external and internal context of the organisation, since these can significantly influence the design of the framework.

Evaluating the organisation's external context may include, but is not limited to:

- the social and cultural, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organisation;
- relationships with, and perceptions and values of, external stakeholders.

Evaluating the organisation's internal context may include, but is not limited to:

- governance, organisational 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);
- information systems, information flows and decision making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders and the organisation's culture;
- standards, guidelines and models adopted by the organisation;
- the form and extent of contractual relationships.

2. Establishing risk management policy

The risk management policy should clearly state the organisation's objectives for, and commitment to, risk management and typically addresses the following:

- the organisation's rationale for managing risk;
- links between the organisation's objectives and policies and the risk management policy;
- accountabilities and responsibilities for managing risk;
- the way in which conflicting interests are dealt with;
- commitment to make the necessary resources available to assist those accountable and responsible for managing risk;
- the way in which risk management performance will be measured and reported;

- commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances.

The risk management policy should be communicated appropriately.

3. Accountability

The organisation should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls.
This can be facilitated by:

- identifying risk owners that have the accountability and authority to manage risks;
- identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;
- identifying other responsibilities of people at all levels in the organisation for the risk management process;
- establishing performance measurement and external and/or internal reporting and escalation processes;
- ensuring appropriate levels of recognition.

4. Integration into organisational processes

Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient. The risk management process should become part of, and not separate from, those organisational processes. In particular, risk management should be embedded into the policy development, business and strategic planning and review, and change management processes.

There should be an organisation-wide risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of the organisation's practices and processes.

5. Resources

The organisation should allocate appropriate resources for risk management.

Consideration should be given to the following:

- people, skills, experience and competence;
- resources needed for each step of the risk management process;
- the organisation's risk processes, methods and tools to be used for managing risk;
- documented processes and procedures;
- information and knowledge management systems;
- training programmes.

6. Establishing internal communication and reporting mechanisms

The organisation should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk.

The mechanisms should ensure that:

- key components of the risk management framework, and any subsequent modifications, are communicated appropriately;
- there is adequate internal reporting on the framework, its effectiveness and the outcomes;
- relevant information derived from the application of risk management is available at appropriate levels and times;
- there are processes for consultation with internal stakeholders.

These mechanisms should include processes to consolidate risk information where appropriate from a variety of sources, taking into account its sensitivity.

7. Establishing external communication and reporting mechanisms

The organisation should develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

- engaging appropriate external stakeholders and ensuring an effective exchange of information;
- external reporting to comply with legal, regulatory, and governance requirements;
- providing feedback and reporting on communication and consultation;
- using communication to build confidence in the organisation;
- communicating with stakeholders in the event of a crisis or contingency.

These mechanisms should include processes to consolidate risk information from a variety of sources, taking into account its sensitivity.

Implementing risk management

1. Implementing the framework for managing risk

In implementing the organisation's framework for managing risk, the organisation should:

- define the appropriate timing and strategy for implementing the framework;
- apply the risk management policy and process to the organisational processes;
- comply with legal and regulatory requirements;
- ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;
- hold information and training sessions;

2. Implementing the risk management process

Risk management should be implemented by ensuring the risk management process outlined in Appendix 3 is applied through a risk management plan at relevant levels and functions of the organisation as part of its practices and processes.

Monitoring and review of the framework

In order to ensure that risk management is effective and continues to support organisational performance, the organisation should:

- measure risk management performance against indicators, which are periodically reviewed for appropriateness;
- periodically measure progress against / deviation from the risk management plan;
- periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;

- report on risk, progress with the risk management plan and how well the risk management policy is being followed;
- review the effectiveness of the risk management framework.

Continual improvement of the framework

Based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and plan can be improved. These decisions should lead to improvements in the organisation's management of risk and its risk management culture.

APPENDIX 3

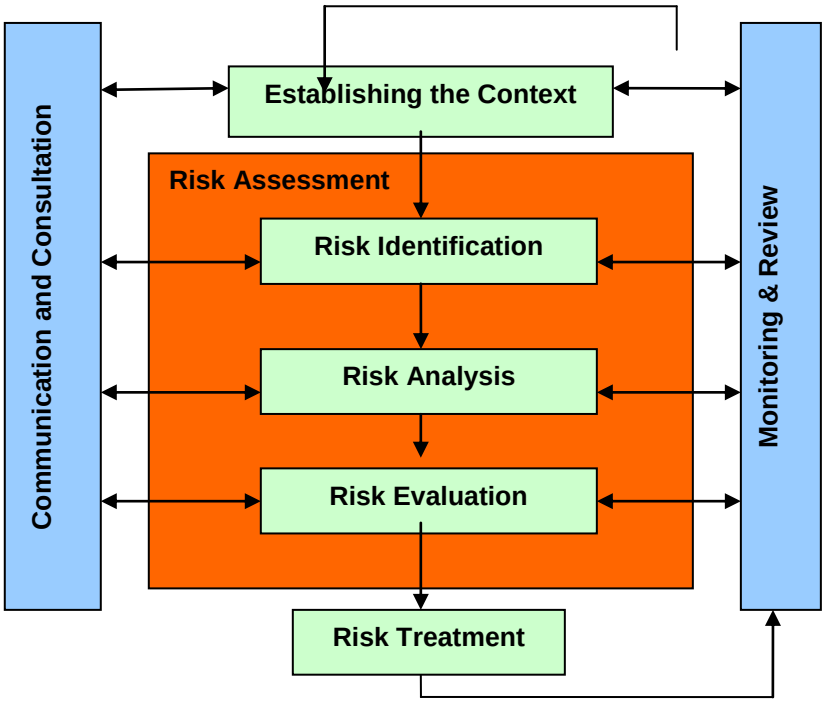
RISK MANAGEMENT PROCESS OVERVIEW

The proposed process for managing the Synod's risks is consistent with International Risk Management Standards ISO/FDIS 31000:2009 and IEC/FDIS 31010 It involves six steps and, throughout the process, includes feedback through a monitoring and review process and appropriate communication and consultation. The risk management process should be an integral part of management, embedded in the culture and practices as well as tailored to business processes.

These processes are outlined below:

Table 1

Process for Managing Risk



Step 1: Establishing the Context

By establishing the context, a Synod body articulates its objectives and defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process.

Contextual factors that should be considered include:

- Applicable laws, regulations, rules or standards;
- Competitors;
- Contractual relationships;
- Goals, objectives and strategies;
- Financial and economic environment;
- Governance, management structures and accountabilities;
- Key areas of resistance;
- Key drivers and trends;
- Level of acceptable risk;
- Major areas of risk ;
- Policies and guidelines;
- Political, social, client, stakeholder and cultural aspects etc ;
- Regional factors;
- Reporting processes;
- Resources;
- Strengths, weaknesses, opportunities and threats;
- Technology and information systems;
- Vision, mission and values.

The objectives, strategies, scope and parameters of the activities of a Synod body should be established. The management of risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk management. The resources required, responsibilities, authorities, and records to be kept should also be specified.

The context of the risk management process will vary according to the needs of the Synod body. It can involve, but is not limited to:

- defining the goals and objectives of the risk management activities;
- defining responsibilities for and within the risk management process;
- defining the scope, as well as the depth and breadth of the risk management activities to be carried out;
- defining the activity, process, function, project, product, service or asset in terms of time and location;
- defining the relationships between a particular project, process or activity and other projects, processes or activities;
- defining the risk assessment methodologies;
- defining the way performance and effectiveness is evaluated in the management of risk;
- identifying and specifying the decisions that have to be made; and identifying, scoping or framing studies needed, their extent and objectives, and the resources required.

Attention to these and other relevant factors should help ensure that the risk management approach adopted is appropriate to the circumstances, to the Synod body and to the risks affecting the achievement of its objectives.
The Synod body should also define criteria to be used to evaluate the significance of risk. The criteria should reflect the Synod body's values,

objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the Synod body subscribes. Risk criteria should be consistent with the Synod body's risk management policy, be defined at the beginning of any risk management process and be continually reviewed.

When defining risk criteria, factors to be considered should include the following:

- the nature and types of causes and consequences that can occur and how they will be measured;
- how likelihood will be defined;
- the timeframe(s) of the likelihood and/or consequence(s);
- how the level of risk is to be determined;
- the views of stakeholders;
- the level at which risk becomes acceptable or tolerable;
- whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

Step 2: Risk Assessment

- **Introduction**

The purpose of risk assessment is to provide evidence based information and analysis to make informed decisions on how to treat particular risks and how to select between options. Risk assessment comprises the processes for identifying, analysing and evaluating risks. Ideally, a Synod body will utilise a range of risk identification techniques including brainstorming, work breakdown analysis, or expert facilitation.

Following the identification of risks, risk analysis considers possible causes, sources, likelihood and consequences to establish the inherent risk. Existing management controls should be identified and effectiveness assessed to determine the level of residual risk. After this analysis, an evaluation of the level of risk is required to make decisions about further risk treatment.

Risk assessment may be undertaken in varying degrees of depth and detail and using one or many of the risk assessment techniques. Refer to Appendix 10 for assessment techniques identified in IEC/FDIS 31010.

Once the risk assessment objectives and scope have been defined, the techniques should be selected, based on applicable factors such as:

- the objectives of the study;
- the needs of decision-makers, as in some cases a high level of detail is needed whereas in others a more general understanding is sufficient;
- the type and range of risks being analysed;
- the potential magnitude of the consequences;
- the degree of expertise, human and other resources needed.;
- the availability of information and data;
- the need for modification/updating of the risk assessment, as some techniques are more amendable than others in this regard;
- any regulatory and contractual requirements.

Various factors can influence the selection of an approach to risk assessment such as the availability of resources, the nature and degree of uncertainty in the available information and the complexity of the application.

- **Risk Identification**

The aim of this step is to generate a comprehensive list of risks (i.e. the effect of uncertainty on objectives) based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. Comprehensive identification is critical, because a risk that is not identified at this stage may not be included in further analysis.

Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. Persons with appropriate knowledge should be involved in identifying risks.

There are various methodologies and tools available to assist in the identification of risks. For example, IEC/FDIS 31010 provides techniques to assist with the various risk assessment stages.

When considering risks it is often useful to consider the following:

- What can go wrong and prevent achievement of objectives (risk sources/events)?
- If something did go wrong, how bad could it be (impact)?
- What is being done or could be done to prevent things going wrong (mitigation)?

These questions should be considered in relation to the risk areas identified in Appendix 4.

In order that risks are identified, documented, recorded and compared on a consistent basis across the Synod, a set of generic categories of risk has been developed. These should be used for risk identification and recording activities.

The categories are as follows:

- Financial / Property;
- Legal;
- Operational;
- Reputation;
- Personal;
- Environmental.

The categories, and key risk areas, are more fully outlined in Appendix 4.

Note that a Synod body may identify additional risk *areas* to those outlined in Appendix 4.

- **Risk Analysis**

Risk analysis is about developing an understanding the level of risk and its nature. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated.

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is analysed by determining consequences and their likelihood, and other attributes of the risk..

The way in which consequences and likelihood are expressed, and the way in which they are combined, will determine the level of risk.

Methods used in analysing risks can be qualitative, semi-quantitative or quantitative. The degree of detail required will depend upon the particular application, the availability of reliable data and the decision-making needs.

Qualitative assessment define consequence, probability and level of risk by significance levels such as “high”, “medium” and “low”, combine consequence and probability, and evaluate the resultant level of risk against qualitative criteria.

Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship.

Quantitative analysis estimates practical values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context. Full quantitative analysis may not always be possible or desirable due to insufficient information about the activity being analysed, or because the effort of quantitative analysis is not warranted. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

For the purpose of the RMF, the RMC has decided to adopt a mainly qualitative method, which is outlined below.

Risk analysis should determine both Inherent and Residual risks. Inherent Risk is the risk which exists in an uncontrolled activity, before control measures are in place. Residual Risk is the risk remaining after risk treatment.

Following the quantification of the inherent risk, it will then be necessary to review the effectiveness of any existing controls and determine a *control rating* in order that the likelihood/consequence of an event occurring can be reassessed*,* so as to determine the *residual risk*.

The level of risk will depend on the adequacy and effectiveness of existing controls. The level of effectiveness for a particular control, or suite of related controls, may be expressed qualitatively, semi-quantitatively or quantitatively. In most cases, a high level of accuracy is not warranted. However, it may be valuable to express and record a measure of risk control effectiveness so that judgments can be made on whether effort is best expended in improving a control or providing a different risk treatment. Table 2 provides guidance for the assessment of risk control.

Table 2

CONTROL RATING	DEFINITION
Excellent	Control can be relied on to prevent risk occurring or to effectively mitigate risk in the event of the risk does occur. 90-100% effective.
Good	In most situations the control can be relied on to prevent risk occurring or to mitigate risk should it occur. 70-90% effective.
Satisfactory	Control is in place and works most of the time. 50-70% effective.
Poor	Controls are in place however are considered to be unreliable or relatively ineffective. 20-50% effective.
Unsatisfactory	Controls are totally ineffective. Risks not controlled. Less than 20% effective.

Part 1: Consequence and Likelihood Analysis

Consequence analysis determines the nature and type of impact which could occur assuming that a particular event situation or circumstance has occurred. Consequence analysis can vary from a simple description of outcomes to detailed quantitative modelling.

In relation to likelihood analysis, three general approaches are commonly employed to estimate probability; they may be used individually or jointly:

- The use of relevant historical data to identify events or situations which have occurred in the past in order to extrapolate the probability of their occurrence in the future.
- Probability forecasts using predictive techniques such as fault tree analysis (refer IEC FDIS 31010).
- Expert opinion can be used in a systematic and structured process to estimate probability.

Risks are measured against criteria for consequence and likelihood by referring to rating scales, which are detailed below. Likelihood can be scored from 1 (Rare) to 5 (almost certain) and Consequence can be rated from 1 (negligible) to 5 (catastrophic).

It is appropriate to focus on risks with potentially very large outcomes, as these are often of greatest concern to managers.

- **Likelihood Rating Scale (Table 3)**

The Likelihood Level for identified risks is documented in the appropriate likelihood column to indicate the estimated likelihood which best reflects the scenario being assessed.

Table 3

CATEGORY RATING	LIKELIHOOD TABLE [FREQUENCY PER ANNUM]
DESIGNATION	
Almost Certain	Expected likelihood to occur is greater than 99% per year
Likely	Expected likelihood to occur is between 50%-99% per year
Possible	Expected likelihood to occur is between 10%-50% per year
Unlikely	Expected likelihood to occur is between 1%-10% per year
Rare	Expected likelihood to occur is less than 1% per year

- **Consequence Rating Scale (Table 4)**

The Consequence Scale is used to allocate a consequence level for each type of consequence. Where the consequence levels for a risk span more than one type of consequence, the worst foreseeable consequence should be used.

CONSEQUENCE TABLE							Table 4
Category Rating		**Financial/ Property Loss**	**Legal Liability**	**Operational**	**Reputation**	**Personal**	**Environmental**
Score	**Designation**						
5	**Catastrophic**	>$20M **OR** > 30% of annual turnover.	Personnel jailed. Multiple third party claims. Fines: >$20M **OR** > 30% of annual turnover.	An issue that renders a critical cornerstone Synod strategy / fundamental operational objective completely unsustainable. Loss of critical systems.	Forced shut down of major church/ agency/ school or significant curtailment of operations. Decline in Church membership >25%. Stakeholders devastated.	Multiple public/ member/ client / employee fatalities. Pandemic: Sustained transmission in general population.	Large scale irreversible environmental harm.
4	**Major**	$10 to $20M **OR** 20% - 30% of annual turnover.	Personnel fined. Multiple third party claims. Fines: $10M-$20M **OR** 20% - 30% of annual turnover.	An issue that seriously threatens the sustainability of a critical cornerstone Synod strategy / fundamental operational objective. Loss of non-critical systems or data availability.	Extended national/ international adverse media campaign. Parliamentary inquiry. Decline in Church membership 10-25%. Stakeholders' reaction causing significant disruption.	Single public / member/ client / employee fatality. Pandemic: Large cluster(s) but human-to-human spread localised.	Major release of pollutants. Significant, long term environmental harm. Release of pollutants to an extremely sensitive area.
3	**Moderate**	$1 to $10M **OR** 10% - 20% of annual turnover.	Third party claims. Fines: $1-$10M **OR** 10% - 20% of annual turnover.	An issue that will have an undesirable, but not excessive, effect on a critical cornerstone Synod strategy / fundamental operational objective. Loss of key personnel.	Adverse State media coverage. Decline in Church membership 5-10%. Stakeholders' reaction causing disruption.	Serious injury, hospitalisation to members/ clients/ public/ employee. Pandemic: Small cluster(s) with limited localised human-to-human transmission	Release of pollutants to sensitive areas. Immediate offsite contamination which is beyond the normal combatant resources available at site.
2	**Minor**	$100K to $1M **OR** 5% -10% of annual turnover.	Third party claims. Fines: $100K-$1M **OR** 5% - 10% of annual turnover.	An issue that will have a small/unimportant effect on a critical cornerstone Synod strategy / fundamental operational objective. Loss of personal property.	Local media coverage. Public (telephone) complaints. Decline in Church membership <5%. Stakeholders' reaction simply managed.	Medical (doctor treatment) to members / clients/ public/ employee. Human infection(s) with a new virus subtype, but no human-to-human spread.	Contamination of UCA property that does not constitute a threat to the environment.
1	**Negligible**	<$100K **OR** < 5% of annual turnover.	Third party claims. Fines: <$100K **OR** < 5% of annual turnover.	An issue that will not have any effect on a critical cornerstone Synod strategy / fundamental operational objective.	Public normally unaware. No impact Church membership. No stakeholder reaction.	Illness or injury, First Aid treatment only or no treatment No new virus has been detected in humans.	Contamination occurs within the confines of protected areas and can be managed through normal operations.

Part 2: Risk Ratings

By plotting the consequence and likelihood ratings utilising the Risk Rating Matrix (Table 5), the level of Inherent risk (and subsequently Residual risk) can be allocated to a risk. As such**,** the consequence/probability matrix is a means of combining qualitative or semi-quantitative ratings of consequence and probability to produce a risk rating.

The matrix is commonly used as a screening tool when many risks have been identified, e.g. to define which risks need more detailed analysis, which risks need treatment first, or which need to be referred to a higher level of management. It may also be used to select which risks need not be considered further at this time. This risk matrix is also widely used to determine if a given risk is broadly acceptable, or not acceptable according to the zone where it is located on the matrix.

Within the Synod, matrix is also used to help communicate a common understanding for qualitative levels of risks across the Synod. The way risk levels are set and decision rules assigned to them are aligned with the Synod's risk appetite.

Use of the tool needs people (ideally a team) with relevant expertise and such data as is available to help in judgements of consequence and probability.

To rank risks, the user first finds the consequence descriptor that best fits the situation then defines the probability with which those consequences will occur. The level of risk is then read off from the matrix.

Many risk events may have a range of outcomes with different associated probability. Usually, minor problems are more common than catastrophes. There is therefore a choice as to whether to rank the most common outcome or the most serious or some other combination. In many cases, it is appropriate to focus on the most serious credible outcomes as these pose the largest threat and are often of most concern. In some cases, it may be appropriate to rank both common problems and unlikely catastrophes as separate risks. It is important that the probability relevant to the selected consequence is used and not the probability of the event as a whole.

Table 5: Risk Rating Matrix

CONSEQUENCE / LIKELIHOOD	NEGLIGIBLE "1"	MINOR "2"	MODERATE "3"	MAJOR "4"	CATASTROPHIC "5"
ALMOST CERTAIN (5)	6	7	8	9	10
LIKELY (4)	5	6	7	8	9
POSSIBLE (3)	4	5	6	7	8
UNLIKELY (2)	3	4	5	6	7
RARE (1)	2	3	4	5	6

Table 6: Risk Significance Table:

RISK SIGNIFICANCE TABLE	
RISK SIGNIFICANCE	**RISK REDUCTION REQUIREMENTS**
LOW	Acceptable risk – Review consequences and likelihood and manage through routine procedures.
MODERATE	Ensure management system controls risk and managerial responsibility is defined.
HIGH	Ensure system and technical controls are such that the risk is as low as reasonably practicable and due diligence systems are in place and assurance can be demonstrated.
EXTREME	Risk must be reduced as soon as possible. If it can not be reduced it must be agreed with the most senior officer/manager (e.g. Parish Minister, CEO, Principal etc) that due diligence systems are in place and assurance can be demonstrated. For any new extreme risks, the Synod Executive Director Administration & Finance (EDAF) must be immediately and formally advised once such risks have been identified. This advice must occur by the completion of the Extreme Risk Proforma (see below). As appropriate, the EDAF will then advise the General Secretary (Victorian and Tasmanian Synod) and the RMC.

Part 3: Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

Risk evaluation involves comparing the level of risk found during the analysis process with risk significance criteria (low, moderate, high, or extreme). Based on this comparison, the need for treatment, as well as priority, can be considered.

Table 6 indicates the significance of a risk, which will assist in the evaluation, prioritisation and deciding what actions which should be undertaken.

While the final decision on whether or not to treat a risk will be based on individual judgement, the factors detailed below should be considered in order to prioritise the risks that require further treatment. Factors to be considered include:

- The risk rating and the potential impact of the risk event occurring;
- The effectiveness of existing controls;
- The risk criteria;
- Previous risk management performance;
- Risk appetite;
- Legal and regulatory requirements;
- Whether an activity should be undertaken;
- Cost / benefit of upgrading controls.

In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way

other than maintaining existing controls. This decision will be influenced by the attitude to risk and the risk criteria that has been established.

Step 3: Risk Treatment

Following the evaluation, risk treatment involves a cyclical process of:

- assessing a risk treatment;
- deciding whether residual risk levels are tolerable;
- if not tolerable, generating a new risk treatment;
- assessing the effectiveness of that treatment.

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk (as the impact of the risk is so great, and/or the options to treat the risk are minimal or extremely costly);
- taking or increasing the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing);
- retaining the risk by informed decision.

Note that where mitigation is not possible or is impractical/uneconomic and the risk is *retained* it is critical that appropriate communication occurs so that that all stakeholders are aware of, and understand, the implications of this approach. It will also be essential to continually monitor such risks.

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment.

- ***Risk Treatment Plans***

Risk treatment plans should be developed after Identifying, assessing and selecting *option(s)* for controlling the risk. The purpose of risk treatment plans is to document how the chosen treatment options will be implemented. A prioritised risk treatment and implementation plan must be prepared for the identified risks that are deemed to be unacceptable.

The proposed actions should be:

- achievable;
- specific, clearly indicating the actions to be taken and those responsible;
- incorporate managerial and technical controls,
- clearly allocate responsibilities;
- measurable, including actions and timelines;
- cost effective and identify what resources will be used;

- integrated within management processes and discussed with appropriate stakeholders.

The information provided in treatment plans should include:

- the reasons for selection of treatment options, including expected benefits to be gained;
- those who are accountable for approving the plan and those responsible for implementing the plan;
- proposed actions;
- resource requirements including contingencies;
- performance measures and constraints;
- reporting and monitoring requirements;
- timing and schedule.

The risk treatment plan should take into consideration the effect on consequence, likelihood and the resource requirements estimated to achieve the mitigation. Controls should be commensurate with the risk associated with an activity.

The risk reduction requirements, particularly for "extreme" and "high" risks, should facilitate better appreciation of risk and changes in risk profile as well as enhanced monitoring of improvement programs.

Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective.

The plan must ensure that risks are monitored, including high level reviews (by the Board, RMC or Senior Management).

A risk treatment plan may incorporate the following processes:

- ***Risk control***

  Risk control involves the development of mitigation and contingency plans.

  The mitigation plan is a strategy or course of action that is taken prior to a particular risk materialising. The plan aims to reduce the probability or consequences of the risk occurring to a level that is as low as reasonably possible.

  Mitigation plans contrast with contingency plans (e.g. Business Continuity Plan), which is a course of action to be taken in the event of a particular risk materialising. The contingency plan will allow quick action to be taken to minimise the impact, but does nothing to counter the probability of the risk occurring.

  Moreover, these plans will incorporate the implementation of policies, standards, procedures, appropriate techniques and management principles, or physical changes to eliminate or minimise adverse risks.

- ***Risk transfer***

  Risk transfer occurs by shifting the responsibility, or burden for loss, to another party through contract, insurance or other means. Risk transfer can also include shifting a physical risk or part thereof elsewhere.

  More specifically, actions may include:

- Risk sharing;
- Activity controls;
- Physical controls;
- Systems of approvals and authorisations;
- Verifications and reconciliations;
- Segregation of duties.

Step 4: Monitoring and Reviewing Risks

As it is essential to ensure that the mitigation strategies are effective and remain relevant, risks and treatment measures need to be monitored to ensure that changing circumstances do not alter priorities.

As part of the monitoring process, regular reviews of the management of risks must be undertaken by senior management and appropriate governing bodies (including the RMC) on a regular basis. Risks with a rating of 7 and above (See Table 5) should be reported on a monthly basis and all identified risks at least on a quarterly basis.

Such reviews are critical so as to ensure that:

- control measures (pre-existing and new) have been implemented and are operating as planned, that is, are risk management outcomes in line with performance indicators;
- periodical review of performance indicators or appropriateness;
- that any changes in the risk, or the dynamic internal or external environment within which the Synod body operates, are adequately reflected in the control measures;
- that the exposure to the assessed risks been eliminated or adequately reduced;
- analysing and learning lessons from events (including near-misses), changes, trends, successes and failures occurs;
- emerging risks are identified;
- if the control measures have created new problems, that appropriate actions have been taken to address these new issues;
- periodical review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;
- report on risk, progress with the risk management plan and how well the risk management policy is being followed;

Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.

A key tool, which assists with the above review and record creation, is a risk register - refer to Appendix 5 for an example of a risk register. Note that the WSP system generates its own system based risk register.

APPENDIX 4

MAIN RISK CATEGORIES

For categorisation purposes within the RMF, risks have been grouped into generic risk categories as follows:

1. **Financial / Property Risks**

These risks arise out of financial and property ownership functions.

Financial risks may arise from a future event, which may accrue either from incurring a cost or by failing to attain some benefit. Such risks will impair a body's capacity to provide a desired financial outcome and may ultimately result in a body being unable to meet its financial obligations.

Property risks arise as such possessions can be destroyed or stolen. Property risks embrace two distinct types of loss, the potential loss of the property, and the potential loss of use of the property resulting in lost income or additional expenses.

Risk areas falling under this include:

- Asset management;
- Audit programs;
- Budgets;
- Buildings;
- Business planning;
- Capital expenditure;
- Cashflows;
- Credit risk management;
- Delegations;
- Economic developments;
- Equipment management;
- Fleet management;
- Fraud;
- Funding;
- Investments;
- Liquidity;
- Maintenance;
- Procurement;
- Property damage;
- Security;
- Solvency;
- Taxation.

2. **Legal Risks**

Legal risk is the risk of loss resulting from failure to comply with laws as well as prudent ethical standards and contractual obligations. It also includes the exposure to litigation from all aspects of a body's activities.

Compliance risks arise as a consequence of the many Legislative Acts, Codes, Standards and regulations that the entire Synod is subject to. Additionally, governments may change the laws in ways that adversely impacts a body.

Risk areas falling under this include:

- Advisory;
- Contractual arrangements;
- Employment;
- Environment;
- Harassment;
- Legislative changes;
- Legislative compliance;
- Molestation;
- Occupational Health and Safety;
- Privacy.

3. **Operational Risks**

The risk of loss from operational risks usually results from inadequate or failed internal processes, people and systems or from external events. Operational risks arise as a consequence of the various functional activities which a body undertakes.

Risk areas falling under this include:

- Business continuity;
- Change management;
- Client management;
- Communication;
- Competition;
- Complaints from neighbours, action groups and employees;
- Confidentiality;
- Contractors;
- Disaster recovery;
- Data management;
- Documentation;
- Governance;
- Government;
- Human resources;
- Incident management;
- Inappropriate behaviour;
- Leadership;
- Operational compliance;
- Organisational behaviour;
- Outsourcing;
- Performance management;
- Policies and procedures;
- Project management;
- Records management;
- Risk management processes and culture;
- Strategy;
- Systems;
- Training;
- Technology;
- Telecommunications;
- Volunteers.

4. **Reputation Risks**

These risks arise as a consequence of undertaking various activities, many of which can impact reputation.

Reputation damage generally arises due to the failure to manage other risks properly. Inappropriate treatment or resolution of reputation issues can further exacerbate the reputation risk.

Risk areas falling under this include:

- Communication;
- Community expectations;
- Complaints;
- Dispute resolution;
- Policies;
- Public relations.

5. **Personal Risks**

Personal risks are those threats that may be directed towards a body's employees or volunteers. These risks often arise out of personnel functions and may originate from either internal or external sources.

Risk areas falling under this include:

- Aggressive clients;
- Career development;
- Discrimination;
- Ergonomics;
- Fire safety;
- Health matters;
- Human resources policies;
- Industrial relations;
- OH&S, work practices;
- Performance management;
- Personal injury;
- Remuneration;
- Skills and knowledge;
- Stress;
- Succession planning;
- Supervision;
- Workforce behaviour.

6. **Environmental Risks**

Environmental risk is the chance that human health or the environment will suffer harm as the result of the presence of environmental hazards. These risks arise out of interaction with the environment .

Risk areas falling under this include any actions/inactions that adversely impact the environment.

Risk areas falling under this include:

- Compliance with environmental legislative requirements;
- Contaminated sites from previous activities or acquisitions;
- Discharges to soil;
- Discharges to water bodies, including stormwater run-off;
- Emissions to atmosphere;
- Energy and resource usage;
- Environmental performance ;
- Nuisance emissions, including noise;
- Waste disposal arrangements (reduction, reuse, recycling and disposal).

APPENDIX 5

SAMPLE RISK REGISTER – ABC SYNOD BODY								REVIEW DATE:	
RISK CATEGORY: FINANCIAL / PROPERTY RISKS								/ /	
		Potential Effects		Measurement of Inherent Risk					
Risk Event	Causes	Financial Impact	Other Impacts	Likelihood of Event Happening [Score 1-5]	Consequence of Event Happening [Score 1-5]	Risk Assessment [Low , Moderate, High or Extreme]	Existing Controls / Control Rating [Excellent, Good, Satisfactory, Poor, Unsatisfactory]	Residual Risk Assessment # [Low , Moderate, High or Extreme]	Risk Priority / Timeline
							Control: Rating: Responsibility:		
							Control: Rating: Responsibility:		

Risk assessment after additional treatment options implemented.

I am aware of the above mentioned risks and confirm that the controls and mitigating actions referred to above have now been implemented.

PRINT NAME: _____ **POSITION / TITLE :** **Chief Executive Officer**

SIGNATURE: _____ **DATE:** _____

EXTREME RISK REPORT

NEW RISK #:	**SYNOD BODY:**	**DATE :** [Risk identified]	**IMPACT :** [Church Wide or Localised]	**INHERENT RISK RATING :** [7, 8, 9, or 10 ONLY]

RISK EVENT DESCRIPTION:

FINANCIAL/PROPERTY IMPACT : **YES** ___ **[** Provide details**]** **NO** ___

LEGAL IMPACT: **YES** ___ **[** Provide details**]** **NO** ___

OPERATIONAL IMPACT: **YES** ___ **[** Provide details**]** **NO** ___

REPUTATION IMPACT: **YES** ___ **[** Provide details**]** **NO** ___

PERSONAL IMPACT : **YES** ___ **[** Provide details**]** **NO** ___

ENVIRONMENTAL IMPACT: **YES** ___ **[** Provide details**]** **NO** ___

LIKELIHOOD OF OCCURRENCE [INHERENT]:				**CONSEQUENCE OF RISK [INHERENT]:**			
ALMOST CERTAIN	___	**LIKELY**	___	**CATASTROPHIC**	___	**MAJOR**	___
POSSIBLE	___	**UNLIKELY**	___	**MODERATE**	___	**MINOR**	___
RARE	___			**NEGLIGIBLE**	___		

CONTROLS **Existing Controls:**	**CONTROLS** **Recommended Additional Controls:**

MITIGATION STRATEGY:

RETAIN ___ **CONTROL** ___ **TRANSFER** ___ **AVOID** ___

[Document the risk mitigation strategy and plans that will be implemented to ensure the risk is managed by using one of the above methodologies].

LIKELIHOOD OF OCCURRENCE [RESIDUAL]:				**CONSEQUENCE OF RISK [RESIDUAL]:**			
ALMOST CERTAIN	___	**LIKELY**	___	**CATASTROPHIC**	___	**MAJOR**	___
POSSIBLE	___	**UNLIKELY**	___	**MODERATE**	___	**MINOR**	___
RARE	___			**NEGLIGIBLE**	___		

PRINT NAME: _____ **POSITION / TITLE:** _____

SIGNATURE: _____ **DATE:** _____

APPENDIX 7

DEFINITIONS

TERM	DEFINITION
Consequence	The outcome of an event affecting objectives, expressed qualitatively or quantitatively,. There may be a range of possible outcomes associated with an event.
Context	**External Context** [External environment in which a body seeks to achieve its objectives]. External context can include: • the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; • key drivers and trends having impact on the objectives of the body ; and • relationships with, and perceptions and values of, external stakeholders. **Internal Context** [Internal environment in which the organisation seeks to achieve its objectives]. Internal context can include: • governance, organisational structure, roles and accountabilities; • policies, objectives, and the strategies that are in place to achieve them; • the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); • perceptions and values of internal stakeholders; • information systems, information flows and decision-making processes (both formal and informal); • relationships with, and perceptions and values of, internal stakeholders; • the organisation's culture; standards, guidelines and models adopted by the organisation; • form and extent of contractual relationships.
Event	Occurrence or change of a particular set of circumstances. An event can be one or more occurrences, and can have several causes or consist of something not happening.
ISO/FDIS 31000: 2009 Risk management - Principles and guidelines	ISO (International Organisation for Standardisation) is a worldwide federation of national standards bodies. The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organisations, governmental and non-governmental, in liaison with ISO, also take part in the work. International Standards are drafted in accordance with the rules given in the ISO Directives. The technical committees prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote. ISO/FDIS 31000 was prepared by the ISO Technical Management Board Working Group on risk management.

TERM	DEFINITION
Key Synod Body	An initial list of those Key Synod Bodies the Synod Risk Management Committee requires to comply with the Risk Management Policy Framework. Refer Appendix 8.
Likelihood	The chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected Monitoring can be applied to a risk management framework, risk management process, risk or control.
Residual Risk	Risk remaining after risk treatment.
Review	An activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. Review can be applied to a risk management framework, risk management process, risk or control.
Risk	Risk: Risk is the effect of uncertainty on objectives. It is the exposure to the possibility of economic loss or gain; any kind of injury, damage or benefit, resulting from a course of action. Inherent Risk: The risk which exists in an uncontrolled activity, i.e. before control measures are in place. Residual Risk: The risk remaining after risk treatment. Acceptable Risk: A real risk imposed by a specific hazard but one that under considered circumstances would not deter the Key Synod Bodies from accepting the likelihood and consequence of that particular risk.
Risk Analysis	The process to comprehend the nature of risk and to determine the level of risk.
Risk Appetite	The amount and type of risk that a body is prepared to pursue, retain, take.
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Attitude	A body's approach to assess and eventually pursue, retain, take or turn away from risk
Risk Control	The measure that is modifying risk. Controls include any process, policy, device, practice, or other actions which modify risk..
Risk Criteria	Terms of reference against which the significance of a risk is evaluated.

TERM	DEFINITION
Risk Evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.
Risk Level	The magnitude of a risk expressed in terms of the combination of consequences and their likelihood.
Risk Management	Risk management refers to the coordinated activities that direct and control a body with regard to risk. It includes the architecture (principles, framework and process) for managing risks effectively and the application of that architecture to particular risks.
Risk Management Framework	The set of components that provide the foundations (policy, objectives, mandate and commitment to manage risk) and organisational arrangements (plans, relationships, accountabilities, resources, processes and activities.) for designing, implementing, monitoring, reviewing and continually improving risk management throughout a body. The risk management framework is embedded within the body's overall strategic and operational policies and practices.
Risk Management Policy	The statement of the overall intentions and direction of a body related to risk management.
Risk Management Process	The systematic application of management policies, procedures and practices to the activities of communicating, consulting, identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Risk Owner	The person or body with the accountability and authority to manage risk.
Risk Treatment	The process to modify risk.
Stakeholders	Person or body that can affect, be affected by, or perceive themselves to be, affected by a decision or activity.
Synod Body	A group of people with an arrangement of responsibilities, authorities and relationships within the Synod of Victoria and Tasmania. These groups will vary in composition from, for example a department through to a complete operation such as a large agency.
Uncertainty	Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

APPENDIX 8

KEY SYNOD BODIES
[As defined in Appendix 7]

CATEGORY	KEY SYNOD BODIES
VARIOUS OPERATIONS:	Synod Head Office Operations
	Funds Management
	Commission for Mission
	Centre for Theology and Ministry
	Wesley Precinct Development
UNITING AGED CARE:	Uniting Aged Care Board
UNITINGCARE AGENCIES:	Wesley Mission Melbourne
	UnitingCare Harrison Community Services
	UnitingCare Community Options
	Connections
SCHOOLS / COLLEGES:	Kingswood College
	Methodist Ladies' College
	Acacia College Development Project
PRESBYTERIES [including Congregations]:	North East Victoria
	Loddon Mallee
	Gippsland
	Port Phillip East
	Port Phillip West
	Western Victoria
	Tasmania
	Yarra Yarra

APPENDIX 9

OVERVIEW OF WSP ONLINE RISK MANAGEMENT SYSTEM

THE COMPANY: **WSP Risk Solutions**

WSP is a global management consulting company focusing on strategic risk management with a particular focus on strategic and operational enterprise risk, health and safety, business management and management systems. Through this work, WSP has developed the WSP core standards and associated methodology to assist organisations such as the Synod of Victoria and Tasmania in understanding their risk exposures and develop strategies to address these.

WSP consultants have a breadth of experience and are focused on delivering practical business solutions for the challenges that organisations face. WSP has a training philosophy in which it is critical that people within the organisation learn skills from the consulting process which can be applied within the organisation an ongoing basis.

WSP has been selected by the Synod Risk Management Committee to assist in the progressive implementation of a risk management system across the Synod, including the development of risk registers, and to initially provide associated risk management training workshops.

SYSTEM OVERVIEW

The Online Risk Register product is offered as an off-the-shelf package, with the features below, pre-configured for UCA.

The product is developed in a powerful, extensible software architecture that supports the customisations required to meet UCA's needs.

The system is designed to assist in the effective management of risks and a key outcome of the system is the generation of a risk register.

Risk Details Recorded

Details to be recorded for each individual risk are:

- Risk Number (automatically generated).
- Risk Standards (a list of categories as defined by UCA).
- Central office and/or entities.
- Risk Description (free text block).
- Current Controls (free text block).
- Current Risk Rating (automatically calculated based on user-selected Likelihood and Consequence ratings. This is based on UCA's rating calculation matrix.
- Mitigation Action (free text block).
- Status (Pending, In Progress or Completed).
- Responsible Person (a single individual who is accountable for the risk. Must be one of the Managers or Team Leaders registered to use the system - see below).

- Due Date (date when all Mitigation Actions must be completed by. Responsible Person will be emailed when a Pending or In-Progress item passes its due date).

- Comments and file attachments (user can update risk by adding unlimited number date/time logged).

Users and Access Levels

Two levels of user access levels are provided in the base product:

- Managers. These users will have full edit/report access to all risks assigned to any department.

- Team Leaders. These users will have full edit/report access to all risks assigned to their department, and cannot access risks in other departments.

Further access levels (e.g. a read-only role with global access for reporting to external audit teams) can be provided, if required.

An additional role for Administration of users (account creation and modification) and organisational structure (adjustment of departmental hierarchy, addition of sub-departments) will be provided to one nominated UCA (Synod) user. After initial setup has been provided by WSP, this role will be responsible for creation and management of new user accounts.

Users, Organisation Structure and Departments

The whole of organisation structure can be supported in the off-the-shelf product. WSP will assist in the initial setup of the organisational structure and user management.

Initial setup covers creation of Synod departments and top-level Agency departments in the product's organisational structure.

Audit Log Tracking

When a user edits a Risk Record all changes will be tracked in an audit log, which is visible to all users who can access the risk. This includes:

- **Status** (records who changed status, and what it was changed to).

- **Current Risk Rating** (records who changed Likelihood and Consequence, and what rating was before and after change).

- **Document attachments** (document attachments in any format (up to 5 MB per file) can be attached to a risk for reference. As part of the audit log, these cannot be deleted, but newer versions can be attached as needed.

Escalation and Email Interaction

When a risk reaches its due date (or another predetermined period) an email can be automatically sent to the user assigned to the risk as its Responsible Person. WSP recommend a proactive approach to managing risks a user is directly responsible for, to avoid Inbox email inundation. Thus it is recommend that users use the report filters to review upcoming due dates.

Reporting

Users will be able to produce on-screen reports, based on risks they have access to.

Reports can be produced based on the following filter criteria:

- **Risk Standard/Category** (select which Risk Standard to view risks from)
- **Department** (show risks in a department as selected by user. Multiple departments can be reported on at the one time, as access rights for user allow).
- **Risk Rating** (report on one of Low/Moderate/High/Extreme risks)
- **Status** (report on one of overdue/in-progress/pending/completed risks)

In addition to producing a report listing all risks in the criteria selected by the user, a dashboard of graphical charts will summarise results of the reports.

Export

A spreadsheet of all risks, that a user has access to, will be available for download in Excel format. This will allow further manipulation and reporting of data entered into the system, and facilitates export of data for use in other systems. This spreadsheet includes all risk data including comments but excludes file attachments.

A printable version of risk register (either all risks, or as filtered for reporting) is also available. This can be sent to a printer, or if Adobe Acrobat Writer (or equivalent) is available on the user's PC then a PDF document can be created for offline reference and backup.

Import

Should UCA units have existing risks in an accessible format (e.g. Excel export) then WSP may be able to assist in importing these into the online tool. WSP is happy to discuss and quote as required.

Software and Hosting

The Risk Register will be accessible online in a web browser. An Internet connection and web browser versions of at least Microsoft Internet Explorer 6 or Firefox 2 will be required for user access. Data transferred to the service will be secured by SSL 128 encryption. The service is hosted in a secure, backed-up web-server managed by WSP. The intellectual property of the software service remains the property of WSP, while all data entered into the system is owned by UCA and available for download by registered users.

All applications hosted by WSP Online Solutions are housed in a fully redundant infrastructure provided by Rackspace (www.rackspace.com) in a secure data centre in the USA. A secondary backup server is housed in the NetRegistry (www.netregistry.com.au) data centre in Sydney, Australia. In the event of a failure at the primary host in the USA, all services will be switched to the backup server in Australia – resulting in minimal disruption to clients.

Backup includes instant database and file replication to secondary server and daily, weekly, monthly database backups for server disaster recovery.

Product Customisations for UCA

The following changes will be provided with the initial system:

- **Residual Risk:** Risk Details page updated to track Residual Risk, by calculating Rating from Residual Risk Likelihood and Consequence values entered by user in same format (and with same matrix for calculations) as current rating is tracked**.**

- **UCA Risk Categories:** Current “Risk Standards” renamed to “Risk Categories” and the list replaced with UCA’s own top-level risk categories**.**

- **UCA Sub-categories:** Addition of a description text block to each top level Risk Category, allowing user to view description of any category (including a list of its subcategories) to aid in selection of a Risk Category. Risks will still only be linked to a top-level Risk Category.

- **UCA Likelihoods, Consequences and Matrices:** Existing versions of the products list of Likelihoods/Consequence ratings and descriptors revised to suit UCA’s Risk Management Framework. The Matrix used to calculate Risk Rating customised to match the UCA Framework (Risk Rating tracked will be one Low/Moderate/High/Extreme).

- **Customised Reporting:**

  - Dashboard and its Filters will be updated to report on Residual Risk in addition to current reporting of Risk Rating.

  - Suitable reporting for Synod/Agency management and Standing Committee. This will allow reporting on the top risks (i.e. manually selected *Extreme/High* rated risks) for each department.

Availability of WSP System

The WSP system is available to those UCA bodies which require a sophisticated system to assist in the management, monitoring and reporting of risks.

In the first instance, contact should be made with either the Synod Project Manager, Risk Management System or the Executive Director Administration and Finance, 130 Little Collins St, Melbourne.

Risk Assessment Techniques

Information relating to Risk Management – Principles and Guidelines can be located on the International Organisation for Standardization website: www.iso.org

APPENDIX 11

REFERENCES

PUBLICATIONS:

ISO/FDIS 31000:2009 Risk management - Principles and guidelines

IEC/FDIS 31010 Risk management - Risk Assessment Techniques