Queensland Government

**Queensland Government Information Architecture**

**Best Practice Guide**

**Information Risk Management**

# DOCUMENT CONTROL

## Document Details

| | |
|---|---|
| Document Reference/Name: | BPG Information Risk Management V1.00.00 |
| Version Number: | V1.00.00 |
| Documentation Status: | ☐ Working Draft X BPG ☐ IS ☐ Archived |
| GIA Domain: | Information Management |
| **Next Scheduled Review Date** | November 2002 |

## Version History

| Version Number | Date | Reason/Comments |
|---|---|---|
| V0.00.02 | July 12, 2001 | Draft |
| V0.00.03 | September 28, 2001 | Revised Draft |
| V0.00.04 | October 22, 2001 | Revised Draft |
| V0.00.05 | October 26, 2001 | Executive Summary added and Finalised |
| V1.00.00 | October 31, 2001 | Issued |

# Contents

# Executive Summary

This Guide reflects the new approach being taken to the implementation of Information Standards. It is based on a risk management process, and is designed to satisfy whole-of-Government requirements as well as provide Agencies with greater flexibility.

Agencies can prioritise and plan for the implementation of all mandatory principles listed in each Information Standard through a risk assessment process. Where mandatory principles are not in place and their absence is determined to be of a high risk (i.e. major consequences and medium/high likelihood of occurrence) to Agency operations, these principles must be implemented within the timeframe set in the particular Standard, usually twelve months from the endorsement of the Standard. For all other risk categories, the Agency will only be required to develop an implementation plan, based on individual business priorities and resources.

The results of the risk assessment process, including the implementation timetable for complying with the mandatory principles, should be published in Agency information plans, or otherwise made accessible to staff in an appropriate manner.

# 1. Introduction

## 1.1. Background

The processes outlined in this Best Practice Guide, have been developed in line with the current *Australian Standard for Risk Management AS/NZS 4360:1999*, *HB 143:1999 Guidelines for managing risk in the Australian and New Zealand public sector* and the MAB-MIAC Advisory Board – *Guidelines for Managing Risk in the Australian Public Service (1996).*

The Guide also takes agency requirements in terms of responsibilities for establishing a policy and systems for risk management into consideration, in accordance with the *Financial Management Standard (1997) (S 83,84 & 85).*

## 1.2. Aim of this document

This guide has been developed to complement the Queensland Government Information Standards. It should be used as additional reference material by Queensland Government Agencies when assessing the impact of new or revised Information Standards and developing their timetable for implementation of mandatory principles.

This guide has been designed to assist agencies in developing an information risk management framework that will provide a systematic methodology for identifying, analysing, assessing, treating and monitoring risks in the information environment. A process for the development of business continuity planning in the information environment is also provided to assist agencies in their planning processes.

This document is provided for general guidance only. Agencies should consider the information provided in this Guide as reference material and interpret these guidelines in the context of their own information environment, developing agency specific information risk management processes.

## 1.3. What is Risk Management

Risk management is the process of implementing and maintaining appropriate management controls including policies, procedures and practices to reduce the effects of risk to an acceptable level. The principles of risk management can be directed both to limiting adverse outcomes and achieving desirable ones. The process involves identifying, analysing, assessing, treating and monitoring risk in all areas of Agency operations and business.

The *Financial Management Standard (1997)* outlines the elements for risk management as:

- Assessing the nature and extent of the risks associated with the agency's operations;
- Determining an acceptable level of loss with regard to identified risks;
- Determining how to treat each risk; and
- Monitoring and reporting the level of risk exposure and evaluating the need for insurance.

## 1.4. What is Information Risk Management

Information risk management adapts the generic process of risk management and applies it to the integrity, availability and confidentiality of information assets and the information environment.

Information risk management should be incorporated into all decisions in day-to-day operations and if effectively used, can be a tool for managing information proactively rather than reactively.

## 1.5. Organisation of this Document

The Information Risk Management Best Practice Guide provides:

- Principles regarding establishing a policy and planning framework for information risk management within agencies (refer Section 2);
- Guidance on using these principles in relation to the Queensland Government Information Standards (refer Section 3);
- An overview of the risk assessment process for Information Standards (refer Section 4);
- Step by step guide to the implementation process (refer Section 5); and
- Supporting references and definitions (refer Sections 6 and 7).

# 2. Principles

## 2.1. Agency Information Risk Management Policy

Agencies should have a policy in place for risk management, and risk management procedures should be embedded in everyday agency business operations. The information risk management policy should be a subset of the overall Agency risk management policy. Both should be communicated to staff to highlight the Agency's commitment to risk management.

The information risk management policy should be linked to Agency information management and information security policies providing the foundation for the Agency's strategic information management framework.

The information risk management policy should address issues including:

- The objectives and basis for information risk management in the agency;
- The link between information risk management and the agency's strategic planning processes;
- The range and extent of information risk management in the agency;
- What is considered an acceptable risk; and
- The responsibilities for information risk management.

## 2.2. Agency Information Risk Management Framework

The formal process of risk management can be applied to decision-making in all areas and levels of the Agency, including information management, security management, strategic, development and operational activities and projects. Risk assessment can be applied throughout the life cycle of any activity, however it is preferable that it be applied at the beginning of a project or operational activity to minimise risk.

The specific environment of each agency including its individual cultural, legal, service, economic and physical environment will determine the context for its management of risk. Effective information risk management practices should support and contribute to the overall agency security culture, operational and business planning processes.

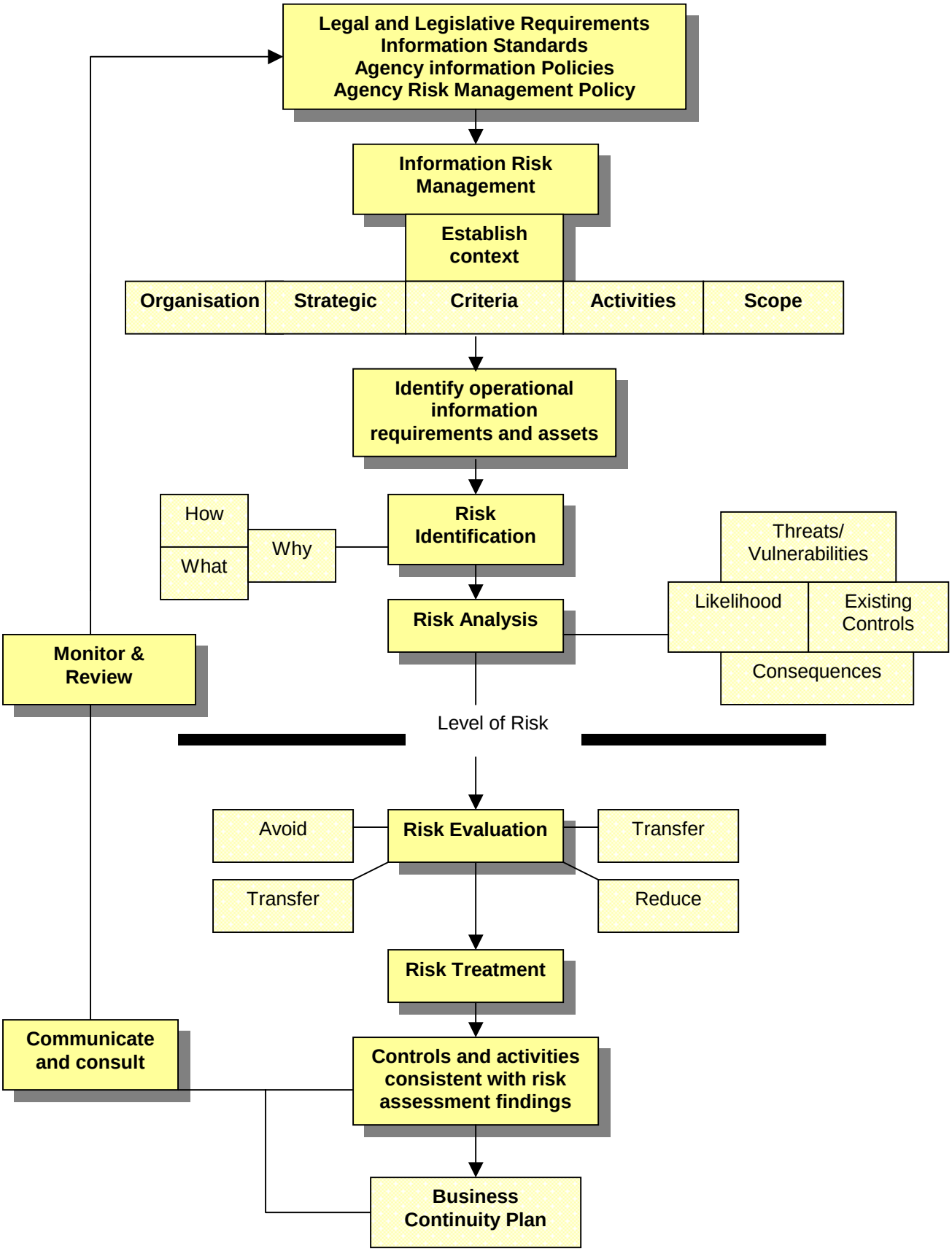
The implementation of successful risk management will reduce the probability of damaging or undesirable incidents, and minimise damage if they do occur. The boundaries and scope of information risk management need to be clearly established in terms of:

- Identifying the business processes that rely on the integrity and availability of information for essential agency decisions;
- Identifying and addressing the issues that need to be considered when assessing information security risks; and
- Identifying the information that needs to be protected and managed, and governance structures that need to be put in place for this information.

The decisions underpinning information risk management need to be consistent with Agency operational and strategic goals and priorities. Agencies also need to determine the critical factors that may support or weaken their ability to manage information securely.

A systematic and logical approach to information risk management is needed regardless of whether risk is being assessed for a large project implementation, for day-to-day operational controls and processes, or the implementation of new or revised information standards. A suggested information risk management process is outlined in the following diagram and further detailed in Section 5 of this Guide.

## Information Risk Management Process



## 2.3. Planning for information risk management

### *2.3.1. Commitment*

Visible management commitment is an important factor in the establishment of a risk conscious organisation. If implemented and managed appropriately, the information risk management process will not only identify and keep undesirable events from affecting agency performance, but, may also identify opportunities that may lead to gain or advantage.

Agency executive forums or Information Steering Committees should provide a significant role in coordinating and fostering a commitment to the implementation of information and security risk management.

To sustain commitment to the process and performance of information risk management, the process can also be formally linked to Agency outputs and performance measurements.

### *2.3.2. Responsibilities and Resources*

If information risk management is to be effectively implemented, the responsibilities for performing tasks and monitoring risks need to be clearly defined. Information risk management coordination falls across all areas of the agency, and all staff have some responsibility for managing risk in their business environments. Resourcing requirements for implementing, monitoring and reviewing information risk strategies, should be identified as a part of Agency business planning for information security and management processes.

### *2.3.3. Review*

The risk review processes should be clearly outlined in the Agency information risk management policy and reflect both its strategic and operational programs. Effective information risk management should deliver cost effective risk treatments and reflect the reality of Agency operations by establishing effective but achievable and realistic goals for the ongoing management of risk to Agency information.

The monitoring and review process is critical to the success of any information risk management strategy or activity, and appropriate review will ensure the ongoing usefulness of the information risk management plan.

### *2.3.4. Documentation*

An important part of information risk management is to ensure that each phase of the process is accurately documented. This will assist in demonstrating the accuracy of the process and provide valuable data for ongoing review processes and information planning activities. The extent of documentation will depend on the complexity and circumstances under which the risk management activity is being conducted.

# 3. Implementation

## 3.1. Agency information environment

Individual agency information profiles, business needs and processes, should guide the extent of the information risk assessment process. Therefore, information risk management will vary greatly across Queensland Government Agencies.

The steps of the information risk management process outlined in Section 5 of this Guide may be combined to provide a complete information risk management framework or where appropriate, relevant steps of the process can be used to conduct simple high-level risk analysis.

The process of managing risk should play an integral role within ongoing information resource management processes. For example, all existing and new systems should be assessed for risk exposure on a regular basis.

The growth of on-line service delivery and the implications of current and emerging legislative obligations provide an ongoing challenge. To ensure that threats and potential impacts to the Agency information environment are assessed adequately, risk review and assessment should be an ongoing activity.

## 3.2. Information Standards

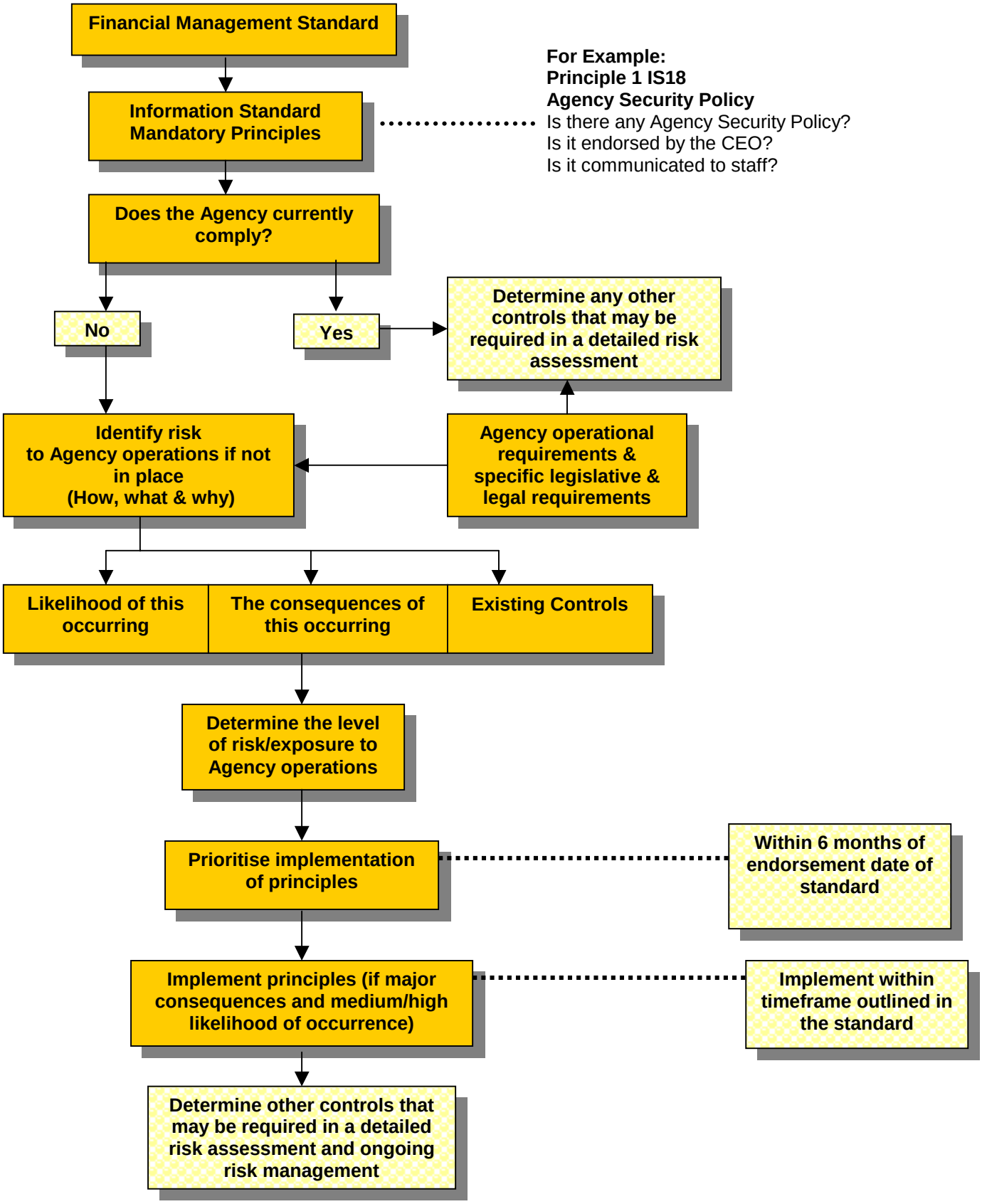
Timeframes for compliance with the mandatory principles of Information Standards will largely be determined by Agencies based on a risk assessment process. Agencies are required to conduct a high-level risk assessment within 6 months of the endorsement of each standard, to determine whether existing Agency controls and procedures meet the minimum requirements of the mandatory principles.

The results of the risk assessment must be prioritised, and a timetable established outlining the implementation of any mandatory principles not currently addressed in the Agency information environment. Where mandatory principles are not in place and their absence is determined to be of a high risk (major consequences and medium/high likelihood of occurrence) to Agency operations, these principles must be implemented as detailed in the particular Standard, usually set at twelve months from the endorsement of the Standard.

Agencies must prioritise and plan for the implementation of all mandatory principles and conduct ongoing detailed risk assessments to ensure that any additional measures are identified and implemented as required. These implementation timetables should be published in Agency information plans, or otherwise made accessible to staff as appropriate.

# 4. Risk assessment process for Information Standards

## 4.1. Preliminary high level risk assessment process diagram



## 4.2. Suggested steps

1. Develop project plan for Risk Assessment activity
2. Identify major areas of responsibility/impact for the mandatory principles of the Standard

   For example Information Standard 18 – Security - some of the responsibilities might be:

| Principle | | Responsibility |
|---|---|---|
| Principle 1 | Agency Security Policy | CEO, Information Steering Committee, Agency Program Managers, CIO |
| Principle 2 | Agency Security Framework | CEO, Information Steering Committee, Agency Program Managers, CIO, Agency Security Officer |
| Principle 3 | Information Asset Classification and Control | CIO, Information Management (IM) managers, IT Managers and relevant business area managers |
| Principle 4 | Personnel Security | CEO, Information Steering Committee, CIO, HR Managers, Agency Program Managers, IT Managers, IM Managers |

3. Develop a checklist of the minimum requirements for each of the mandatory principles.
4. Conduct workshop/meetings with each of those identified in step 2 to identify:
   - If the minimum mandatory controls are in place – if yes, are there any other controls that could be implemented to improve existing controls?
   - If the minimum mandatory controls are not in place – assess possible consequences, how these could occur and the likelihood of occurrences, taking into account all Agency business and legal obligations;
   - Determine the level of risk for those controls not in place; and
   - Prioritise and develop a timeframe for implementation of all controls not in place.
5. Plan and implement controls needed for those mandatory principles not in place that are exposing Agency operations to a high level of risk (major consequences and medium/high likelihood of occurrence) within the timeframe specified in the Information Standard.
6. Implement remaining mandatory principles that are of lesser impact to Agency operations in-conjunction with detailed risk assessments of the Agency information environment.
7. Implement ongoing risk management into the operations and planning of the Agency information environment.

# 5. Generic Implementation Process

The previous section deals with a suggested process for a preliminary and high-level risk assessment for Information Standards. This section focuses on the risk management activity in the context of an Agency wide information risk assessment. The same steps may also be applied to small scale and project orientated information risk management activities.

## 5.1. Context of Risk

### *5.1.1. Establish the organisational and strategic context*

In order to establish the context for information risk management within the Agency, the Agency's structure, capabilities, goals, strategic objectives and operational processes need to be understood. An understanding of these will assist in determining what is considered an acceptable level of risk to Agency information and information systems and form the foundation for the controls and risk treatments that will be required.

This part of the information risk management process involves:

- Understanding the Agency's strengths, weaknesses, threats and opportunities;
- Understanding key internal and external stakeholder objectives and perceptions; and
- Understanding the financial, operational, competitive, political, client, social and legal functions of the agency.

The Agency's information policies, together with its business and strategic plans, may also assist in determining the context for information risk management within the Agency.

### *5.1.2. Establish the risk management context*

#### 5.1.2.1. Scope

Before conducting the information risk assessment, the boundaries and scope of the process need to be established. Agencies need to consider if the information risk assessment is to be carried out on a whole of agency basis or in a phased approach.

Carrying out a risk assessment in a single risk analysis activity may not be practical. Prioritising the Agency's most critical information assets and processes and then continuing with further reviews of those with a lower priority may provide a simpler and more manageable course of action.

#### 5.1.2.2. Timing & location

Agencies need to consider the timeframes needed to complete the process and what locations are to be covered by the information risk management assessment.

#### 5.1.2.3. Stakeholders

Establishing the Agency's major stakeholders, both internal and external, is important in establishing the risk context. Individual stakeholders may change over time and should be reviewed as a part of the ongoing monitoring and review process. Stakeholder requirements may also change as a result of new risks and changes to other parts of the information and business environment.

#### 5.1.2.4. Resourcing

Resourcing requirements of the risk assessment process, including the responsibilities of the various business sections in relation to risk assessment process, need to be considered. The relationship between the risk management process and the business will need to be closely managed, to ensure a successful and comprehensive risk assessment.

Agencies should also consider whether internal or external resources are appropriate for conducting the process. This decision will be subject to the nature and scope of the activity.

The use of a risk management software package may also be an option for data collection and assessment and should be a consideration when defining required resources and tools.

### *5.1.3. Develop risk criteria*

Appropriate risk criteria needs to be established at the commencement of the information risk assessment process to determine how risk will be measured.

The criteria used for assessing risk in the information environment, should evolve around the three information security principles of:

- Confidentiality of information;
- Integrity of information; and
- Availability of information.

The risk criteria should also be guided by Agency legal and statutory obligations, Queensland Government Information Standards' mandatory requirements and client and stakeholder expectations.

Consideration needs to be given to the level of risk that the Agency is willing to accept. The acceptability of risks and the treatment of these risks may be based on, and defined according to, operational, technical, financial, legal, social or other relevant criteria. Agencies will need to determine the measurements for their individual requirements and examine all sources of risk to the information environment from the perspective of stakeholders both internal and external to the Agency.

Generally, the measures used to evaluate risk are based on:

- Client perception;
- Regulatory impacts;
- Business impacts; and
- Operational impacts.

#### 5.1.3.1. The criteria

As the review process evolves, the criteria may change, according to the risks identified and the type of analysis techniques used. The criteria should also be regularly reviewed in line with changes to strategic direction, business operations or information systems.

The table below outlines examples of possible information measurements and how they could be determined.

| Rating | Description |
|---|---|
| Very High | • Confidentiality and integrity of information must be guaranteed at all times.<br>• The failure of information systems could lead to total collapse of the agency or have severe consequences for the Government, its clients, partners and the public.<br>• Information is most likely classified as "Highly Protected". |
| High | • Information must be correct and any errors detectable and avoidable.<br>• Short periods of down time can occur, but processes must be carried out within a strict timeframe.<br>• In the event of system damage, critical areas can no longer function resulting in a considerable harm to the agency, the Government, its clients and the public.<br>• Information is most likely classified as "Protected". |
| Moderate | • Confidentiality of information must be guaranteed for internal use only.<br>• Minor errors in data can be tolerated and business activities will allow moderate periods of downtime.<br>• Information is most likely classified as "X-in Confidence". |
| Low | • Confidentiality of information is not required.<br>• Errors in data and downtime of systems will have minor impact to the agency.<br>• The consequence of damage is only a minor disruption to the agency, the Government and its clients, with limited impact on the public. |

#### 5.1.3.2. The structure

The information risk assessment process requires a logical structure to ensure that significant risks to the information environment are not overlooked. The structure of the review will vary according to the scope and nature of the risk assessment activity. The following activities should be carried out when establishing the structure for identifying risks in the information environment:

1. Information Assets

   When conducting a risk assessment for the information environment it is crucial that all major information assets are identified and an inventory formulated. Details on this can be found in Information Standard 18 – *Information Security – Principle 3 Asset Classification and Control.*

2. Information Classification

   To establish the appropriate protection and risk management strategies for Agency information, sensitive information needs to be identified and classified. Details on this and classification schemes for agency information can be found in Information Standard 18 – *Information Security – Principle 3 Asset Classification, Control,* and *Attachment B* of the standard.

3. Information Requirements

   Establishing the Agency's requirements for information and systems in its business operations is also important in determining the risk criteria. Determining the business processes, and the dependencies and relationships between these processes and the information holdings, systems and resources, is important. Once documented, this data can also be used in Agency Business Continuity processes. Refer to Section 4.8.2 for details of this process.

### *5.1.4. Suggested Documentation for Context of Risk Phase*

To ensure the accuracy of the process and provide data for ongoing risk review, it is suggested that the following documentation should be produced in this phase of the risk management process:

1. Scoping document – For example, risk project assessment boundaries, location, timing, stakeholders, resourcing requirements;
2. Listing of risk criteria – Ranking of risks and description of what constitutes the criteria for risks;
3. Listing of elements to be assessed – For example, inventory of information assets and key information processes.

## 5.2. Identification of Risks

Having identified the information assets, information and information processes that are important to the Agency, the risk events that could impact upon them need to be established.

The questions .. what can happen? how and why could it happen? .. need to be applied to each of the information elements and systems identified. At this point in the process, it is crucial to the overall success of the risk assessment that all potential risks to the information environment are identified and documented including those internal and external to the Agency.

### 5.2.1. What can happen

Risk to information is the likelihood of an adverse event and the impact that the event would have on the Agency information. Each potential source of risk and the areas or elements that could be impacted by the risk event need to be documented.

Generic sources of risks and impacts are typically categorised under the following but are relative to the nature and scope of the risk assessment.

**Sources/Threats to Agency information**

- Commercial/contract, legal
- Economic
- Technological
- Environmental/ natural events
- Human behaviour/ individual activities
- Operational processes

**Impacts/Exposure**

- Loss of revenue
- Incurring of costs (direct and indirect)
- Assets (information, personnel, equipment etc)
- Provision of service / Performance
- Loss of Reputation

Agencies should re-assess risk sources and impacts on an ongoing basis to ensure that any changes to the business and information environment are accurately reflected in the information risk management plan.

### 5.2.2. How and why it can happen

When a list of risks and impacts has been identified for information assets and systems susceptible to risk, the next step is to identify and document the possible causes and circumstances for each of the risk events.

Agencies should re-assess these on an ongoing basis to ensure that changes to the business and information environment are reflected.

### 5.2.3. Tools

Some of the methods that may be used to gather the data on information risk event sources, impacts, causes and circumstances, could include:

- Interviews/workshops;
- Audits;
- Survey’s or questionnaires;
- Past risk reviews;
- Industry data; and
- SWOT analysis.

There are numerous types of methodologies that can be used to present the collected data. Including flowcharts and specialised software packages, all are similar in their approach. Agencies need to decide which method best suits the individual Agency culture and the scope of the risk assessment they are conducting.

### *5.2.4. Suggested Documentation for the Risk Identification Phase*

To ensure the accuracy of the process and provide data for ongoing review processes, it is suggested that the following documentation should be produced in this phase of the information risk management process.

1. Listing of all information assets, systems and processes with all potential risk sources, risk impacts, risk causes and consequences of the risk event.

Refer to Attachment A – Risk Register template for suggested format.

## 5.3. Analysis of Risks

This step of the information risk management process focuses on the extent of the consequences that would arise from a risk event and the likelihood of that event occurring. These are combined to create the level of risk. This data then allows the Agency to determine minor and acceptable risks to information, and separate them from those considered to be major and unacceptable risks.

### *5.3.1. Existing controls*

Existing information controls, operational procedures and systems need to be identified and documented, including their strengths and weaknesses. This data may be gathered through a variety of methods including inspections and assessments or can be gathered during the risk identification process.

### *5.3.2. Consequence and likelihood*

The likelihood and consequences of a risk event need to be looked at from the perspective of possible consequences with existing controls in place, and possible consequences if these controls weren't in place.

There are various ways to gather this information and formulate the level of risk, including using past experience and risk review data, industry experience, specialist or expert advice, interviews and workshops.

#### 5.3.2.1. Analysis methods

There are various methods for determining the level of risk. It may be assessed using qualitative, semi-quantitative or quantitative methods.

| Method | Process |
|---|---|
| Qualitative | Involves using specific descriptive scales to determine the extent of the consequences and the likelihood of an event. |
| Semi-quantitative | Involves assigning numbers to qualitative scales to determine the extent of the consequences and the likelihood of an event. |

| Method | Process |
|---|---|
| Quantitative | Involves using numerical values to determine the consequences and likelihood of events. |

Qualitative analysis is more often used when initiating a risk assessment process to obtain an indication of the level of risk present, such as assessing the implementation of Queensland Government Information Standards. A more detailed quantitative analysis can then be conducted if a high level of risk is identified. Examples of simple scales for performing a qualitative analysis are described below, however these measures should be adjusted to suit the requirements of the risk assessment being conducted.

**Consequence Scale**

| Measure | Description |
|---|---|
| **Major** | Major problems would occur and threaten the provision of important services resulting in significant financial loss. |
| **Moderate** | Services would continue but would need to be reviewed or changed. |
| **Minor** | Effectiveness of services would be threatened but dealt with. |
| **Insignificant** | Dealt with as a part of routine operations. |

**Likelihood Scale**

| Measure | Description |
|---|---|
| **High** | Is expected to occur in most conditions (1 or more times per year). |
| **Medium** | The event will probably happen in most conditions (2 years). |
| **Possible** | The event should happen at some time (5 years). |
| **Unlikely** | The event could happen at some time (10 years). |

**Levels**

| Measure | Description |
|---|---|
| **High** | Likely to threaten the effectiveness of the organisation financially and politically if not treated. |
| **Moderate** | Likely to threaten the running or services of the organisation and can be managed by implementing new or modified controls. |
| **Low** | Unlikely to threaten and can be managed through routine controls. |

The next step involves matching consequences to likelihood to determine levels of risk.

**Level of Risk**

| LIKELIHOOD | CONSEQUENCES | | | | |
|---|---|---|---|---|---|
| | **Insignificant** | **Minor** | **Moderate** | **Major** | **Catastrophic** |
| **Almost Certain** | M | H | H | E | E |
| **Likely** | M | H | H | H | E |
| **Possible** | H | M | H | H | E |
| **Unlikely** | L | T | M | M | E |
| **Rare** | L | L | M | H | E |

**Legend**
E: extreme risk; immediate action required
H: high risk; senior management attention needed
M: moderate risk; management responsibility must be specified
L: low risk; manage by routine procedures

### *5.3.3. Analysis approach*

The recommended approach when analysing risks to the information environment is to firstly conduct a high level analysis to identify and remove common and trivial risks from further analysis. These risks can normally be dealt with using existing controls and processes.

A high level analysis focuses on the information systems and information handling more from a business point of view. Risks that pose an unusual or serious threat, including areas where there are inadequate controls, should have a more detailed analysis conducted.

If any of the following issues present a high risk, a detailed analysis should be conducted:

- There is a high dependence on the Agency's ability to conduct its business despite the failure of a system or loss of information integrity, availability or confidentiality;
- There is a high dependence of the Agency on the information or system to achieve its business objectives;
- There is a high level of commitment in maintaining, replacing or developing information or systems; or
- There is a high $ value of a system or information asset to the Agency.

A more detailed analysis looks in depth at the risk in terms of the threats and vulnerabilities that could impact on information systems, assets or processes. The level of risk is usually determined by analysing the relationship between threats and vulnerabilities using a quantitative method (refer following table).

| Rating | Description |
|---|---|
| 5 | Threatens the provision of critical services, which threaten business and political capabilities |
| 4 | Major services would be significantly affected |
| 3 | Loss of services would impact short term business |
| 2 | Inconvenient but no great business impact |
| 1 | Possibly not a major activity needs to be reviewed |

### *5.3.4. Suggested Documentation for Analysis Phase*

To ensure the accuracy of the process and provide data for ongoing review processes, it is suggested that the following documentation should be produced in this phase of the risk management process.

1. Explanation of risk measurement scales and analysis methods;
2. Assessment of existing controls
    - Likelihood of event with and without control
    - Severity of consequences with and without controls;

Refer to Attachment A – Risk Register template for suggested format.

## 5.4. Evaluation of Risks

This step in the information risk management process compares the level of risk for consistency with the risk criteria established earlier in Step 1 of the process (Refer to Section 5.1.3). Risks are prioritised based upon what is and what is not determined to be an acceptable risk to the Agency.

The importance of the information asset, group of assets or process in the agency's overall operations, needs to be considered in evaluating the risk. The reasons why a risk may be considered acceptable include:

- The level of risk is insignificant or low enough that treatment is not viable;
- There is no available treatment;
- The cost of treatment outweighs the benefits in treating the risk (normally a lower ranked risk); and
- The opportunities associated with the activity outweigh potential incidents or threats.

The risks that are not considered acceptable will require controls or countermeasures to be planned and documented.

### *5.4.1. Information Asset Value*

Determining the value and significance of information assets is important in determining risk priorities. The monetary value assigned to an asset can be used to determine the level of protection and the cost/benefit of protection. The monetary value given to an asset (or group of assets) should be based on:

- The cost of the original and/or replacement system;
- Damages arising from violation of regulatory or statutory obligations;
- Potential loss of revenue; and
- Embarrassment and damages arising resulting from misuse, disclosure or destruction of information.

When assessing the value of information assets a qualitative scale of low, moderate, high and very high can be used. The impact of potential damages should also be considered, and could result from:

- Violations of regulatory, statutory or contractual obligations;
- Degradation or loss of agency business and services;
- Loss of reputation;
- Breach of confidentiality;
- Financial loss; and
- Endangerment of personal or environmental safety.

### *5.4.2. Documentation*

To ensure the accuracy of the process and provide data for ongoing review processes, it is suggested that the following documentation should be produced in this phase of the information risk management process.

1. Listing of acceptable risks including reason for risk being deemed acceptable;
2. Listing of unacceptable risks in priority order.

Refer to Attachment A – Risk Register template for suggested format.

## 5.5. Treatment of Risks

### *5.5.1. Treatment Options*

Agencies need to manage risk to a point where the security of information and operations is acceptable and the cost/benefits of treating the risk are also acceptable. Broadly speaking, the treatment options available range from avoiding the risk completely, accepting the risk and controlling it, through to transferring the risk to another party.

#### 5.5.1.1. Risk aversion

The treatment for the risk may be, where practical, not to conduct the activity that creates the risk. However, it should be noted that in some situations, avoiding a risk could cause other risks to become significant. Therefore, the decision to adopt this option should be carefully analysed. Where risk aversion relates to the implementation of mandatory requirements of Information Standards, Agencies should refer to the exemption process outlined in Information Standard 1 - *Framework for the Management of Queensland Government Information Standards* (under review).

#### 5.5.1.2. Transfer of risk

Transferring the risk to another party either in full or sharing the risk may be an option in some scenarios. When adopting this solution, risks should only be allocated to the party that can provide the most effective control of the risk.

#### 5.5.1.3. Retaining the risk

If the analysis establishes that, taking existing controls into account, the level of risk remains unacceptable, and it is not practical to avoid or transfer the risk, agencies should bear the responsibility of the risk. Controls and detection measures should be then implemented appropriately.

#### 5.5.1.4. Reduction of likelihood or consequences

The likelihood of a risk may be reduced through additional controls, which may minimise the frequency of, or opportunity for error, by way of policies and procedures, quality assurance, training etc.

### *5.5.2. Assessing treatment options and controls*

When assessing the best option for treating risks in the information environment, Agencies should weigh-up the cost of implementing controls with the benefits provided by them. Generally, the cost of treatment should be proportionate to the benefits provided.

It may also be necessary to take political or social costs and benefits into consideration in some situations. A cost/benefit analysis comparing the total cost of the risk impact and the cost of managing the risk should be undertaken.

Applying one risk treatment will not always provide a complete solution. In some cases, agencies may need to apply a combination of options. The option to reduce the likelihood and consequences of an event together with transferring some of the residual risk and maintaining some of it within the agency may be adopted in some situations.

When considering controls to manage risk to the information environment the main issues that need to be asked are:

- Who is responsible for treating and managing the risk?
- What are the current controls in place and are there any further safeguards that could be implemented to reduce the risk?
- Are the existing or proposed controls cost and resource effective in light of the value of the asset and the consequences of an undesirable event?

When selecting appropriate controls or reviewing existing controls, consideration should also be given to the type of protection measures that can reduce the level of vulnerability.

In terms of compliance / non compliance to Queensland Government Information Standards, Agencies need to treat, defer or show reason for seeking an exemption to the mandatory requirements.

Controls in terms of information security control and risk treatment can be categorised in terms of:

- **Prevent/Protect** A control designed to prevent damage or impact to the information environment from an action or event occurring;
- **Detect** A control that provides notification that something has gone wrong;
- **Correct/Recover** A control that has the ability to correct identified problems;
- **Deter** Control to avoid or prevent an undesirable event.

### *5.5.3. Preparing and implementing plans*

Agencies should prioritise and plan the implementation of controls identified to protect the information environment from risk events. The priorities should be ranked according to the outcomes of a cost benefit analysis, the business priorities and risk implications and impacts.

A plan to treat the risks of the Agency information environment should be documented, outlining responsibilities, timing of implementations, expected outcomes, budgeting, monitoring and performance indicators and how the ongoing risk and security situation will be monitored.

### *5.5.4. Suggested Documentation for Treatment of Risks Phase*

To ensure the accuracy of the process and provide data for ongoing review processes, it is suggested that the following documentation should be produced in this phase of the risk management process:

1. Listing of options for treatment;
2. Risk action plan for implementing risk treatments; and
3. Identification of any possible residual risk.

## 5.6. Monitoring and Review

The ongoing review of the information risk environment is critical to overall agency information management, security and continuity of business. Due to the changing nature of the information environment, new risks will continue to be introduced on an ongoing basis. Changes to the information and business environments may affect the likelihood and consequences of risks and necessitate a change to existing controls.

Therefore, it is important that agencies repeat the risk assessment process on a regular basis and that information risk review is fundamental to overall Agency risk management practices.

To ensure that risk to the information environment is regularly reviewed, agencies should include risk assessment and review as an ongoing activity in corporate and business planning activities. The role of Agency Internal Audit and information security roles should be actively involved in the monitoring and review of Agency risk. Refer to Information Standard 18 – *Information Security Section 5.2 Roles and Responsibilities* for further details.

## 5.7. Communication and consultation

Key stakeholders and management need to be actively involved in the initial planning of information risk management activities and in any ongoing risk reviews.

Initial activities and ongoing risk review, should include participation from the operational sections of the Agency. The involvement, education and awareness of staff in identifying and reporting possible risks to the information environment should be clearly outlined in Agency policies for the management of risk within their organisation.

## 5.8. Business continuity

### *5.8.1. The business continuity management process*

The management of business continuity in the information environment is an integral part of the risk management framework. Business continuity is an adverse risk event and the activity of business continuity planning is a risk treatment.

The current Information Standards that require Agencies to have business continuity mechanisms in place include: Information Standard 24 *Policies for the management of Information within Government* and Information Standard 18 *Information Security*. This section of the *Information Risk Management Best Practice Guide* has been designed to assist Agencies in complying with these standards.

The primary objective of information risk management is to prevent undesirable events from occurring. However, when a risk to the information environment becomes a reality it is necessary to have treatments in place that will limit the impact on Agency information and systems continuity and business operations and service.

The events or interruptions that are of concern from a business continuity focus are referred to as outages. An outage will create significant disruption to, or loss of, key information, processes and systems. The impact of that outage focuses on consequences to the continuity of Agency operations. The duration of interruption or outage to Agency operations becomes the major criteria for assessing the impact.

The information in this section focuses on providing a broad framework for implementing business continuity management and planning in the information environment.

### *5.8.2. Identification of key business processes*

#### 5.8.2.1. Prioritise key business processes

Key business processes that require information and information systems need to be ranked in order of importance to reflect the significance of the process in assisting the Agency to achieve its business objectives and to deliver its outputs. The ranking may consider:

- the Agency's ability to meet legal and statutory obligations for service delivery;

- the Agency's ability to meet client and stakeholder expectations; and
- the financial implications to the Agency in providing essential business operations.

To formulate and determine the ranking, the use of structured interviews or workshops including executive and senior management are recommended tools. Defining the importance of the information in terms of its business use will also assist in categorising and ranking the processes. For example:

| Classification | Process types |
|---|---|
| Strategic information and information processes | For example, organisational structure and development, designing of outputs, structure, planning, audit. |
| Operational information and information processes | For example, external service provision, policy advice. |
| Support information and information processes | For example, internal service provision; purchasing, payments, payroll, human resources, information and technology services. |

#### 5.8.2.2. Identify information activities

The next step is for each business unit or service area to identify the information related activities that support their key business function and map any interdependencies between these. The activities may be performed by a single operational area or may be a combination of a number of areas including external providers.

#### 5.8.2.3. Identify resources

Having identified the activities that support the key information processes, the resources required to support these activities should then be identified.

These could include:

- Staff that are critical to the success of the activity;
- Infrastructure used to deliver services and produce outputs (for example, buildings, communication networks);
- Assets which are used by the people and the processes as part of the activity; and
- Funding.

### *5.8.3. Business impact analysis (BIA)*

A Business Impact Analysis (BIA) is conducted for all key business processes identified in the previous step. The analysis establishes the recovery priorities and determines the length of time or maximum acceptable outage (MAO) that the Agency can be without key business processes before corrective actions need to be taken. The process also looks at any activities and systems that if unavailable would create a danger to the Agency's survival and its business.

#### 5.8.3.1. Determining the MAO

To establish a maximum acceptable outage (MAO) for each business process, a scale or framework needs to be formulated to assess the overall impact of loss of a process and the impact of losing the supporting activities and resources. The MAO sets a point at which there would be a major impact on activities and resources resulting in failure of the business process.

A scale similar to that used in determining the consequences in the risk management framework could be used. For example:

| Measure | Rating | Description |
|---|---|---|
| Catastrophic | 5 | Threatens the provision of critical services, which threatens business and political capabilities. |
| Major | 4 | Major services would be significantly affected. |
| Moderate | 3 | Loss of services would impact short term business. |
| Minor | 2 | Inconvenient but no great business impact. |
| Insignificant | 1 | Possibly not a major activity, needs to be reviewed. |

These ratings should then be applied to resources and activities and the impact on them. The level of impact can be set at the same as used in the risk management process, based around the following criteria:

- Agency Outputs;
- Resources;
- Agency Reputation;
- People / Community; and
- Compliance.

The MAO for each activity and resource is scored based on the impact of its unavailability or loss.

### *5.8.4. Continuity treatments*

This step forms the foundation of the business continuity plan by identifying the actions required to minimise the effects of disruptions to critical business process where a MAO has been established. The step also identifies what is needed for continued availability of critical processes and resources during an outage.

The process involves reviewing existing recovery controls such as data backup, to evaluate their effectiveness in the event of a disaster. This process can also be used to assist in identifying recommendations for improvement to current business process and therefore reduce the likelihood of the outage in the first place.

#### 5.8.4.1. Identify and evaluate options

This step identifies and evaluates treatments for each of the key business processes identified in the BIA process. Treatment options can be those that:

- Reduce exposure, impact of or loss of the processes and supporting resources; and
- Provide alternate activities/processes and resources and plans to recover from an outage.

When evaluating alternate activities and/or resources, it is critical that the following resources are addressed in respect to each identified disruption.

| Resource | Description |
|---|---|
| **People** | ▪ Loss of key personnel - human resource issues, administration procedures, replacement and training of staff and loss of knowledge.<br>▪ Disruption of personnel - the absence of facilities, telecommunications, information systems and business processes.<br>▪ Affects - approaches to communication, psychological effects of the disruption on staff morale. |
| **Facilities** | ▪ Assessment of facilities - damage, salvage and restoration.<br>▪ Equipment and resources - those within the premises.<br>▪ Restoration or relocation - continuing essential business activities.<br>▪ Backup services - agreements and activities required to keep the essential services functioning.<br>▪ Documentation - procedures to support business facility recovery and restoration. |
| **Telecommunications** | ▪ Recovery - loss or interruption to internal/external voice and data communications.<br>▪ Alternate - design or services redundancy.<br>▪ Spare equipment and software.<br>▪ Uninterruptible power supplies (UPS). |
| **Information systems** | ▪ Physical records - storage facilities, distribution, handling and processing of information.<br>▪ Electronic records – computer and network facilities, off-site storage of critical data.<br>▪ Preventative controls. |

| Resource | Description |
|---|---|
| **Communications** | ▪ Media communications.<br>▪ Staff communications. |

#### 5.8.4.2. Select alternate activities and resources

To ensure that the recovery options not only satisfy business needs but also are cost effective, a comprehensive costing analysis should be done. The costing should include direct costs (spare or extra equipment) and indirect costs (costs to establish and maintain new equipment).

In most situations, it is possible to defer all or most of the costs until the continuity plan is put into practice. The alternate processes and resources should be documented.

### *5.8.5. Implement continuity treatments*

After the selection of continuity and recovery treatments, the next step in the process is to implement and document the procedures and recovery arrangements to support recovery from a disruption to business.

#### 5.8.5.1. Implement preliminary controls

Using the data from the BIA this step identifies the resources needed to recover and restore critical and essential business processes.

In the event of an incident where the BCP needs to be put into action, information relating to the business processes, resources and activities will need to be available. Storing recovery procedures and resources off-site will ensure information and supplies essential to continued business are available when required.

It is also important that the recovery procedures are continually aligned and updated with operational activities to ensure successful recovery and resumption of current business processes. Arrangements and details for alternate facilities and resource suppliers should be included in the documentation for the implementation of the recovery treatments.

The issue of records management continuity extends beyond the resumption of business processes and can have long-term implications for the agency. Document management procedures for the management of physical and electronic records should be in place and considered when formulating the BCP.

#### 5.8.5.2. Prepare the Business Continuity Plan (BCP)

The format and content of the BCP is extremely important. The plan needs to be easy to read and follow. The plan should start at the point the plan needs to be activated, guiding the reader through each step in the response and recovery process. There should be space left in the plan document for the recovery processes and issues to be recorded. This will also allow for a review and debriefing after the event.

The plan needs to identify and address all stages of the recovery process. These phases are:

Response: From the declaration of a disaster until critical systems and processes have been re-established;

Interim: The details on alternate processes and resources; and

Restoration: Return to normal systems and business operations.

The Agency BCP is a compilation of individual business areas' recovery and contingency plans brought together as a high-level coordination and management plan. The plan deals with business disruption from the initial disaster response up to where normal business is resumed.

Quality assurance reviews of the Plan throughout preparation and its life are recommended to ensure that content remains relevant with the current business operations, processes and outputs.

The details to be included in the BCP will vary and agencies should determine their individual needs. The general issues that need to be addressed in the Plan include:

1. Roles and responsibilities within the Agency and of the recovery teams

   Suggested roles to include in the continuity recovery organisation are:

   - Recovery coordinator – coordinates the recovery and reports directly to the DG/CEO;
   - Service recovery and management teams – business service areas teams responsible for implementation of plans and recovery of systems;
   - Recovery plan support – resources necessary to support recovery plans including facilities, human resource management and communication plans;
   - Team leader – for each recovery area, a team leader should be identified in the plan as being responsible for that area.

2. Event log

   The plan should include space for an event log to use for recording details of the event reviewing and debriefing after normal operations have been established. The log can also provide a common description of the event for briefing the recovery teams or the media.

3. Management recovery plan

   The management recovery plan integrates all individual service/operational area recovery plans into a coordinated plan for the Agency as a whole. The plan should outline the criteria for activating the plan and the issues that the Agency needs to respond to, following the announcement of a disaster. This section of the plan should address the following issues:

   - Disaster escalation process;
   - Team assembly directions
   - Recovery phase steps;
   - Interim phase steps; and

- Restoration phase steps.

4. Service/operational area recovery plans

   A major component of the BCP is to put together the individual recovery plans for each of the service/operational areas. Individual plans should identify roles and responsibilities, team assembly directions, interim processing steps, restoration phase steps. Overlaps or interdependencies of service recovery across service areas should also be documented in each area's plan, but assigned to one recovery team.

5. Reference Procedures

   Details of information, supplies, equipment, inventories and associated vendor contact details, including vendor contacts and agreement details.

6. Technical recovery items

   Details of server and communication configurations and IT recovery plans.

7. Contact Lists

   A comprehensive contact list should be established and maintained. Contact lists should be kept current and include emergency service contacts, recovery team contacts, recovery team participants, key stakeholders and key staff lists with after hours contact details.

8. Inventory

   Details of supplies and resources needed, including budget and additional resource details. Supplies required should be stored offsite.

9. Limitations

   Details of any issues that may limit the success of the recovery process, including those effecting the people, facilities, information systems and communication aspects.

10. Testing and review

    Details of the testing schedules and review timeframes for the plan.

### *5.8.6. Test and maintain the plan*

To ensure that the plan reflects the Agency's current objectives and key business functions and outputs, it is necessary to review its relevance on an ongoing basis. The recommended timeframe for testing all major components of the plan is on an annual basis. The plan should always be amended with the results and finding of each test.

Each component needs to be independently tested and requires the commitment from management to ensure availability of resources. It is not recommended the plan be tested as a whole.

There are various ways to approach the testing of the plan. One possible approach is to have each recovery team go through the recovery process of their operations, with the other teams challenging them pointing out any weaknesses. Testing should include verifying, validating and rechecking the availability of resources, data, supplies and/or other hardcopy documents, equipment, vendors, and facility arrangements.

A structured walk through of the plan may also be used. This type of test requires the development of a disaster scenario and the acting out and verification of procedures through a simulated recovery process.

Ongoing responsibilities should be defined to ensure the ongoing maintenance of the plan. Individual recovery plans should be regularly updated, with administrative procedures developed to provide for periodic testing and documentation maintenance of the service area recovery plan. Where components of the plan could be affected by modifications to the operational or business environment, the changes should be evaluated using a BIA, which looks at any new issues and relationships. If the plan needs to be changed, testing may also be necessary.

# 6. References/Supporting Documentation

**Current Government Information Standards:**

24 Policies for the Management of Information Within Government (PDF) (Word)

31 Retention and Disposal of Government Information (PDF) (Word)

33 Information Access and Pricing (PDF) (Word)

38 Use of Communication and Information Devices (PDF) (Word)

**Other Supporting Documentation**

*Queensland Financial Administration and Audit Act 1977*

*Queensland Financial Management Standard 1997*

| | |
|---|---|
| Australian Standards – | *AS/NZS 4360:1999* *Risk Management* |
| Australian Standards – | *HB:143:1999* *Guidelines for Managing Risk in the Australian and New Zealand Public sector* |
| Australian Standards – | *AS/NZS 4444.1: 1999* *Part 1: Code of practice for information security management* |
| Australian National Audit Office | *Business Continuity Management - Keeping the wheels in motion – Jan 2000* |
| Defence Signals Directorate - | *Australian Communications Electronic Security Instruction 33 (ACSI 33)* |
| Commonwealth Government - | *Protective Security Manual Australian Government Publishing Service, Canberra; 2000* |
| Guidelines for Managing Risk in the Australian Public Service - | *MAB/MAIC Report No.22 October 1996* |
| Guidelines on Risk Management & Insurance | Queensland Treasury – 1994 |

# 7. Definition of Terms

| | |
|---|---|
| **Availability** | Ensuring that information and vital services are available to users when required. |
| **Business Continuity Plan** | Plans which describe a sequence of actions, and the parties responsible for carrying them out in response to a series of identified risks, with the objective of restoring normal business operations as quickly as possible. |
| **Classification** | The systematic arrangement of information into logical categories. |
| **Confidentiality** | Protecting sensitive information from unauthorised disclosure or intelligible interception. |
| **Controlled Environment** | Environment where *security measures* have been implemented. |
| **Information** | A collection of data in any form which is maintained by an Agency or person, and which may be transmitted, manipulated, and stored by the information system. |
| **Information Assets** | The resources associated with information systems. |
| **Integrity** | The assurance that information has been created, amended or deleted only by the intended authorised means. |
| **Networks** | Include communication capability that allows one user or system to connect to another user or system. |
| **On-line** | Use of the Internet for information service delivery. |
| **Probability** | The likelihood of a specific outcome, measured by the ratio of specific outcomes to the total number of possible outcomes. |
| **Records Management** | Records management is the task of effectively and efficiently managing records from their creation to disposal. |
| **Residual Risk** | The remaining level of risk after all risk treatment measures have been taken. |
| **Risk Analysis** | A systematic use of available information to determine how often specified events may occur and their likely consequences. |
| **Risk Assessment** | An evaluation of system assets and their vulnerabilities to threats, including potential losses that may result from threats. |
| **Risk Avoidance** | Not becoming involved in a risk situation by ceasing the activity or process |
| **Risk Control** | The provision of appropriate policies, procedures and standards of protection to avoid or minimise identified risks. |
| **Risk Identification** | The process of determining possible outcomes or occurrences associated with an activity, why these might occur and how. |

| | |
|---|---|
| **Risk Level** | The level of risk calculated as a function of likelihood and consequence. |
| **Risk Management** | The systematic application of policies and practices to the tasks of identifying, analysing, assessing, treating and monitoring risk. |
| **Risk Retention** | Retaining the responsibility for loss. |
| **Risk Transfer** | Shifting the responsibility for loss to another party. |
| **Risk Treatment** | Selection and implementation of appropriate management options for dealing with identified risk. |
| **Security Incidents** | Security incidents may include, but are not limited to, any act that:<br>• Does not comply with the requirements of this policy;<br>• Exposes Queensland Government to actual or potential monetary loss through the compromise of security;<br>• Involves the disclosure of confidential or private information or the unauthorised use of Queensland Government information;<br>• Results in the loss of Queensland Government information; or<br>• Involves the use of hardware, software or information for unauthorised or illicit purposes, which may include violation of any law, regulation or reporting requirements of any law enforcement or Government body. |
| **Security Controls** | Hardware, programs, procedures, policies and physical safeguards which are put in place to assure the integrity and protection of information and the means of processing and accessing it. |
| **Standards** | A published document, which sets out technical or other specifications necessary to ensure that a material or method will consistently do the job it, is intended to do, i.e. ‘what’ must occur to achieve the desired result. |
| **User** | A person who employs a computer system and its facilities to undertake a task. |

# 8. Attachment A

**Risk Register**

| Risk Description | Consequences of the Event | | Existing controls | Consequence rating | Likelihood rating | Level of risk | Risk priority |
|---|---|---|---|---|---|---|---|
| | Consequences | Likelihood | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |