NSW RURAL FIRE SERVICE

# POLICY P7.1.10
# ENTERPRISE RISK MANAGEMENT

| ITEM | DESCRIPTION |
|---|---|
| Version Number | v3.0 |
| SOPs | › SOP P7.1.10-1 Risk Management Process<br>› SOP P7.1.10-2 Business Continuity<br>› SOP P7.1.10-3 ICT Disaster Recovery |
| Owner | Executive Director People and Strategy |
| Contact | Director Strategy and Programs |
| Approved Date | 20 September 2022 |
| Effective Date | 20 September 2022 |
| Next Review Date | 20 September 2027 |
| Document Control | Electronic - Printed Copies are Uncontrolled |

## 1 Purpose

1.1 This policy outlines the NSW RFS commitment to contemporary risk management practices that facilitate consistent risk-based decision making and support the achievement of NSW RFS strategic objectives in an inherently dangerous, uncertain and volatile context.

1.2 The NSW RFS manages risk in accordance with the relevant legislation and standards, including:

a. NSW Treasury Policy Paper TPP20-08 Internal Audit and Risk Management for the General Government Sector;

b. NSW Treasury Policy Paper TPP12-03 Risk Management Toolkit for the NSW Public Sector;

c. The *Government Sector Finance Act 2018*; and

d. Australian Standard AS ISO 31000:2018 Risk management – Guidelines.

1.3 This policy establishes and maintains an enterprise risk management framework for the NSW RFS.

## 2 Definitions

2.1 Definitions listed in the NSW Treasury Policy TPP20-08 and Australian Standard AS ISO 31000 – 2018 shall be applicable unless otherwise stated. For the purpose of this policy document, the following additional definitions apply:

a. **Enterprise Risk Management (ERM) Framework:** the set of components that provide a structure for designing, implementing, monitoring, reviewing and continually improving risk management in the NSW RFS.

b. **Enterprise Risk Management Group(s) (ERMG):** Directorate or functional groups established to provide expert advice, oversight, and recommendations to the Senior Executive Team about risk management within their areas of expertise.

c. **Senior Executive Team (SET)**: includes the Commissioner, Deputy Commissioners and Executive Directors (i.e. roles at Band 2 and Band 3).

# 3 Policy

3.1 The NSW RFS is committed to effectively managing risk through a framework that strengthens risk governance, streamlines processes that empower risk-based decision making, and allows the identification and management of uncertainty that ultimately helps us achieve our objectives.

3.2 The risk management framework is appropriate for the NSW RFS and is consistent with NSW public sector compliance requirements. The framework applies the risk management process at the enterprise, functional and operational levels.

3.3 Managers and decision makers at all levels in the agency are accountable for managing risk within their sphere of authority and in relation to the decisions they make.

3.4 All members (volunteers and staff including permanent, temporary and contracted personnel) are responsible for managing risk in their day-to-day activities, including carrying out their roles in accordance with policies and procedures, identifying risks and inefficient or ineffective controls and reporting these to the appropriate level of management.

3.5 This policy is linked with and should be read in conjunction with more specific risk-related policies, procedures and guidelines, including but not limited to those concerning business continuity management, ICT disaster recovery, child protection, fraud and corruption prevention, project management, and work health and safety.

### Roles and Responsibilities

3.6 **Commissioner**

a. Holds ultimate accountability for enterprise risk management and promotes a positive risk culture in the NSW RFS.

b. Endorses and supports the NSW RFS ERM Framework.

c. Provides a formal attestation to NSW Treasury each year regarding compliance by the NSW RFS with the core requirements of TPP 20-08.

d. Communicates risk with the SET through regular reporting and briefings, and includes risk updates to all members at appropriate meetings/forums.

3.7 **Audit and Risk Committee (ARC)**

a. Provides independent oversight and assurance that the Service's risk management environment is operating effectively in accordance with the ARC Charter.

b. Advises and guides the Commissioner on the agency's governance processes, risk management framework and external accountability obligations.

3.8 **Senior Executive Team (SET)**

c. As Risk Stewards, oversees the ERM Framework and the key enterprise risks underpinning the achievement of strategic objectives.

d. Monitors strategic risks including impacts of assurance activities, changes to key risk indicators and tracking of risk treatment plans.

e. Promotes a positive risk management culture within their area of responsibility and influence.

3.9 **Chief Risk Officer (CRO)**

a. Develops, maintains and implements the NSW RFS ERM framework.

b. Provides assurance to the Commissioner and the ARC on the effectiveness of the risk management framework including the design and operational effectiveness of internal controls and business resumption priorities.

3.10 **Chief Information Officer (CIO)**

a. Develops, maintains and implements the NSW RFS ICT Business Continuity Plan (ICT BCP) and Disaster Recovery (DR) arrangements.

b. Ensures the Service's ICT BCP and DR framework complies with the NSW Government Cyber Security Strategy and Policy.

c. Provides assurance to the NSW RFS ICT Governance Group on the effectiveness of the ICT BC & DR framework including the results of exercises and any actions resulting from the exercise.

3.11 **Chief Audit Executive (CAE)**

a. Establishes and maintains an internal audit function and is responsible for providing strategic leadership and managing the internal audit function within the agency.

b. Ensures the internal audit function is consistent with the International Standards for Professional Practice for Internal Auditing.

c. Ensures the agency has an Internal Audit Charter that is consistent with the content of the TPP20-08 'model charter'.

3.12 **Enterprise Risk Management Groups (ERMGs)**

a. Incorporate risk management discussion and challenge to identify pervasive / systemic and interdependent operational risks that may need to be consolidated and escalated for discussion at the SET level.

# 4 Related documents

- NSW Treasury TPP 20-08 Internal Audit and Risk Management Policy for the NSW Public Sector
- ISO 31000:2018 Risk management – Guidelines
- NSW Treasury TPP 12-03 Risk Management Toolkit for the NSW Public Sector
- The Business Continuity Institute Good Practice Guidelines
- NSW RFS Business Continuity Guidelines
- NSW Cyber Security Strategy

# 5 Amendments

| AMENDMENT DATE | VERSION NO | DESCRIPTION |
|---|---|---|
| 1 August 2011 | 1.0 | Initial release |
| 1 July 2014 | 1.1 | • Repealed and remade P7.1.10 v1.0<br>• Annual Review - 2013/14<br>• Reviewed to coincide with review of ORM processes<br>• Negative Consequences table added to SOP P7.1.10 – 1 |
| 24 August 2015 | 1.2 | • Repealed and remade P7.1.10 v1.1 |

| AMENDMENT DATE | VERSION NO | DESCRIPTION |
|---|---|---|
| | | › Annual Review - 2014/15<br>› Reviewed to reflect release of updated Treasury Policy – revised from TPP 09-05 to TPP 15-03 |
| 30 June 2015 | | › Annual Review - 2015/16<br>› No amendments required |
| 11 May 2017 | 2.0 | › Repealed and remade P7.1.10 v1.2<br>› Annual Review - 2016/17<br>› Reviewed to reflect changes in the NSW Government policy framework<br>› Reviewed to align with NSW RFS Organisational Risk Management Framework<br>› Refined approach to risk treatment, including links to Business Plans |
| 30 July 2018 | 2.1 | › Repealed and remade P7.1.10 v2.0<br>› Annual Review – 2017/18<br>› Reviewed in line with the release of ISO 31000:2018: Risk management – Guidelines |
| 20 August 2019 | 2.2 | › Repeals and remakes P7.1.10 v2.1<br>› Annual Review – 2018/19<br>› Update of review cycle to normal 3 – 5 year review cycle<br>› Reviewed to reflect the release of AS ISO 31000:2018 |
| 20 Sept 2022 | 3.0 | › Repeals and remakes P7.1.10 v2.2<br>› Repeals P7.1.9 Business Continuity v2.0, and incorporates content into new SOP P7.1.10-2<br>› Repeals P5.1.7 ICT Disaster Recovery and incorporates content into new SOP P7.1.10-3<br>› Complete review in line with the Enterprise Risk Management framework |

# SOP P7.1.10-1
# RISK MANAGEMENT PROCESS

## 1 Purpose

1.1 Policy P7.1.10 Enterprise Risk Management reflects the commitment of the NSW RFS to a contemporary risk management approach to support decision-making and the achievement of strategic objectives.

1.2 This procedure supports the policy by outlining how risk will be managed proactively, consistently and systematically so that the NSW RFS identifies and responds to the risks it faces in a balanced manner.

## 2 Risk Management Process

2.1 The NSW RFS risk management process is consistent with AS ISO 31000:2018 *Risk management Guidelines* as shown in Figure 1:

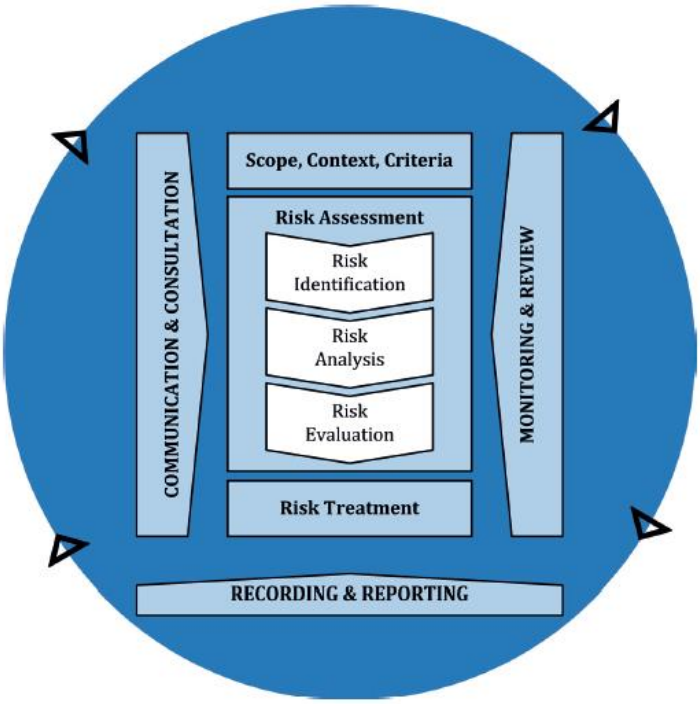



*Figure 1: NSW RFS risk management process*

### Identifying Risks

2.2 The risk assessment process begins with identifying risks. Risks in the NSW RFS may be identified through a number of means including:

a. Examination of organisational functions, plans, policies and procedures;
b. Strategic planning and performance monitoring;
c. Projects, new initiatives and developing situations;
d. Assessment of compliance obligations;
e. Discussion or workshops with internal and external stakeholders;
f. Lessons management processes;
g. Audit and review outcomes

## Analysing and Evaluating Risks

2.3 The NSW RFS has established a standard process and set of tools to ensure that risk is analysed and evaluated consistently and that actions taken to manage the risk are appropriate to achieving the organisation's goals.

| | |
|---|---|
| **Step 1. Establish the risk context and control environment** | Start by describing the risk and the strategic or operational outcomes that the NSW RFS hopes to achieve by adequately managing the risk. Consider:<br><br>**Contributing Factors** – Details on why the risk has arisen and the key aspects that contribute to the significance of the risk. The contributing factors should be high-level points that are used to guide thinking around the critical success factors, current controls and risk treatment activities.<br><br>**Critical Success Factors** – are the "what must go right" areas for effectively managing the risk. The critical success factors help establish the key areas to focus on when managing the risk. Critical success factors can relate to existing controls and processes for managing the risk, or they can be aspirational factors that would make risk management more effective.<br><br>**Implications** – What may happen if the risk is not appropriately managed.<br><br>**Current Controls** – The programs or activities that are currently in place to manage the risk. |
| **Step 2. Rate the risk and current control effectiveness** | Rating risk means determining the potential consequence of the risk and its likelihood of occurrence, then using the Risk Rating Matrix (Figure 4) to rate the risk from Low to Critical.<br><br>**Inherent Risk Rating** is the risk assessed in an uncontrolled environment, whilst the **Residual Risk Rating** considers the risk after controls have been applied.<br><br>A combination of the two ratings (inherent and residual) indicates how reliant the NSW RFS is on the control environment for effectively managing the risk.<br><br>*Refer Figure 2: Determine the consequence – with and without controls*<br>*Refer Figure 3: Determine the likelihood – with and without controls*<br>*Refer Figure 4: Rate the inherent risk (without controls) and residual risk (with controls)*<br><br>**Control effectiveness rating** is the degree to which the controls are successful in reducing the likelihood and/or consequence of a risk.<br><br>*Refer Figure 5: Rate the effectiveness of existing controls* |
| **Step 3. Determine required action** | Based on the ratings of the inherent risk and the control effectiveness determined in Step 2, plot the risk on the Risk Action Matrix (Figure 6).<br><br>The matrix will provide guidance on the recommended course of action for managing the risk. Actions can range from:<br><br>› Developing risk treatment plans to enhance the control environment<br>› Undertaking assurance over the effectiveness of controls which are managing high inherent risks<br>› Monitoring the risk to determine if any action is required in the future as a result of movement of the risk rating and control environment<br>› Accepting the level of risk with no further action required.<br><br>*Refer Figure 6: Risk action matrix and Figure 7: Risk action narrative* |

*Figure 2: Consequence Matrix*

| Consequence Rating | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Rating** | **Health & Safety Impact** | **Business Capability** | **Community Impact** | **Environmental Impact** | **Financial Impact** | **Reputational Impact** | **Legal/Regulatory/ Compliance Impact** |
| **5 Extreme** | Multiple fatalities and/or injuries with widespread medical attention required | Loss of key service delivery requiring extended external assistance >1 week | Community impact severe and lasting >1 week; not functioning without support | Long term (>5yr) significant environmental damage or clean-up costs >$5m | Financial loss or unrecompensed expense of >$30m<br>Fraud >$1m | Damage to corporate reputation at national or international level<br>Major loss of community support | Parliamentary scrutiny/major government intervention<br>Significant prosecution, fines or class action<br>Imprisonment of responsible officers |
| **4 Major** | Single fatality, serious injuries or occupational illnesses with potential acute or chronic disabilities | Loss of key service delivery requiring external assistance between 1 day and 1 week | General and widespread community impact on functioning for a period of up to one week | Medium term (1-5yr) significant environmental damage or clean-up costs $1 to $5m | Financial loss or unrecompensed expense of $10 - $30m<br>Fraud >$500,000 | Damage to corporate reputation at state or national level<br>Significant decrease in community support | Ministerial inquiry/government intervention<br>Requires external legal assistance<br>Prosecution by regulator<br>Litigation<br>Responsible officers charged with offence |
| **3 Moderate** | Medical treatment required with potential for short term absence <1 week with no fatalities or serious long-term disabilities | Loss of service delivery causing disruption of up to 1 day | Normal community functioning with some inconvenience for 24 to 48 hours | Short term (<1yr) environmental damage or clean-up costs up to $1m | Financial loss or unrecompensed expense of $1 - $10m<br>Fraud >$50,000 | Damage to corporate reputation at state or regional level<br>Moderate decrease in community support | Regulatory breaches with investigation or report to authority with prosecution powers<br>Requires intervention by senior management<br>Fines possibly incurred |
| **2 Minor** | Minor injuries only, medical treatment required. Sick leave not required | Loss of service delivery causing disruption of less than half a day | Some community disruption for less than 24 hours | Small and short-term environmental damage requiring less than $250,000 to clean up | Financial loss or recompensed expense of $100,000 to $1m<br>Fraud >$5,000 | Damage to corporate reputation at regional or local level<br>Minor decrease in community support | Minor policy non-compliances or regulatory breaches, managed at local level |
| **1 Insignificant** | On-site first aid may be required | Inconsequential loss of service delivery. No impact on operations | Inconsequential disruption to the community | Small environmental impact, clean up on-site managed within normal operating budget | Financial loss or unrecompensed expense of less than $100,000<br>Fraud <$5,000 | Local awareness of an issue exists but there is no public concern | Minor compliance issues |

*Figure 3: Likelihood Matrix*

| Likelihood Rating | |
|---|---|
| **Likelihood** | **Detailed description** |
| **5 Highly Likely** | • Strong likelihood of re-occurring, with much opportunity and means to occur<br>• The consequence is expected to be experienced in most circumstances (monthly)<br>• High level of known incidents (records/experience) |
| **4 Likely** | • Considerable opportunity and means to occur<br>• The assessed level of consequence will probably be experienced in most circumstances (annually)<br>• Regular incidents known (records/experience) |
| **3 Possible** | • Some opportunity and means to occur<br>• The assessed level of consequence should be experienced at some time (2 to 5 years)<br>• Few infrequent, random occurrences recorded/experienced |
| **2 Unlikely** | • Little opportunity or means to occur<br>• The assessed level of consequence could be experienced at some time (5 to 15 years)<br>• No known incidents recorded or experienced |
| **1 Highly Unlikely** | • Almost no opportunity to occur<br>• The assessed level of consequence may be experienced only in exceptional circumstances (15+ years)<br>• Not known to have ever occurred |

*Figure 4: Risk Rating Matrix*

| | Consequence | | | | | |
|---|---|---|---|---|---|---|
| Likelihood | | **Insignificant (1)** | **Minor (2)** | **Moderate (3)** | **Major (4)** | **Extreme (5)** |
| | **Highly Likely (5)** | Low | Medium | High | Critical | Critical |
| | **Likely (4)** | Low | Medium | High | High | Critical |
| | **Possible (3)** | Low | Low | Medium | High | Critical |
| | **Unlikely (2)** | Low | Low | Low | Medium | High |
| | **Highly Unlikely (1)** | Low | Low | Low | Low | Medium |

*Figure 5: Control effectiveness rating*

| Control Effectiveness Rating | Description / Guide |
|---|---|
| Fully Effective (1) | • Controls in place and can be relied upon to prevent risk materialising<br>• Controls are formally documented, current and well understood by staff<br>• Management ensures compliance with controls<br>• Effectiveness of controls are formally reviewed and monitored by responsible management on a regular basis<br>• Management activity promotes a strong control environment<br>• Ownership for the controls is clearly defined. |
| Substantially Effective (2) | • Controls in place and can be relied upon to mitigate or detect risk materialising in most circumstances<br>• Formal documentation of some controls which are reasonably understood by members<br>• Management ensures that controls are operating as defined, although there is no formal monitoring or measurement of effectiveness of controls<br>• Management actively promotes effective controls. |
| Partially Effective (3) | • Majority of controls in place. Basic risk will be controlled. However, scope exists to improve controls<br>• Formal documentation of some controls which are reasonably understood by members<br>• Management has identified and understand the controls, but monitoring is informal. |
| Largely Ineffective (4) | • Basic controls in place. No guarantee risk will be controlled<br>• Informal documentation of some controls exist<br>• Members are not fully aware of and/or do not understand the controls. |
| Totally Ineffective (5) | • Significant gaps<br>• No documentation of controls exists<br>• Members are not aware of and/or do not understand the controls<br>• Either our actions do not treat the causes, or they do not operate at all effectively. |

*Figure 6: Risk action matrix*

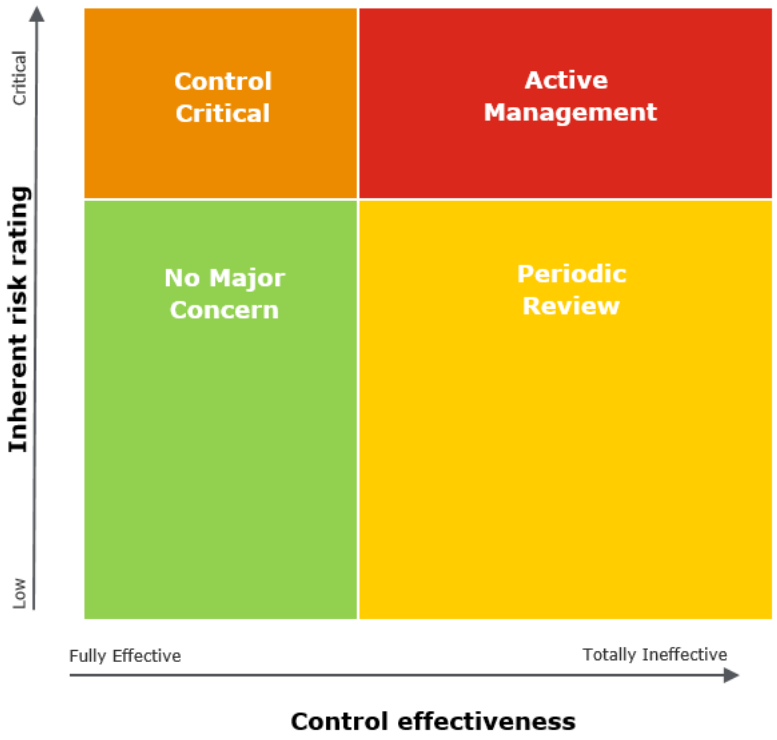



*Figure 7: Risk action descriptions*

| | |
|---|---|
| **Active Management** | This level of risk is generally unacceptable in any circumstance. Urgent treatment is required to reduce the level of risk, with ongoing active review of treatment options and supporting plans. |
| **Control Critical** | The inherent level of risk is high however there are strong controls in place. Consequently there is a high reliance on the operating effectiveness of these controls to minimise the likelihood or impact should the risk event occur. Controls need to be constantly monitored to confirm their effectiveness. |
| **Periodic Review** | While the controls are not always strong, the inherent risk rating is not at the highest levels either. Management should consider options to improve the control environment through appropriate risk treatments, or monitor the risk profile to ensure it does not increase over time. |
| **No Major Concern** | Risks where systems and processes managing the risk are adequate. Monitoring of the controls and the risk profile should occur periodically. |

# 3 Risk Ownership and Roles

3.1 The NSW RFS risk management process is applied at three levels of risk ownership, which are aligned to the Three Lines of Defence model of organising risk roles and functions.

3.2 The Commissioner and the Senior Executive plays an oversight role over all three lines of defence at the Enterprise Level.

### Enterprise Level (Executive oversight and Third Line of Defence)

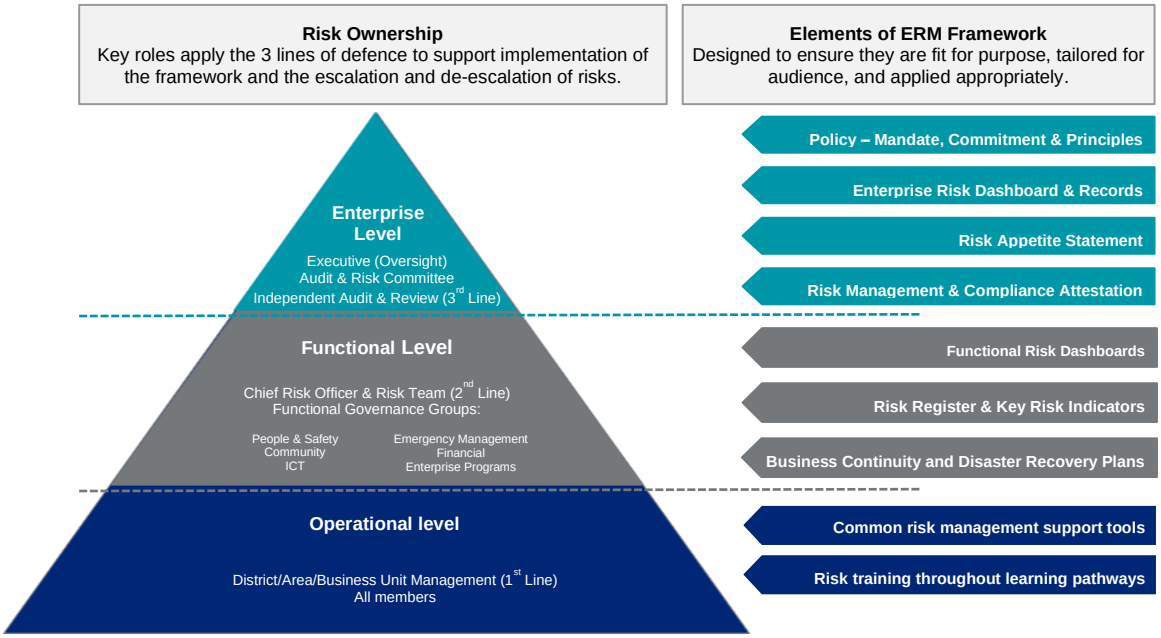
- Management of Service-wide or strategic risks through executive oversight of identified risks. The Senior Executive team are the Risk Stewards
- Independent oversight and assurance of implementation and effectiveness of controls

### Functional Level (Second Line of Defence)

- Establishes processes to manage and monitor risk and ensure risk is being adequately identified, discussed, and escalated:
- Functional governance and risk ownership is applied to implement and monitor controls, identify and escalate emerging risks. This may occur across a range of existing committees, governance groups, or senior leadership teams as appropriate for each enterprise risk and at the direction of the Risk Steward.

### Operational Level (First Line of Defence)

- Managers monitor the effectiveness of controls and escalate risks to Functional Governance Groups through the Risk and Research Team at riskandresearch@rfs.nsw.gov.au
- All members are trained and focused on identification and management of hazards, applying organisational controls and escalating risks where appropriate.



# SOP P7.1.10-2
# BUSINESS CONTINUITY

## 1 Purpose

1.1 This procedure details the responsibilities and processes for business continuity management to ensure the NSW RFS is able to deal with a business disruption while continuing to help keep the community safe.

1.2 Business continuity is an element of the Enterprise Risk Management Framework which is focussed on the specific arrangements to prepare for, reduce the impact of, and recover from a disruptive event so that critical business functions and services can be maintained at an acceptable level.

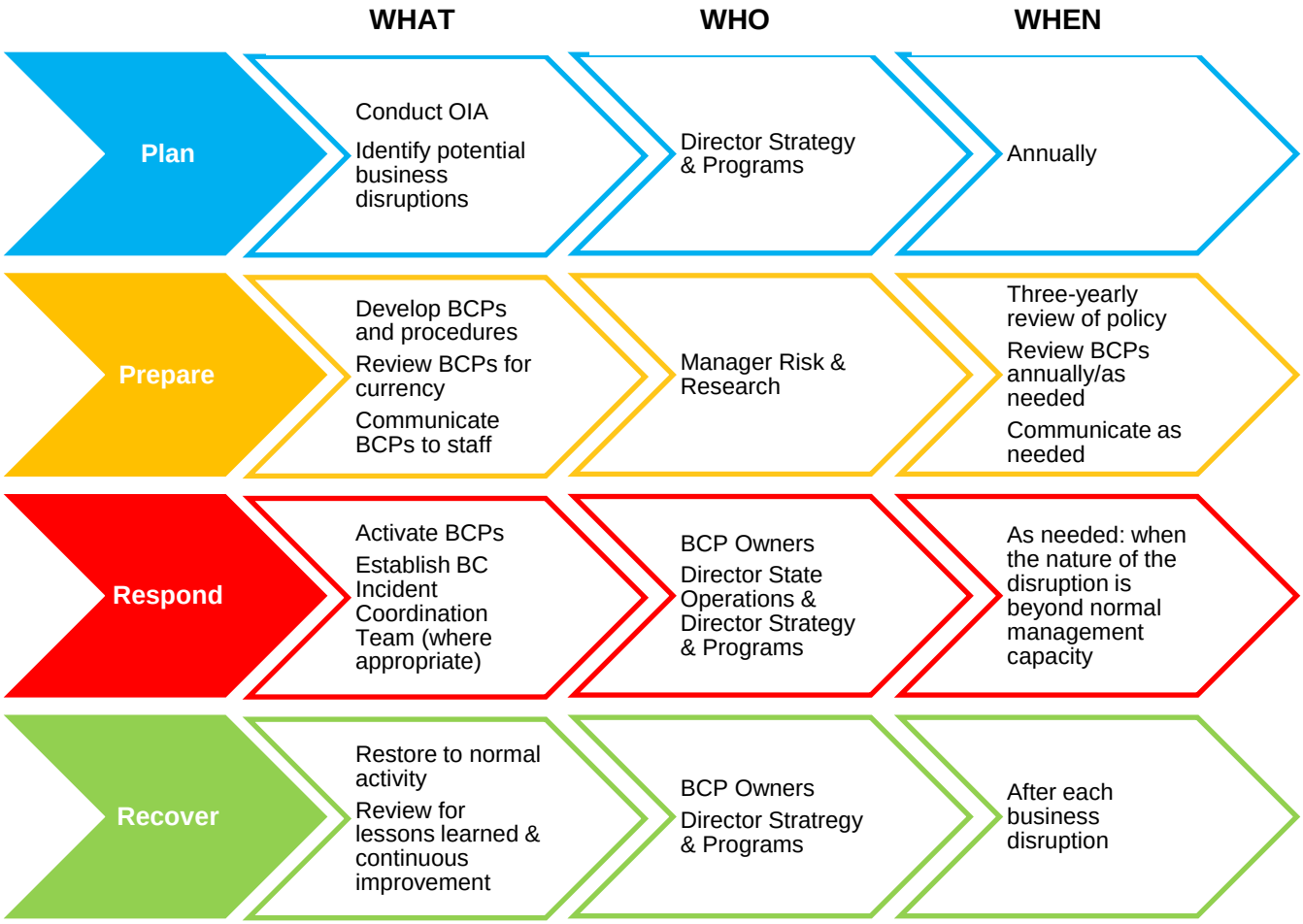
## 2 Business Continuity Framework

2.1 Business continuity activities in the NSW RFS are to be undertaken in accordance with the Business Continuity Framework and Guidelines.

2.2 The framework integrates business continuity with the broader corporate governance and risk management systems of the NSW RFS, and is consistent with relevant standards and better practice guidelines.

**NSW RFS Business Continuity Framework**

# 3 Business Continuity Process




### Organisational Impact Assessment

3.1 The Organisational Impact Assessment (OIA) is the foundation of the BC program and consists of a formal assessment and analysis of NSW RFS business activities and the effect that a significant disruption might have upon them.

3.2 The services and products identified as the highest priority are those that if unavailable, the NSW RFS cannot operate for long without experiencing a negative impact.

3.3 The Executive Director People and Strategy shall ensure the OIA is conducted every two years and reviewed annually.

### Business Continuity Plans

3.4 The Business Continuity Plan (BCP) is a subset of the data gathered from the OIA and reflects the risk ratings and arrangements resulting from the OIA.

3.5 The BCP owner is the manager of the business unit in which the activity or function occurs, as identified in the OIA.

3.6 The BCP is a documented collection of procedures and information to assist in re-establishing business functions after an incident occurs, as well as identifying and informing necessary internal and external stakeholders of the unplanned business disruption.

3.7 Development and review of the BCP is undertaken alongside the OIA.

3.8 BCPs shall be stored in the NSW RFS record management system.

### BC Exercising

3.9 An exercise program shall be developed to ensure business continuity arrangements and plans remain fit for purpose.

### Business continuity plan activation and incident reporting

3.10 All business disruptions at any NSW RFS site shall be reported to the Operational Communications Centre (OCC) in the first instance.

3.11 The OCC shall advise the State Duty Officer (SDO) and the Director Strategy and Programs of the business disruption.

3.12 If an unplanned event occurs that may exceed the capacity of normal management methods, the BCP must be activated.

3.13 A BC Incident Coordination Team, responsible for control of the overall response and recovery effort, will be established when the event is beyond the ability of local resources to manage or carries significant strategic consequences.

### After Action Review

3.14 An after action review (AAR) shall be held for all business continuity incidents.

### Audit and Reporting

3.15 In accordance with the principles of continuous improvement, the NSW RFS BC program shall be subject to periodic audit.

3.16 Business continuity activity shall be reported to the NSW RFS ARC annually.

### Roles and Responsibilities

3.17 The Executive Director People and Strategy shall oversee the NSW RFS business continuity framework.

3.18 The Director Strategy and Programs shall ensure the OIA is conducted every two years through consultation with key stakeholders, and monitor compliance and reporting as appropriate.

3.19 The Manager Risk and Research is responsible for the development and maintenance of the framework documents and supporting tools.

3.20 Directors and Managers shall participate in the OIA and the development of BCPs relevant to their functional responsibilities, and undertake actions assigned to them in the event of a disruption.

## 4 Related documents

- NSW RFS Business Continuity Guidelines
- Business Continuity Institute Good Practice Guidelines (BCI GPC)

# SOP P7.1.10-3
# ICT DISASTER RECOVERY

## 1 Purpose

1.1 The NSW RFS ICT group takes a risk management approach to the continuity of the critical resources that support the operation of the Service.

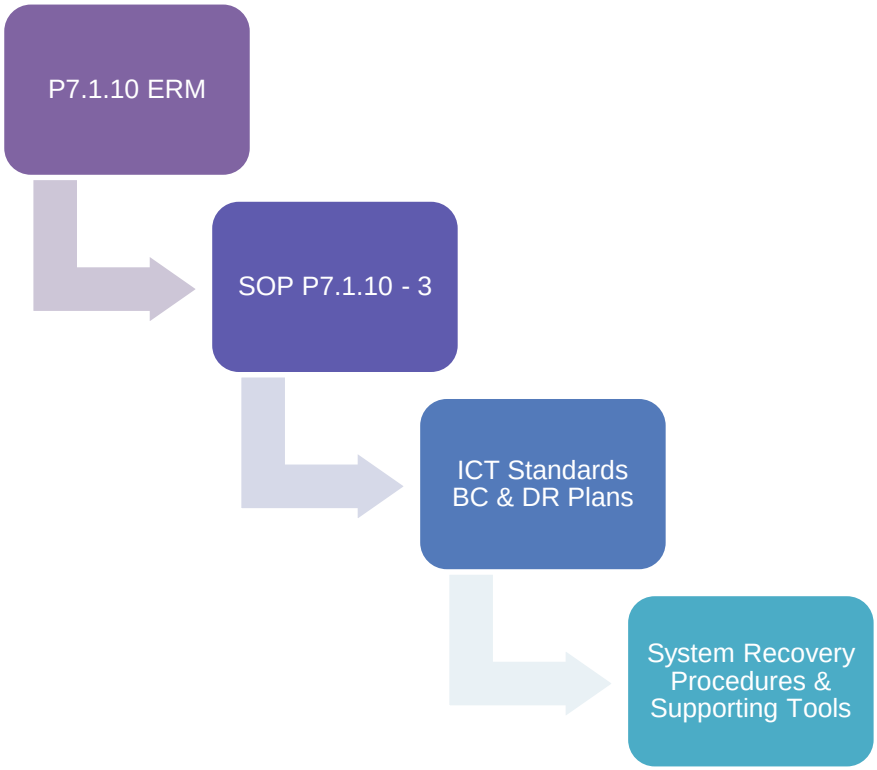
1.2 The framework integrates ICT business continuity and disaster recovery with the broader corporate governance and risk management systems of the NSW RFS, and is consistent with relevant NSW Government requirements, standards and better practice guidelines.

1.3 This procedure provides guidance on the responsibilities and processes for the management of the NSW RFS ICT business continuity and disaster recovery arrangements to ensure the availability of critical ICT resources in the event of an unplanned disruption.

## 2 ICT Business Continuity and Disaster Recovery Framework

2.1 ICT business continuity and disaster recovery is undertaken in accordance with the ICT Business Continuity and Disaster Recovery framework.

2.2 The framework incorporates risk management principles to ensure the risk to the Service's ICT resources is appropriately identified and managed.



### ICT Standards

2.3 The ICT Business Continuity Plan and the ICT Disaster Recovery Plan have been published as ICT Standards. These are indexed documents and are subject to annual review to ensure they remain fit for purpose.

2.4 The ICT Business Continuity Plan and the ICT Disaster Recovery Plan are two separate but related ICT Standards.

2.5 Other ICT Standards may be developed as the need arises.

### ICT Business Continuity Plan

2.6 The Business Continuity Plan provides guidance in the event of a significant unplanned disruption affecting ICT operations. It outlines the strategy to prepare for and respond to a disruption so as to minimise the impact on end-users and the operation of the NSW RFS.

### ICT Disaster Recovery Plan

2.7 The Disaster Recovery Plan provides guidance for the recovery of ICT services in the event of an ICT disaster. It has been developed to facilitate the effective recovery of those ICT infrastructure components and systems that underpin the operation of the NSW RFS.

2.8 The plan outlines the high-level process for recovery of critical ICT infrastructure and systems

### ICT System Recovery Procedures

2.9 The ICT System Recovery Procedures detail the steps to be taken to recover a specific system.

2.10 System Recovery Procedures will be developed for each system rated at the appropriate level of priority.

2.11 Access to System Recovery Procedures is limited to appropriate members of the ICT team to maintain system security.

## 3 ICT Business Continuity and Disaster Recovery Process

### Identify and Assess Critical Systems

3.1 The Director ICT will ensure a risk assessment is conducted to determine the criticality of ICT resources and those resources requiring high availability.

### Activating the ICT Business Continuity Plan

3.2 The ICT Business Continuity Plan is activated when there is an event that has been assessed as causing significant disruption to the ICT group's operations. Not every disruption or outage will require activation.

3.3 The Director ICT is responsible for the decision to activate the Plan. The Director or delegate will declare a 'BCP event' based on assessment of the extent of the impact on normal operations, and the ICT BCP will be activated.

### Disaster Declaration

3.4 The Disaster Recovery Plan will only be activated after declaration of a disaster by the Director ICT or delegated authority. The Director ICT may consult with other members of the ICT group at his/her discretion before declaring a disaster.

3.5 The decision to declare a disaster will be based on an objective assessment influenced by the timing, likely duration and expected business impact of an outage to ICT services.

### Disaster Recovery Exercising

3.6 NSW Government Cyber Security Strategy requires that Disaster Recovery Plans are tested annually. Where possible and appropriate DRP testing is to be incorporated into the organisational business continuity and State Operations systems testing regime.

### After Action Review

3.7 An after action review (AAR) is to take place after each activation. The AAR is to be held according to the requirements of Service Standard 1.5.6 Lessons Management Framework.

3.8 The findings of the AAR are to be reported to the ICT Governance Group.

### Reporting

3.9 Any activation of the ICT Business Continuity Plan and the ICT Disaster Recovery Plan are to be reported to:

- Executive Director Technology, Finance and Legal
- Director Programs and Strategy as the Chief Risk Officer and responsible for organisational business continuity
- Audit and Risk Committee by the Chief Risk Officer

### Roles and Responsibilities

- The Director ICT is responsible for the ICT Business Continuity and Disaster Recovery framework.
- The ICT Security Officer is responsible for the security of the ICT System Recovery Procedures.

### Review

3.10 The ICT Business Continuity Plan and the ICT Disaster Recovery Plan are to be reviewed annually, or:

- After activation of either plan
- After the implementation of a significant change to the ICT environment
- Following organisational change or realignment or implementation of new technology.