

## Risk Management Policy

<b>Contact Name and Details</b>	Mrs Louise C Wilkins, Conference Officer for Legal and Constitutional Practice
<b>Resolutions</b>	72/1. The Council adopts the Risk Management Policy set out in the report.

1. The Council is required to review annually its risk management policy in order to ensure that the policy reflects its risk appetite and correctly identifies those areas of risks that the Council would consider to have the most significant impact on its ability to fulfil *Our Calling*.
2. The policy is current for both the corporate risk register and the Connexional Team register. The corporate risk register identifies the fundamental risks to the Methodist Church (and in particular those aspects of connexional life for which the Council and the Conference has particular oversight), and the Connexional Team risk register identifies the risks that might impede the ability of the Team to resource the wider Connexion.
3. The policy has been updated to ensure that the policy reflects the Methodist Council objectives and the relationship between the risk registers and those objectives. It has been significantly amended in order to seek to clarify the purpose of the policy, where responsibilities for risk management lies and process, how risks are identified, escalated and controlled.
4. The amended policy is presented to the Council for its adoption.

### \*\*\*RESOLUTION

**72/1. The Council adopts the Risk Management Policy set out in the report.**

Version: 1.4  
Updated: 24.09.2019  
Date of last Council review: January 2019  
Date for next Council review: October 2019

## Risk Management Policy

### Contents

1. Introduction
2. Purpose
3. Policy Statement
4. Risk Appetite
5. Responsibilities
6. Risk Management Procedure
  - 6.1. Important Risk Management Concepts
  - 6.2. Identifying Risks
  - 6.3. Assessing Risks
  - 6.4. Prioritising Risks
  - 6.5. Risk Control
7. Risk Registers
8. Monitoring and Reporting
9. Escalating Risks
10. Audit and Review

### 1. Introduction

- 1.1. This Policy provides the framework for the management of strategic, corporate and operational risk in the performance of the Methodist Church's activities to meet the requirements of good corporate governance, to protect the interests of the Church's stakeholders and to deliver the calling of the Church to respond to the gospel of God's love in Christ and to live out its discipleship in worship and mission. It is the responsibility of Council members, Committee members, Senior Managers and the Connexional Team to ensure that risks are understood and appropriately managed in accordance with this policy. At all levels of the organisation, risk management, reporting and auditing processes will reflect the requirements set out in this policy.
- 1.2. *Risk* is the exposure to danger, harm or loss and, in the context of running an organisation, issues or events that may prevent the achievement of the aims or goals of one or more key strategic or operational business areas or projects. *Risk management* is the systematic process of identifying and mitigating possible risks, problems or disasters before they occur to protect the Church's resources, income, reputation and to help deliver its core aims.
- 1.3. This policy sets the framework which allows the Connexional Team to maintain appropriate procedures to identify and analyse risk before assessing whether such risks should be avoided, minimised or accepted with actions to minimise negative impact.
- 1.4. Effective risk management is fundamental to maintaining and developing the mission of the Methodist Church in line with *Our Calling* and ensuring the Methodist Council is provided with a means to control risk within its strategic planning and priorities. The Methodist Council is the key governance body for overseeing risk management for the activities of the Connexional Team and is delegated responsibility by the Conference for overseeing the corporate risk register.

## **2. Purpose**

2.1 The purpose of this policy is to define the standards and procedures applicable to all relevant bodies, committees and Connexional Team members for the effective management of operational and corporate risks. This is achieved by:

- setting out respective responsibilities for operational and corporate risk management for the Connexional Team, the Senior Management Team, the Sub-Committees (SRC and Audit Committee) and the Methodist Council;
- explaining the methods used to assess, monitor and mitigate both operational and corporate risks effectively;
- delivering a clear policy framework to deliver the Church's Risk Management Strategy.

2.2 The Council is committed to implementing appropriate strategies and processes that identify, analyse and manage the risks associated with our activities as a means of minimising the impact of undesired and unexpected events on our activities. It will therefore:

- identify objectives that reflect the interests of all stakeholders and the delivery of *Our Calling*;
- identify the threats to the achievement of those objectives;
- identify all over risks posed to the Church's activities;
- determine the Council's appetite for and tolerance of risk;
- assign accountability to sub-committees and members of the Connexional Team for various parts of the risk management process;
- control and manage exposure to risk by appropriate risk reduction and mitigation actions
- regularly review the exposure to all forms of risk and reduce it as far as reasonably practicable or achievable
- apply robust risk management processes as part of a wider management system
- educate and train staff in risk management
- regularly review the risks that are faced as a result of its business activities and of the business and economic climate in which the Church operates
- identify cost effective risk treatment options
- regularly review key risk controls to ensure that they remain relevant, robust and effective

2.3 The Council will demonstrate achievement of the individual components of this Policy through the preparation of documented procedures, the reporting and review of risk at all levels and a monitoring and audit programme to ensure that the processes are being implemented.

2.4 The Council shall encourage self-accounting entities that report to it or to the Conference and those that form part of the Church's consolidated accounts to refer to this policy as part of their approach to forming effective risk management frameworks and protocols. The Council shall utilise this policy when assessing the risks posed within self-accounting entities.

## **3 Policy Statement**

3.1 The Council is committed to ensuring the delivery of *Our Calling* whilst protecting its reputation and interests of our stakeholders including members and staff and will do this by actively managing the uncertainties of operational and corporate risks through the implementation of a clear and robust risk management framework. The Council will seek to adopt best practice in risk management, employ new technologies to help manage risk and ensure the Connexional Team staff are appropriately trained to manage the risk associated with its activities.

3.2 The Council acknowledges that it is not possible or desirable to eliminate all risks and will encourage positive risk-taking in keeping with its statement of risk appetite (below) where risks

may result in positive benefits for delivery of *Our Calling* and the protection of all individuals who have a role, responsibility or interest in the life of the Church.

3.3 To this end risk management will form an integral part of the Council's decision-making process and part of the day to day decision making of the Connexional Team. The Council and senior management meeting shall ensure that this policy is referred to regularly as part of all decision-making processes. In particular, this policy shall be considered by the Council and senior management:

- before entering into any long-term planning, whether of a strategic or operational nature.
- whenever the Council is considering new activities of the Connexional Team or the adoption of new policies.

## **4 Risk Appetite**

4.1 *Risk Appetite* is the amount of risk that the Council is willing to accept. The Council shall, through delegation to the Strategy and Resources Committee and senior management, minimise the likelihood of a risk occurring and its impact whenever possible but shall not take steps that impede the ability of the Connexional Team to resource the Church in furthering its mission.

4.2 The Council recognises that taking risks is vital when seeking to communicate the Gospel, and that the Methodist Church was founded because of risks taken by John Wesley. The Council therefore embraces any risk which seeks to advance the objectives of the Methodist Church whilst ensuring that the Council is a good steward of church resources and seeks to avoid or minimise any actions that would have a negative impact on reputation or personnel.

4.3 The Council accepts that in seeking to fulfil *Our Calling*, the Council must take risks to ensure the Church increases the awareness of God's presence and to celebrate God's love; to help people to grow and learn as Christians, through mutual support and care; to be a good neighbour to people in need and to challenge injustice, and to make more followers of Jesus Christ. The Council will always seek to mitigate risks but is prepared to accept those risks that come from reaffirming *Our Calling*. The Council however notes that it has zero risk appetite for anything that might compromise the safety of individuals in terms of safeguarding and/or injury or result in breaches of regulation or legislation.

4.4 Prior to any risk being accepted, full consideration must be given as to the likelihood of the risk occurring and the impact on the Church or the Connexional Team if the risk were to occur. Any risk that seriously threatens the ability of the Methodist Church now or in the future to communicate the Gospel will not be acceptable.

## **5 Responsibilities for Risk Management -**

Members of the Council and Senior Management of the Connexional Team shall be provided with appropriate training on risk management and be clear on their role and responsibilities in implementing the risk management policy.

### **5.1 The Council shall:**

- approve and annually review the risk management policy
- set the risk appetite and tolerance and outline this in its risk management policy
- ensure risk management is embedded in the day to day working of the Connexional Team
- consider the impact of any new strategy or policy on the risk register and seek to mitigate such risks occurring through the decision making process;
- receive regular reports from the Audit Committee as to how risks are being actively managed and whether appropriate controls in place and working effectively

- make decisions that reflect its appetite for risk
- ensure that senior management of the team are clear who the risk owners in respect of the risk register and shall hold such risk owners to account for their action to mitigate the identified risk
- annually review the corporate risk register unless significant new risks arise during the course of the year, in which case the Council shall receive an updated corporate risk register

**5.2 The Strategy and Resources Committee shall:**

- annually review the Risk Register for the Connexional Team
- receive from the senior management a report on any serious risks that arise or that have a heightened impact or likelihood during the course of the year
- receive a regular report from the Conference Officer for Legal and Constitutional Practice on any serious incident report made to the Charity Commission or another external regulator during the course of the year that affects the Methodist Church in Great Britain.

**5.3 The Audit Committee shall:**

- report to the Council on internal controls and shall alert the Council to any emerging issues
- oversee internal audit and external audit and report to the Council its monitoring of risks identified by the internal or external audit process
- advise the Council on the effectiveness of the internal control system, including the Team's system for the management of risk.
- receive the risk management policy at its meeting in May and receive updates to the Connexional Team and Corporate Risk Registers in May, October and December.

**5.4 The Senior Management Group shall:**

- ensure the Connexional Team receives risk management training
- lead the embedding of risk management throughout the Connexional Team and encourage forward planning to assess potential future risks
- administer and implement risk management within the Team
- meet quarterly as a Risk Management Group to review the Connexional Team Risk Register and the actions being taken to mitigate the risks;
- remove from the Register any risks that have ceased to exist and identify emerging risks.
- at its , September, November, February and April, meeting review the Connexional Team and Corporate Risk Registers
- report to the Strategy and Resources Committee and the Methodist Council on any serious new risks or serious risks that have heightened impact or likelihood of occurring at any appropriate time during the course of the year;
- when meeting as the Risk Management Group, identify and evaluate the significant risks faced by the Team using the process outlined below.
- provide at least an annual report to the Methodist Council in October on the Team and Corporate Risk Registers.
- Identify whether the financial impact of any risks can be insured against and if so, obtain insurance quotes and report these to the SRC Finance Sub-Committee for decision.

**5.5 The Connexional Team shall:-**

- report any new risks that arise or are identified or those that might have ceased to exist to their line manager
- understand the purpose of risk management and undertake its work in the knowledge of the Council's risk appetite

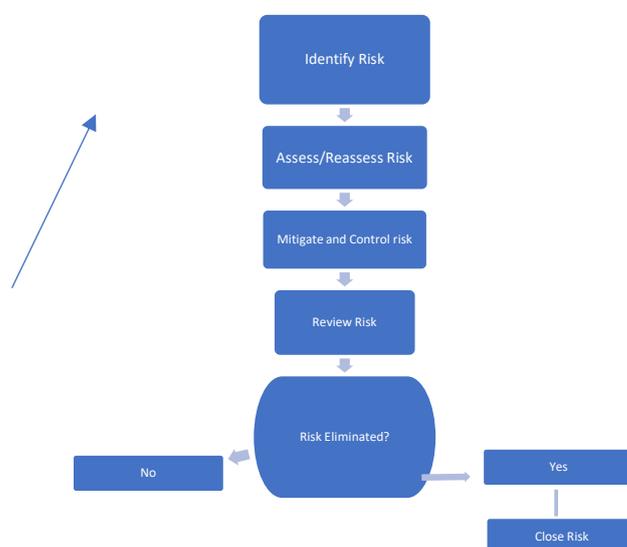
## 6 Risk Management Procedure

### 6.1 Important risk management concepts:

As part of the Church's commitment to effective risk management:

- there should be an environment where risks are openly discussed and where mistakes and untoward events are dealt with in a non-punitive and responsive manner;
- risks should be assessed objectively not subjectively. This means when completing a risk assessment reference is to fact not opinion, and to explanation instead of judgement;
- when a risk assessment is completed it needs to be reviewed accordingly. The higher the risk rating score the more frequently a risk assessment should be reviewed;
- risk management is a dynamic continuous process.

The model below sets out the life-cycle for a risk within the Church's procedures and is useful to use when regularly reviewing risks:



### 6.2 Identifying Risks

There are different ways to identify risks, for example:

- pro-active risk assessment (eg carrying out a risk assessment; considering risks in preparation for a major project, new contract etc);
- reactive risk assessment (eg as a result of a serious incident)
- as part of an internal audit
- as a result of assessments or inspections by external bodies;
- from feedback from stakeholders;
- as a result of enquiry or complaints;
- as a result of new legislation or guidance issued;
- as a result of a national and regional safety alert;
- through observation or review of current practices.

In all business areas, the Connexional Team will carry out regular risk assessments and identification, record the findings (on risk assessment forms or Registers as appropriate - see below) and take appropriate management actions in a timely fashion. Risk reviews will specifically address

business, operational, financial and reputational risks as well as risks covered by Health and Safety and other relevant legislation.

Risk reviews may be undertaken through the use of risk assessment forms.

The following activities, because of the intrinsic risks or from past experience, present particularly high risk profiles and will require formal risk management activities to be undertaken:

- where safeguarding requirements or concerns form a central part of the activity
- where public interest is particularly high

Where appropriate, the Connexional Team may need to consider specialist advice for areas such as:

- health and safety (including safeguarding)
- fire and security
- disaster recovery
- safety-critical systems and operations
- insurance
- media/public relations

**Risk Areas** – the following table should be used as a guide when identifying risks:

Area	Sub categories	Examples ( <i>these are examples only and is not an exhaustive list</i> )	Risk Owners
Risks to the achievement of the Methodist Council objectives  <i>(Such risks will form part of the Corporate Risk Register)</i>	Current objectives: <ul style="list-style-type: none"> <li>• Proclaiming the Gospel through worship</li> <li>• The ministry of the whole people of God in the life of the world</li> <li>• Resources for the Church: the use of God's good gifts_</li> <li>• Oversight and Leadership</li> <li>• A Church for all people</li> <li>• Social Holiness</li> <li>• Evangelism</li> <li>• One Mission</li> </ul>	Identify the risks to each of the aims that sit under each objective: <i>For example, "The Council will aim to ensure the support and training is offered to resource local arrangements appropriately."</i>  Risks to this may include lack of finance to fund training; inconsistency of training quality etc.	
Finance, IT & Resources	<ul style="list-style-type: none"> <li>• Cash flow</li> <li>• Budget</li> <li>• Financing/Income</li> <li>• Economy</li> <li>• Fraud</li> </ul>	<ul style="list-style-type: none"> <li>• inadequate reserves and cash flow</li> <li>• movements between different account codes are not scrutinised, which could conceal error or fraud</li> </ul>	<ul style="list-style-type: none"> <li>• Connexional Secretary</li> <li>• Director of Finance &amp; Resources</li> <li>• Procurement Manager</li> <li>• Director of Strategic Property Development</li> <li>• IT Manager</li> </ul>

		<ul style="list-style-type: none"> <li>• errors, omissions and inappropriate transactions are not identified and acted upon</li> <li>• data lost due to insecure device management</li> <li>• IT firewalls do not provide adequate security</li> </ul>	<ul style="list-style-type: none"> <li>• Data Protection Officer</li> <li>• Budget Holders</li> </ul>
Human Resources & Development	<ul style="list-style-type: none"> <li>• Legal inc claims</li> <li>• Recruitment</li> <li>• Retention</li> <li>• Training</li> </ul>	<ul style="list-style-type: none"> <li>• breach of immigration rules</li> <li>• loss of key staff</li> <li>• serious accident or injury occurring to staff overseas</li> </ul>	<ul style="list-style-type: none"> <li>• Director of HR &amp; Development</li> </ul>
Reputation	<ul style="list-style-type: none"> <li>• Mission</li> <li>• Communications &amp; Media</li> <li>• Political</li> <li>• Safeguarding</li> </ul>	<ul style="list-style-type: none"> <li>• failure to effectively handle negative media stories</li> <li>• allegations around political bias</li> <li>• grant money not reaching intended recipients</li> </ul>	<ul style="list-style-type: none"> <li>• Director of Engagement</li> <li>• Joint Public Issues Team Leader</li> <li>• Director of Communications</li> </ul>
Conference Office/Governance	<ul style="list-style-type: none"> <li>• Regulation</li> <li>• Compliance</li> <li>• Business Interruption</li> <li>• Health &amp; Safety</li> </ul>	<ul style="list-style-type: none"> <li>• acting in breach of trust</li> <li>• poor knowledge of legal responsibilities;</li> <li>• poor knowledge of regulations and procedures</li> <li>• changing government policy</li> <li>• conditions in server room present a health &amp; safety risk or potential fire hazard</li> <li>• failure to comply with health &amp; safety legislation</li> </ul>	<ul style="list-style-type: none"> <li>• Conference Officer for Legal and Constitutional Practice</li> <li>• Assistant Secretary of the Conference</li> <li>• Connexional Safeguarding Adviser</li> <li>• Connexional Property Coordinator</li> </ul>

### 6.3 Risk Analysis

All identified risks must be assessed based on the likelihood of it occurring and the relative impact if it does.

#### Heat Matrix Schedule – scoring of risks

##### Impact:

Descriptor	Score	What is the scale of the potential impact?
Low	1	<ul style="list-style-type: none"> <li>No harm to beneficiaries</li> <li>Minimal financial loss through error (up to £5,000)</li> <li>Minimal impact on the work of the Team or Council's ability to fulfil Our Calling</li> <li>No loss of personal data</li> <li>No breach of regulation or legislation</li> <li>No impact on membership</li> </ul>
Medium	2	<ul style="list-style-type: none"> <li>Potential for adverse publicity – avoidable with careful handling</li> <li>Minimal harm to beneficiaries, ministers and staff (not children or vulnerable adults)</li> <li>Moderate financial loss through error or fraud (up to £25,000)</li> <li>Minimal loss of personal data that can be contained</li> <li>Minimal decline in membership</li> </ul>
High	3	<ul style="list-style-type: none"> <li>Adverse publicity not avoidable (local media)</li> <li>Harm to small number of beneficiaries including children and vulnerable adults</li> <li>Limits ability of the Council to further <i>Our Calling</i></li> <li>Significant financial loss through error or fraud (up to £100,000)</li> <li>Loss of personal data (not sensitive)</li> <li>Breach of regulation that results in small fine</li> <li>Small number of local churches or circuits want to leave the connexion</li> <li>Litigation that results in financial loss</li> <li>Moderate decline in membership</li> </ul>
Very High	4	<ul style="list-style-type: none"> <li>Major adverse publicity (national media)</li> <li>Serious harm to beneficiaries including children and vulnerable adults</li> <li>Prevents Council from being able to further Our Calling</li> <li>Breach of regulation or legislation that results in significant fine and potential criminal liability</li> <li>Major financial loss (over £100,000)</li> <li>Major loss of sensitive personal data to unknown source and not recoverable</li> <li>Litigation that result in financial loss and reputational damage</li> <li>Investigation by external regulator or police</li> <li>Significant number of local churches or circuits wanting to leave the Connexion</li> <li>Significant decline in membership</li> </ul>

**Likelihood:**

Descriptor	Score	What is the likelihood that this could happen?
Low	1	Expected to occur in a few circumstances
Medium	2	Expected to occur in some circumstances
High	3	Expected to occur in many circumstances
Very High	4	Expected to occur frequently and in most circumstances or has occurred before

**6.4 Prioritisation of Risks**

A total risk score must be allocated to each risk; this will be multiplying the impact and likelihood scores. Scores should be given to risks:

- Absolutely (Gross) = ie before the application of controls; and
- Residually (Net) = ie after the application of mitigation / controls.

This allows you to assess whether any mitigation and controls are effective.

The likelihood and impact scores are multiplied to give the total risk score.

		Example
Scored 1 to 3	Low risk	Impact 1 x Likelihood 1 = total risk of 1
Scored 4 to 6	Moderate risk	Impact 2 x Likelihood 2 = total risk of 4
Scored 7 to 9	High risk	Impact 3 x Likelihood 3 = total risk of 9
Score 10 or above	Very high risk	Impact 4 x Likelihood 4 = total risk of 16

**‘The Heat Matrix’**

Impact	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		<b>Likelihood</b>			

**6.5 Risk Control**

At this stage a decision must be made as to what should be done with the risk. The decision must be proportionate to the level of risks, the costs of any controls and likely benefits.

There are four main actions that can be taken in addressing risks. They are listed below:-

- **Terminate**- this could be by stopping the relevant activity that is causing the risk
- **Treat**- The greatest number of risks would be addressed this way. Any action taken should be to constrain the risk to an acceptable level and the type of action that could be taken is listed into different types of control action that could be taken and listed below:-
  - a) Preventative – to limit the possibility of an undesirable outcome being realised- e.g. independent inspection
  - b) Corrective- to correct undesirable outcomes which have been realised- e.g. contingency planning
  - c) Directive - to ensure a particular outcome is achieved- e.g. training required
  - d) Detective eg asset checks

- **Transfer**- for some risks the best response may be to transfer them, either through conventional insurance or paying a third party to take the risk on.
- **Tolerate**- some risks may be tolerable without action. It could also be possible that due to budgetary constraints nothing can be done.

It is important to compare the absolute and residual risk scores to make an assessment over the strength of the existing control environment for the purposes of managing each risk.

**Once it has been decided how to control the risk, the risk must be managed:**

- Assessed risks should be addressed by levels of management appropriate to the nature and magnitude of the risk and an overall view of the portfolio risk to the business is taken.
- Decisions documented and the resulting actions implemented through appropriate procedures
- Appropriate and cost-efficient actions taken to manage and control risks.

**7. Risk Registers**

Each risk scenario should be logged onto the respective risk register:

- Corporate Register– those broad risks that effect the Methodist Church at a strategic/organisation-wide level. This register is owned by the Conference and delegated to the Council for ongoing maintenance and monitoring. The Corporate Register shall be reviewed annually by the Council and the register reported to the Methodist Conference.
- Connexional Team Register - those risks that relate to the work of the Team. The Connexional Team Register shall be prepared by the Senior Management Group through the identification and assessment of risks to the work of the Team. The Risk Register is separated into cluster/office categories so that the risk owners for each one are clear.

**8. Monitoring and Reporting**

**8.1 Monitoring**

8.1.1 The Connexional Team Risk Register shall be maintained by designated risk owners who shall be responsible for the ongoing monitoring of risks and identification of emerging risks, determine the likelihood of the risks and how best to mitigate them within that Cluster. The relevant Senior Manager for each office shall be responsible for ensuring that all risks are being monitored.

8.1.2 The Senior Management Group shall meet as the Risk Management Group on a quarterly basis and shall review the register and consider whether any scores should be amended and whether there are emerging risks or whether any of the existing risks can be removed.

8.1.3 The Risk Registers shall be presented to the Strategy and Resources Committee annually.

**8.2 Reporting**

**8.2.1 Annual Cycle of Risk Management**

- Connexional Team members should update and monitor their risks on a continuous basis;
- Senior Management Group should meet once a quarter as the Risk Management Group to review the Connexional Team Registers during the following months: September, November, February and April;
- A detailed annual review of the Risk Register, the Risk Management Policy and the wider systems of internal control to take place in the July Risk Management Group meeting;
- The Connexional Team Risk Register should be reviewed by the SRC at its meeting in September;
- The Council should review the Corporate Risk Register and risk management policy at its meeting in October;

- The Audit Committee receives the risk management policy at its meeting in May and updates to the Connexional Team and Corporate Risk Registers in May, October and December.

## **9. Escalating risks**

- 9.1 The Church ensures appropriate oversight and scrutiny of significant risks by adopting processes for risk escalation.
- 9.2 There are three levels of risk register –
- Function
  - Connexional Team
  - Corporate
- 9.3 Risk escalation, is determined by risk score, with risks over a certain level being escalated to the level above and reassessed at each level.
- 9.4 Decisions to escalate or de-escalate risks will be based on risk score:
- Function – if scored 4 or above, will be reported to Risk Management Group;
  - Connexional Team – if scored 12 or above, will be reported to each SRC meeting for information (with full register going annually);
  - Corporate Register – if scored 12 or above will be reported to each Council meeting for information (with full register going annually).
- 9.5 This escalation process ensures that the Council and its sub-committees have frequent view of the most serious risks facing the Church outside of the annual full review.
- 9.6 There is also provision for escalating risks outside of the defined escalation process where a member of the Connexional Team has immediate concerns about a risk.

## **10. Audit and Review**

- 10.1 A programme of regular audits and reviews to ensure that the risk management procedures are being followed and that planned risk reduction/mitigation actions have been implemented.
- 10.2 An annual review of the risk management policies and procedures to ensure that they continue to meet Charity Governance Code requirements and the needs of the Church.

### **10.3 Evidence of Compliance**

To demonstrate compliance with this Policy, the following documentation is to be available for audit:

- risk management policy (this document)
- related policy statements and procedures
- any risk assessment of the Church's activities including risk assessments undertaken for particular projects
- risk registers
- crisis management plan (business continuity plan)
- minutes of Board/Committee meetings
- internal audit reports