# Policy Guide and Checklist

This front page is to guide users in developing their Risk Management Policy and Procedures. To help you complete your policy and procedures:

* Basic instructions and choices between specific terms are indicated by yellow highlighting.
* Sections requiring detail are indicated by green highlighting.

For further guidance, the following resources are recommended:

* Institute of Community Directors Australia [The Main Areas of Risk for Not-for-Profit Organisations](https://www.communitydirectors.com.au/help-sheets/the-main-areas-of-risk-for-not-for-profit-organisations)
* Justice Connect [Insurance and Risk Management for Community Organisations](https://content.nfplaw.org.au/wp-content/uploads/2023/06/Insurance-and-risk-management-for-community-organisations.pdf?_ga=2.211857428.1413195313.1727917173-894528289.1723155320)
* MinterEllison Risk and Regulatory Consulting [Risk Management Guide & Health Check – A guide for not-for-profits and social enterprises](https://www.minterellison.com/articles/a-guide-to-risk-management-for-not-for-profits-and-social-enterprises)
* Australian Council of Social Service (ACOSS) [Managing Your Risk: Risk Register](https://resilience.acoss.org.au/the-six-steps/managing-your-risks/risk-register)
* Community Door [Risk Management](https://communitydoor.org.au/resources/risk-management)
* Brisbane City Council [Risk Management for Community Organisations](https://www.brisbane.qld.gov.au/things-to-see-and-do/council-venues-and-precincts/community-facilities-leasing-sport-and-recreation/managing-your-community-organisation/risk-management)
* Our Community [Help Sheet: Identifying Risks](https://www.ourcommunity.com.au/insurance/view_help_sheet.do?articleid=341)
* Queensland Government [Business Continuity Planning](https://www.business.qld.gov.au/running-business/risk/continuity-plan)

We also recommend that you source and use resources focused on particular areas of risk relevant to your organisation. For example, if you have staff undertaking home visits, WorkSafe Queensland [A Guide to Working Safely in People’s Homes](https://www.worksafe.qld.gov.au/__data/assets/pdf_file/0012/22233/community-working-safely-in-peoples-homes.pdf) and WorkSafe Victoria [Working Safely in Visiting Health Services: A handbook for workplaces](https://content-v2.api.worksafe.vic.gov.au/sites/default/files/2018-06/ISBN-Working-safely-in-visiting-health-sevices-handbook-for-workplaces-2006-06.pdf).

Before submitting this document for approval, check that you have completed the following:

Read the current[[1]](#footnote-2) HSQF Framework Version.

Read the current HSQF User guide – Certification or HSQF User Guide – Self-Assessable (as appropriate to your service agreement and organisation).

Checked the most recent HSQF Version Control Register and Log of Changes and included any relevant changes in your policy draft.

Included the document code/version number in accordance with your organisation’s version control procedure.

Replaced all reference to organisation with your organisation name.

Customised or deleted (as appropriate) all yellow highlighted sections.

Drafted content for or deleted (as appropriate) all green highlighted sections.

Customised the Relevant Legislation and Standards, Related Policies and Procedures and Supporting Documents lists.

Customised, removed or added to the Appendices (as appropriate).

Updated the header and footer to reflect the document name, version and other relevant details for your organisation.

Added a review date.

Logged any changes to policies/procedures in your organisation’s Policies and Procedures Register.

Deleted all footnotes.

Removed QCOSS branding and replaced it with your organisation’s branding.

**Delete** these two pages once your Risk Management Policy and Procedures has been approved and finalised.

Risk Management Policy and Procedures

#### Document Code / Version Number

# Policy Statement

Risk management is essential to the safety of our staff, clients and community members; effective service delivery; and our viability as an organisation. Organisation follows a structured approach to identify, analyse and manage risks. Our risk management framework and practices are regularly reviewed. The governance body has oversight of risk management.

## Scope

This policy and associated procedures apply to Organisation as a whole, including all employees, volunteers, and governance body members.

# HSQF Related Standards

* Human Services Quality Standard Indicator 1.4

and elements of

* Human Services Quality Standard Indicator 1.1, 1.3, 1.5, 1.6, 1.7 and 4.2

# Relevant Legislation and Standards

To customise/complete the table below:

* Add any relevant documents; for example, if your organisation uses a risk management standard, link to that standard; if you have contracts/agreements that specify risk management processes/standards, include reference to these.
* Check for updates to guidelines, models, etc., and update links as appropriate.

|  |  |
| --- | --- |
| **Common**  Add to list as appropriate |  |

# Definitions

**Assumptions:** Ideas about factors relevant to risk that underpin decisions, e.g., organisational resources, particular regulations or the political environment in which the organisation operates

**Consequence:** Impact of a risk event if it occurs; often referred to by severity (e.g., insignificant/trivial, minor, moderate, major or critical)

**Control:** Measures to reduce the likelihood and/or consequences of a risk[[2]](#footnote-3)

**Inherent risk level:** The assessed risk rating where no controls are in use (see *residual risk level*)

**Likelihood:** Chance of a risk event occurring (e.g., rare, unlikely, moderate, likely or almost certain)

**Residual risk:** The risk that remains after controls have been applied

**Residual risk level:** The assessed risk rating where controls have been applied

**Responses to risk:**

**Acceptance/retention:** Accepting that a risk may occur and planning a response if it does; accepting the potential benefits or costs of a risk

**Avoidance:** Removing exposure to a risk by stopping or not starting an activity that creates a the risk

**Treatment:** Reducing the likelihood or consequences if a risk occurs

**Transfer:** Passinga risk on to another body (e.g., through insurance)

**Risks:** Possibility of harm or negative effects on a person, group, organisational asset or the organisation’s priorities, aims and viability

**Risk appetite:** The level of risk an organisation is willing to take; may be referred to as the **acceptable level of risk**

**Risk assessment:** The process of identifying and analysing risk

**Risk event:** An event that causes harmful effects or where management strategies are needed to prevent the harmful effects (e.g., an accident or critical incident, theft, cybersecurity breach)

**Risk level:** Determination of the seriousness of a risk in light of its likelihood, consequences and controls in place

**Risk management:** Coordinated activities to reduce or control risk

**Risk management process:** Effective implementation of risk management policies, procedures and activities

**Risk treatment:** Selecting and implementing controls to reduce risk

**Risk tolerance:** Level of a particular risk that the organisation can accept

**Stakeholder:** A person, group or organisation affected or potentially affected by risk management processes and strategies

Add/modify definitions as appropriate

# Principles

The principles that support organisation’s Governance Policy and Procedures, and associated practices, are:

Add/adapt definitions relevant to your organisation’s risk management

**Risk is inherent in all our activities.**

**Risk appetite:** Organisation’s governance body sets, monitors and updates our risk appetite for different types/areas of risk to guide staff decisions, and communicates this clearly to all staff.

**Risk management:** Risks are not inherently bad or to be avoided, but must be effectively addressed. Identifying, assessing and controlling risks is integrated into all our activities and decision.

* **Positive risk culture:** Risk culture refers to shared or common attitudes, values and behaviours relating to risk within the organisation; a positive risk cultures involves staff awareness of risk and the integration of appropriate and well-balanced risk management across the organisation.

# Procedures

## Risk Management Process

Outline your risk management process. The following is a generic process that may be adapted to your context.

The overall risk management process we undertake is:

1. Identify current or potential risk and log this in the Risk Register.
2. Assess risk, including all foreseeable consequences and risk levels.
3. Determine the approach to the risk. Where the risk is not avoided, continue with steps 4-7.
4. Identify potential risk controls or methods to increase potential benefits; determine the appropriate/preferred risk controls, with internal and/or external consultation as appropriate.
5. Implement chosen risk management strategies.
6. Monitor outcomes and assess any continuing or newly arising risk, including
   * effects of risk controls;
   * residual risk; and
   * changes in the operating environment that change the risk assessment or other factors affecting likelihood, consequences, risk appetite or risk tolerance.
7. Repeat from step 2 as appropriate.

Add to/adapt process as appropriate.

Refer to relevant appendices/supporting documents, e.g., See Appendix 1: Risk Management Process for details and Appendix 2: Risk Management Plan/Worksheet when undertaking risk assessment and management planning. See Appendix 3: Common Areas of Risk for examples of key risks in our sector/work.

## Roles and Responsibilities

### All Staff Responsibilities

All staff, including volunteers and managers, are responsible for:

Familiarising themselves with the risk management framework.

Implementing risk management plans and other aspects of the risk management framework as appropriate to their roles and competencies.

Proactively identifying and reporting potential risks and hazards for management, including:

* + risks that are currently unmanaged or inadequately managed;
  + incidents, including near misses; and
  + instances in which other people within scope of this policy and procedures are not acting in accordance with it.

Abiding by this and all related policies and procedures to promote effective risk management and protect the safety of people and the viability of the organisation.

Add/adapt responsibilities as appropriate.

### Management Responsibilities

Managers/Senior staff/Members of the leadership team hold additional responsibilities for risk management, specifically:

Appropriately inducting new staff, and refreshing the knowledge and skills of existing staff, in risk management.

Facilitating the identification and internal reporting of risks and hazards.

Entering and monitoring risks and associated strategies in the Risk Register.

Reporting on risks and the application of risk management strategies to the governance body regularly.

Reviewing the organisation’s Risk Register and overall risk management frequency and reporting on this to the governance body.

Reviewing the organisation’s risk management framework frequency and reporting on this to the governance body.

Add/adapt responsibilities as appropriate.

### Governance Body Responsibilities

The governance body is responsible for setting and maintaining Organisation’s risk management framework and overseeing its operation. This includes:

Determining and communicating risk appetite, tolerance, and plan to management and staff.

Integrating risk management into their regular meetings, documenting the outcomes of this discussion, and completing follow-up actions or communicating the need for actions and monitoring these where management or other staff are required to undertake follow-up activities.

Reviewing the Risk Register and overall risk management frequency.

Reviewing the function of the risk management framework frequency, including:

* + the assumptions underpinning the framework;
  + their own and staff decisions and the outcomes of these;
  + incident and other risk-related reports; and
  + the strategies management and other staff are employing in carrying out their work activities.

Identifying where changes in circumstances or information indicate that a change or changes to the framework are appropriate, and facilitating this.

Providing considered and timely guidance on risk management as requested by staff.

Add/adapt responsibilities as appropriate.

## Business Continuity/Disaster Planning

**Note:** Guidance on developing a business continuity plan is attached at Appendix 4. You may like to include a process for developing the plan, highlighting the steps in Appendix 4, here, or refer to the Appendix 4.

Organisation has and regularly reviews and updates a Business Continuity Plan to outline the purposes of your plan, e.g. guide actions that will reduce the consequences of events beyond our control that impact our ability to undertake our regular operations, such as electricity and/or IT outages, extreme weather events, pandemics, and staff shortages. The plan is intended to minimise the disruption to our operations, in particular our service delivery.

Outline responsibilities relating to the plan, e.g., All staff are responsible for maintaining familiarity with this plan and their responsibilities if the plan is enacted.

Senior staff/Management and the governance body are further responsible for:

Reviewing and, where appropriate, updating the plan frequency and where changes in circumstances warrant additional review (e.g., extreme weather is expected, staff shortage risks increase).

Inducting new staff and monitoring the familiarity of existing staff with the plan.

Determining when the plan will be enacted and ensuring it is enacted where appropriate.

Guiding staff in enacting their responsibilities under the plan.

The current Business Continuity Plan is available at hyperlink.

# Related Policies and Procedures

List all relevant/related policies and procedures, including any that discuss particular risk management responsibilities and all those referred to in the body of this document.

Governance Policy and Procedures

Financial Management Policy and Procedures

Continuous Improvement Policy and Procedures

Positive Behaviour Support and Child Protection Policy and Procedures

Human Rights Policy and Procedures

Client Safety and Wellbeing Policy and Procedures

Preventing, Reporting and Responding to Harm, Abuse and Neglect Policy and Procedures

Incident Management Policy and Procedures

# Supporting Documents

List all relevant/related documents that are not policies and procedures, including registers, agreements, and guidelines and all supporting documents referred to in the body of this document.

Risk Management Worksheet/Plan

Risk Register

Business Continuity Plan

# Review

This document was last reviewed on date.

This document will be reviewed by date.

# Appendix 1: Risk Management Process

Adapt as appropriate or replace with your organisation’s risk management process/framework document. You may like to provide an introduction about the organisation’s approach to risk, the risk culture you hope to create or maintain, etc. You may like to provide guidance on the types of risk the organisation categorises identified risks and risk management by, e.g., governance, financial, human resources, operational (processes and systems), legal, reputational, project-specific, etc. A pictorial tool, such as the one below, can help communicate the process. **Note:** This appendix expands upon the overall risk management process outlined in the relevant procedure; if an appendix/’Risk Management Process’ guide isn’t included here, you will need to provide guidance on following that procedure elsewhere.

## 1. Risk Identification

Provide an introduction to risk identification responsibilities, e.g., Risk identification is a continuous activity within the organisation. Risks can exist whether they are currently recognised or subject to controls. Risk identification is a shared responsibility, with all staff (including managers and volunteers) are responsible for identifying risks that are currently managed (and working in accordance with the management plan), risks that are identified but inadequately managed, and risks that have not been identified or managed.

We identify risks through list relevant activities, e.g.,

Discussions, interviews and/or brainstorms with teams, full organisation staff, all stakeholders/representatives of all stakeholder groups, etc..

Project planning.

Business as usual activities/day to day service delivery/ observations of work processes/practices.

Site inspections.

Internal audits (may be multiple specific audits, e.g., work health and safety audit, financial audit, policy and procedure audit, compliance audit, etc.).

External audits.

Consulting experts, such as equipment providers, peak bodies, funders and unions.

Using guidelines and resources relevant to our operation type, work activities, etc.

Equipment checks.

Review processes for complaints, incidents, plans, (may be multiple specific, plans, e.g., strategic plan, operation plan, etc.), policies and procedures, contracts, etc..

## 2. Risk Assessment

Provide guidance on your risk assessment process. Below is a generic process that can be adapted or replaced as appropriate.

Risk is assessed by integrating information about:

* **Likelihood:** The chance of a risk event occurring
* **Consequences:** Impact of a risk event if it occurs

A single risk event or type of risk is likely to have multiple potential consequences that need to be assessed.

### Rating the Likelihood Level

**Likelihood** of a risk event is rated as:

**Rare:** Very unlikely to happen; not expected to happen within the next decade, for example.

**Unlikely:** May occur infrequently; may happen once every 5-10 years, for example.

**Possible:** May happen but unlikely in a given year; may be expected approximately once every 3 years, for example.

**Likely:** Will probably occur; expected to happen once a year, for example.

**Almost certain:** Expected to occur in most circumstances or several times per year.

Likelihood is influenced by the nature of tasks undertaking, knowledge and skills of people involved, operating environment, etc., and can change unexpectedly. When a factor influencing a risk changes, the risk must be re-assessed.

### Rating the Consequence Level

A **consequence** of a risk event is rated as:

* **Insignificant:** Trivial impact with no ongoing repercussions, such as provide examples that are relevant to your organisation, e.g., a minor injury requiring only first aid and requiring no time off work; causing a minimal disruption to service delivery; surface-level damage to equipment that doesn’t affect its operations.
* **Minor:** Effectsare limited and manageable, for example provide examples that are relevant to your organisation, e.g., an injury or illness requiring basic medical attention or minor injury; easily manageable expenditure (e.g., minor repairs to equipment).
* **Moderate:** Impacts are not severe or long-lasting but may be significant, particularly in the short-term, such as provide examples that are relevant to your organisation, e.g., an injury or illness requiring brief hospital admission or up to 10 days off work; temporary and recoverable damage to the organisation’s reputation; significant disruptions to service delivery or other operations.
* **Major:** Very serious or lasting harm, such provide examples that are relevant to your organisation, e.g., as significant injuries or illness requiring substantial treatment and/or more than 10 days of work; reputational damage that damages funding or ongoing operational capacity; a legal liability with significant legal costs.
* **Critical:** Extremely serious harm, for example, provide examples that are relevant to your organisation, e.g., life-threatening, disabling or fatal injury or illness; legal liability, reputational damage or regulatory non-compliance that results in the organisation being defunded and losing the right to run its programs (e.g., failure to address HSQF non-compliances leading to de-certification).

### Determining the Risk Level

Likelihood and consequence ratings are combined to identify the **risk level** using the matrix below (or replace with your matrix/rating tool).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Likelihood** | Almost certain | **Medium** | **High** | **High** | **Extreme** | **Extreme** |
| Likely | **Medium** | **Medium** | **High** | **High** | **Extreme** |
| Possible | **Low** | **Medium** | **High** | **High** | **High** |
| Unlikely | **Low** | **Low** | **Medium** | **Medium** | **High** |
| Rare | **Low** | **Low** | **Medium** | **Medium** | **High** |
|  | Insignificant | Minor | Moderate | Major | Critical |
| **Consequence** | | | | | | |

Risk assessment must be discussed with your line manager, a member of the management team and/or the governing body.

Outline the responsibility levels within your organisation, e.g.:

**Low level risks** may be managed by all staff with controls approved by their managers. Management is ongoing.

Assessment of **medium level risks** and their management must be considered by management/ executive management/leadership team. Medium level risks may be acceptable, but risk controls should be undertaken wherever *reasonably practicable[[3]](#footnote-4)*.

**High and extreme risks** must be urgently reviewed and managed by the CEO/executive director/ manager and governance body.

The risk level, reasons for the assessment, internal reporting and discussions, and further management must be document, regardless of risk level. All risks require ongoing management, monitoring and review via the Risk Register and reporting (as described in the policy and procedures).

## 3. Determining the Risk Approach

Provide guidance on the process for determining the approach to risk. Below is a generic process that can be adapted or replaced as appropriate.

When a risk has been assessed, the approach to risk is decided on. The risk may be:

**Accepted:** The risk level is considered acceptable – the organisation accepts the likelihood and potential consequences of the risk – and the activity goes ahead because:

* + the risk level is deemed reasonable for the kind of activity or organisation type, or
  + after control options are considered, risk treatment is unavailable or deemed so costly that it outweighs the benefits and the activity is appropriate to the organisation’s purpose, or
  + that the potential benefits make taking the risk worthwhile.

Low level risks are most likely to be acceptable; in general, extreme and high risks cannot be accepted. Accepting the risk doesn’t mean that the risk is insignificant and that ongoing monitoring is essential, with the potential for re-assessment in future.

**Reduced, shared or transferred:** Strategies are used to reduce, share or transfer the risk, such as through insurance against potential consequences or contracting with an external expert to undertake the activity. Residual risk assessment and ongoing monitoring remains a requirement.

**Controlled:** Strategies to eliminate or reduce the risk will be used, with ongoing management and monitoring.

**Avoided:** The activity is discontinued or not undertaken; a lower-risk alternative activity or approach may be considered.

The decision, the factors considered, and the people making this decision must all be documented.

## 4. Risk Treatment: Determining Controls

Provide guidance on the process for determining controls. Below is a generic process that can be adapted or replaced as appropriate.

When a risk is to be treated, seek strategies that eliminate the risk, reduce its likelihood and/or reduce the severity of the consequences if it occurs. Strategy types include:

Providing relevant training and guidance to staff member (e.g., induction training, appropriate policies and procedures, supervision).

Creating regulatory ‘checks and balances’.

Instituting barriers (physical or digital) to accessing certain areas.

Installing monitoring processes and equipment.

Developing comprehensive reporting and review systems.

Audits or quality assurance/control checks.

Developing and resourcing business continuity/disaster plans.

Use of personal protective equipment (PPE).

Control strategies must be tailored to the type of risk, the environment where the risk occurs and the people who will be using risk control strategies. For example, one control measure for financial risk is to have secure banking arrangements with two identified signatories required to approve financial transactions over a certain amount; one control measure for risk of car accidents is to have the currency of drivers licences of anyone who may drive as part of their work before they begin employment; and so on.

Before settling on a control or controls to use:

Discuss the suitability of potential controls with the appropriate manager and/or governance body member(s), as well as any staff who will be responsible for carrying it out, seeking potential weaknesses in the proposal and alternatives.

Consult any guidelines, experts or other resources that may provide information, ideas or perspectives that strengthen your risk management planning (e.g., you might consult WorkSafe Queensland regarding unsafe work tasks or environments, an accountant or auditor regarding a financial risk, etc.).

Critically evaluate the proposed control(s), considering how much they are likely to reduce the risk likelihood or consequences, whether this is adequate and any residual risk.

Where residual risk is present, repeat the risk management process (Steps 1-4) in relation to the residual risk.

## 5. Implementing Risk Controls

Provide guidance on the process for implementing controls. Below is a generic process that can be adapted or replaced as appropriate.

Implementation of risk controls involves:

Communicating the risk, the need for control, and the control strategy(ies) to all relevant stakeholders, particularly those responsible for undertaking or monitoring the controls. This can be done through a combination of:

* + Discussion in regular meetings.
  + A special meeting.
  + Providing training.
  + Circulating a new procedure or process document.

Providing guidance on implementing the risk control to those with responsibility for doing so; the guidance must be thorough and accessible, providing all the information required to effectively implement the control. In relation to some risks, expert supervision may be required in the early stages or training/certification before independent implementation is appropriate.

Continuous review of the risk and the controls in place.

You may also need to integrate the risk controls into other policies and procedures, induction processes for new staff, and refresher training/upskilling/discussions or regular reviews with responsible people.

## 6. Monitoring and Ongoing Management

Provide guidance on the process for monitoring and ongoing management. Below is generic information that can be adapted or replaced as appropriate.

Depending on the nature and level of the risk, monitoring of ongoing risk management may be intensive or relatively infrequent. For a high risk level, this may involve very regular reviews of processes, reports, incidents and other relevant information, while reviews and other monitoring activities may be annual for very low level risks. The key things are to make sure that:

A plan for timely and effective monitoring is developed and approved by the appropriate manager/management group/governance body.

The person or group responsible for monitoring is clearly identified and informed of their responsibilities in this area.

There is a process for all necessary reviews and reporting, including documentation in the Risk Register or other relevant document.

Monitoring activities are undertaken according the plan and reviewed by senior management or other relevant role/group and the governance body.

Changes in the risk environment, likely risk level or effectiveness of controls are proactively identified and reported to the relevant person or group for further risk assessment and control.

## 7. Further Assessment and Control

Provide guidance on the process for determining controls. Below is a information that can be adapted or replaced as appropriate.

When regular monitoring or other risk identification activities indicate that the controls are not as effective as expected, results of a risk assessment are out of date or inaccurate, or there is residual unmanaged risk, the risk management process returns to Step 2.

## Documentation Requirements

Provide guidance on the process for documenting risk management. Below is a list of general improvements that can be adapted or replaced as appropriate.

Information about all these steps must be documented, including:

Each risk identified.

Likelihood, severity and risk level for each potential consequence.

Determination of approach to risk

Any controls attempted.

Results of reviews, residual risk assessments, changed circumstances, etc.

All people involved in any of these steps.

The factors considered in this process.

# Appendix 2: Risk Management Worksheet/Plan

Adapt as appropriate or replace with your organisation’s risk management tool. This tool has been formatted as a table; you may like to format it using your organisation’s colour, style, etc..

Use the Risk Management Process for guidance as you work through this worksheet/plan.

## 1. Risk Identification

|  |
| --- |
| Describe the risk, including the type of risk (physical, governance, human resource, etc.), what potential risk events may be (e.g., fire, breach of regulation, barrier to retaining skilled workforce, etc.) and circumstance or other factors that could influence risk level. *For risks associated with multiple risk events, identify all potential risk events, number them for ease of reference, and apply the steps below to each type of risk event. You can use separate worksheets for each or use the extra spaces in the relevant segments below by clicking the downward arrows.* |
|  |

## 2. Risk Assessment

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Consider the likelihood of the risk event under the current circumstances and potential consequences if it occurs. Identify any assumption that influence your assessment and consider whether these may be inaccurate or likely to change.*If you identify multiple potential consequences with different severities, make each of these a risk event and assess them separately.* | | | | | | | | |
| What is the likelihood? | Rare | Unlikely | | Possible | | Likely | | Almost certain |
| How severe are the consequences? | Insignificant | Minor | | Moderate | | Major | | Catastrophic |
| What is the risk level? | Low | | Medium | | High | | Extreme | |
| What *assumptions* influence this assessment? |  | | | | | | | |

For further risk assessment boxes, click the triangles below for additional boxes.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Consider the likelihood of the risk event under the current circumstances and potential consequences if it occurs. Identify any assumption that influence your assessment and consider whether these may be inaccurate or likely to change. | | | | | | | | |
| What is the likelihood? | Rare | Unlikely | | Possible | | Likely | Almost certain | |
| How severe are the consequences? | Insignificant | Minor | | Moderate | | Major | Catastrophic | |
| What is the risk level? | Low | | Medium | | High | | | Extreme |
| What *assumptions* influence this assessment? |  | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Consider the likelihood of the risk event under the current circumstances and potential consequences if it occurs. Identify any assumption that influence your assessment and consider whether these may be inaccurate or likely to change. | | | | | | | | |
| What is the likelihood? | Rare | Unlikely | | Possible | | Likely | Almost certain | |
| How severe are the consequences? | Insignificant | Minor | | Moderate | | Major | Catastrophic | |
| What is the risk level? | Low | | Medium | | High | | | Extreme |
| What *assumptions* influence this assessment? |  | | | | | | | |

## 3. Risk Approach

|  |
| --- |
| What kind of approach to this risk do you think is appropriate? *Identify whether accepting, reducing/sharing/transferring, controlling or avoiding the risk is appropriate and outline the reasons for your decision.*  *If reducing/sharing/transferring or controlling the risk, continue through all steps.*  *If accepting or avoiding the risk, go to Step 6.* |
|  |

## 4. Risk Treatment

|  |  |
| --- | --- |
| What strategies will mitigate this risk? *Outline the strategies you recommend to reduce or control this risk.* | |
|  | |
| Is there residual risk?*If yes, work through Steps 2-4 and summarise assessment, approach and control strategies for the residual risk.* | |
| **Residual risk assessment:** |  |
| **Approach to residual risk:** |  |
| **Additional risk treatment strategies:** |  |

## 5. Implementing Risk Controls

|  |  |  |
| --- | --- | --- |
| What will implementing risk controls involve and who will be responsible for them?*Detail the actions required to implement your risk treatment strategy.* *If further actions are required, use the ‘insert row’ function.* | | |
| **Action:** | **Responsible person:** | **Due date:** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 5. Monitoring and Ongoing Management

|  |  |  |
| --- | --- | --- |
| How will the management of this risk be monitored and maintained or updated?*Detail the actions required to monitor and update your risk treatment strategy.* *If further actions are required, use the ‘insert row’ function.* | | |
| **Action:** | **Responsible person:** | **Due date:** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Authority | | | |
| Who was involved in this document/plan? *Include names and positions.* |  | | |
| Date of plan: |  | | |
| Entered in Risk Register by: |  | Date: |  |
| Manager/CEO signature: |  | Date: |  |

# Appendix 3: Common Areas and Types of Risk

It is a good idea to provide a list of common or key risks for your organisation and its operating environment. Below is a generic list that can be adapted or replaced as appropriate.

Key risks for community organisations and their workers include:

**Physical health and safety risks**, including

Injury and illness risks to staff, and damage risks to the environment, the organisational site and assets

Risks posed by work activities, hazards in the work environment, the presence of animals or other people who could cause harm, and machinery (including vehicles)

**Human resources risks**, including

Risks associated with recruiting and employing inappropriate or underqualified staff

Workplace harassment and abuse

Harms to individuals and the organisation through inadequate human resources systems and processes

**Regulatory, financial and legal risks**, including

Failure to meet regulatory or compliance requirements

Inappropriate practices or inadequate risk management leading to financial costs and/or legal liabilities

Risk of fraud, particularly from people in responsible/management/governance positions

**Reputational risks**, including

Poor service delivery or publicity regarding inappropriate operational or governance practices that reduces trust in, funding for or donations to the organisation

The potential for actions of people associated with the organisation to reflect badly upon it

**IT risks**, including

Hacking and other cybersecurity breaches

Data losses

# Appendix 4: Business Continuity Plan[[4]](#footnote-5)

Your business continuity or disaster plan should include

* An **overview** summarising the plan, it’s objectives and key terms.
* A **risk management** plan, with identified risks, preventative actions, contingency plans, business insurance details, and data security and backup strategies.
* A **business impact analysis**, where you outline the potential impacts of disruption and how long recovery is likely to take.
* An **incident response plan** outlining how you will respond to relevant events, including checklists, procedures, information about emergency kits, roles and responsibilities, key contracts, and an event log. Review [Preparing and Incident Response](https://www.business.qld.gov.au/running-business/risk/incident-response-plan) and [Preparing for a Natural Disaster](https://www.business.qld.gov.au/running-business/natural-disaster/disaster-hub) for further details.
* Details about **recovery** methods, including a recovery plan, incident recovery checklist, contracts, details for making an insurance claim, and assessment tools for key issues (e.g., impacts upon staff). See [Developing a Recovery Plan](https://www.business.qld.gov.au/running-business/risk/recovery-plan).
* A plan for **rehearsing, maintaining and reviewing** the plan, including training and review schedules.

1. At time of writing, the current Quality Framework is V9.0. For the latest version of the Quality Framework and associated User Guides, contact DCSSDS 1800 034 022, [hsqf@qld.gov.au](mailto:hsqf@qld.gov.au) or [their website](http://www.dcssds.qld.gov.au/our-work/human-services-quality-framework). [↑](#footnote-ref-2)
2. This template focuses on preventative controls (controls that reduce the likelihood or impact if a risk event occurs). Depending on the risk understanding and established practices in your organisation, you may like to include additional detail, such as the potential for detective (controls that assist in identifying incidents/effects) and responsive (methods for reducing impacts after a risk event has occurred) and provide guidance on detective and responsive controls. [↑](#footnote-ref-3)
3. A determination that a control is reasonably practicable involves taking into account the likelihood, consequences, knowledge of the risk and controls, availability of risk elimination or control strategies, and whether the costs of elimination or control is “grossly disproportionate to the risk” ([WorkSafe Queensland](https://www.worksafe.qld.gov.au/__data/assets/pdf_file/0022/72634/how-to-manage-work-health-and-safety-risks-cop-2021.pdf), 2021, p. 7). [↑](#footnote-ref-4)
4. Adapted from information provided by Queensland Government [Develop a Business Continuity Plan](https://www.business.qld.gov.au/running-business/risk/continuity-plan). The Queensland Government also provides a [Business Continuity Planning Template](https://www.publications.qld.gov.au/dataset/business-continuity-planning-template/resource/63f7d2dc-0f40-4abb-b75f-7e6acfeae8f3). [↑](#footnote-ref-5)