NSW RURAL FIRE SERVICE

POLICY P7.1.10
ORGANISATIONAL RISK MANAGEMENT

ITEM	DESCRIPTION
Version Number	2.2
SOPs	› SOP P7.1.10 - 1 Risk Assessment and Treatment Process › SOP P7.1.10 - 2 Risk Registers – Format and Maintenance › SOP P7.1.10 - 3 Risk Tolerance and Escalation › SOP P7.1.10 - 4 Risk Reporting
Owner	Executive Director, Membership and Strategic Services
Contact	Director, Corporate Planning, Risk and Learning
Approved Date	20 August 2019
Effective Date	20 August 2019
Next Review Date	20 August 2024
Document Control	Electronic - printed copies are uncontrolled

1 Purpose

1.1 Effective corporate governance is essential to the performance, integrity and transparency of the NSW Rural Fire Service (NSW RFS). Management of risk is a component of good governance that creates and protects value. It aids the achievement of State Government and NSW RFS objectives and contributes to improved performance.

1.2 This Policy ensures there is an Organisational Risk Management (ORM) process in operation that is appropriate to the needs of the NSW RFS and takes a consistent approach to both operational and organisational risk.

1.3 This Policy reflects the commitment of the NSW RFS leadership to the integration of risk management in assisting in setting strategy, achieving objectives and making informed decisions.

1.4 All NSW RFS members are responsible for the management of risk and contribute to, and participate in, risk management by raising potential risks and complying with procedures that may contain embedded risk controls.

1.5 This Policy outlines how risk is managed proactively, consistently and systematically so that the NSW RFS responds to the risks it faces in a balanced manner.

1.6 This Policy is aligned with the relevant provisions of: NSW Treasury Policy and Guidelines Paper TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector; ISO 31000:2018 Risk Management – Guidelines, AS ISO 31000:2018 Risk management –Guidelines; the NSW RFS Organisational Risk Management Framework; AS ISO 19600:2015 Compliance management systems—Guidelines and the NSW RFS Corporate Governance Statement.

2 Definitions

2.1 For the purpose of this policy, the following definitions apply:

a. **Business Plan**: NSW RFS Business Plans articulate the actions that will be undertaken by a business unit / section to meet corporate objectives and outcomes as stated in the NSW RFS Corporate Plan. They also provide the mechanism for measuring success in delivering these objectives and outcomes.

b. **Chief Risk Officer**: the role that has designated responsibility for designing the NSW RFS risk management framework and for the day-to-day activities associated with coordinating, maintaining and embedding the framework in the NSW RFS.

c. **Consequence**: as defined in AS ISO 31000:2018, is the outcome of an event affecting objectives. That is, an event or circumstance that may have an effect on the objectives of the NSW RFS. An event or circumstance can have positive or negative consequences.

d. **Control**: as defined in AS ISO 31000: 2018, is a measure that maintains and/or modifies risk. Controls include processes, policies, devices, practices or other actions which modify or support the management of risk.

e. **Event*:*** as defined in AS ISO 31000: 2018, is an occurrence or change of a particular set of circumstances.

f. **External context**: the external environment within which the NSW RFS operates to achieve its objectives. It can include the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environments, as well as key drivers and trends that have an impact on the objectives of the NSW RFS. It can also include relationships with, and the perceptions and values of, external stakeholders.

g. **Hazard**: any source of potential damage, harm or adverse effect on the achievement of organisational objectives.

h. **Internal context**: the internal environment within which the NSW RFS operates to achieve its objectives. It can include organisational values, governance and structure, roles and accountabilities, policies and procedures, capabilities, information systems, decision-making processes and the risk management framework itself.

i. **Likelihood**: as defined in AS ISO 31000: 2018, is the chance of something happening.

j. **Negative consequence**: a consequence that impedes the achievement of NSW RFS objectives.

k. **Organisational Risk Management (ORM)**: the consistent systematic application across the organisation of management policies, procedures and practices that manage risk, support decision-making and assist the NSW RFS to achieve its objectives.

l. **Positive consequence**: a consequence that assists in the achievement of NSW RFS objectives.

m. **Potential Exposure (PE)**: the plausible maximum impact on the NSW RFS that could arise from a risk if controls were not applied. It is expressed in terms of a consequence rating (using the negative or positive consequence tables).

n. **Risk**: as defined in AS ISO 31000:2018, the effect of uncertainty on objectives. Risk may be positive or negative.

o. **Risk action plan**: a detailed plan to treat a risk. It includes the actions, responsibilities, milestones and due dates which have been developed and approved to treat a risk.

p. **Risk action plan lead**: the staff member allocated the responsibility to coordinate the development, implementation and quarterly reporting of the risk action plan.

q. **Risk assessment**: the overall process for identifying, analysing and evaluating a risk.

r. **Risk analysis**: the process to understand the nature of a risk and determine the level of a risk. It includes assessment of the:

   i. Key controls in place (if any) used to treat the risk;

   ii. Effectiveness of the existing key controls;

   iii. Potential consequences associated with the reasonable worst (or best) case (taking the controls into account);

   iv. Likelihood of the risk event being realised and leading to the assessed level of consequence (taking the controls into account);

   v. Overall risk rating indicated by the consequence and likelihood ratings; and

   vi. Potential exposure of the NSW RFS to the risk if all the controls fail.

s. **Risk management**: as defined in AS ISO 31000:2018, the coordinated activities to direct and control an organisation with regard to risk.

t. **Risk management context**: the scope, or working environment of the activity, project, organisation etc., to which the risk assessment process is being applied.

u. **Risk management framework**: refers to the set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout an organisation (including this Policy).

v. **Risk maturity**: an organisation's level of attainment of risk management capabilities.

w. **Risk owner**: the Executive Director is the owner of all risks held on risk registers within their directorate and other relevant risks from the Organisation risk register.

x. **Risk rating**: the combination of the likelihood and consequence of a risk.

y. **Risk register**: the repository for the collection of information relating to a number of risks.

z. **Risk register owner**: the staff member responsible for the risk register. The Executive Director is the owner of the directorate risk register and the business unit manager is the owner of the business unit risk register.

aa. **Risk treatment**: processes applied to further control a risk. Risk treatment can involve:

i. Avoiding the risk;

ii. Taking or increasing the risk to pursue an opportunity;

iii. Removing the source of the risk;

iv. Changing the likelihood of the risk;

v. Changing the consequence of the risk;

vi. Sharing the risk with another party or parties; and

vii. Retaining the risk, by informed decision.

bb. **Risk tolerance**: the readiness of the NSW RFS to bear a specified level of risk in order to achieve its objectives. Note that risk tolerance may be influenced by legal, regulatory or compliance requirements.

cc. **Uncertainty**: the state, even partial, of deficiency of information related to understanding or knowledge of an event or situation, its consequence or likelihood.

3 Policy

3.1 The management of risk within the NSW RFS is appropriate to organisational needs and aligns with appropriate International and Australian standards. It is integrated with NSW RFS systems, processes, activities and decision-making at all levels, including, but not limited to:

a. Strategic, corporate and business planning;

b. Policy development and management;

c. Project management;

d. Work Health and Safety management;

e. Business continuity management;

f. Event management;

g. Engineering;

h. Training;

i. Internal audit;

j. Financial management, including procurement activities;

k. ICT security controls and objectives (including cyber security); and

l. Compliance management.

3.2 ORM must be used to assist in prioritising strategies and actions to address uncertainties that the NSW RFS may face.

3.3 In accordance with NSW Treasury Policy TPP 15-03, the Commissioner shall provide a formal attestation each year regarding compliance by the NSW RFS with the core requirements of the Policy, including the risk management component. This attestation must be made to the NSW Treasury and published in the NSW RFS Annual Report.

3.4 The Commissioner will nominate a Chief Risk Officer who is responsible for promoting and oversighting risk management within the NSW RFS, as recommended by NSW Treasury Policy TPP 15-03.

3.5 The Audit and Risk Committee (ARC) will provide an oversight role, including monitoring and review of the performance of the NSW RFS in relation to ORM, and reporting on this to the Commissioner.

3.6 Risk reporting must be in accordance with SOP P7.1.10 - 4 Risk Reporting.

4 Related documents and links

- *Annual Reports (Departments) Act 1985*
- Annual Reports (Departments) Regulation 2015
- NSW Treasury TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector
- ISO 31000:2018 Risk management – Guidelines
- AS ISO 31000:2018 Risk management - Guidelines
- AS ISO 19600: 2015 Compliance management systems - Guidelines
- HB 158:2010 Delivering assurance based on ISO 31000:2009 Risk management – Principles and guidelines
- NSW Treasury TPP 12-03 Risk Management Toolkit for the NSW Public Sector
- NSW Treasury TPP 17-06 Certifying the effectiveness of internal controls over financial information
- NSW Treasury TPP 18-07 Organisational Resilience
- NSW Government Cyber Security Strategy
- NSW Government digital NSW – Designing our digital future
- NSW RFS Corporate Governance Statement
- NSW RFS Corporate Plan
- NSW RFS Organisational Risk Management Framework
- NSW RFS Project Management Handbook
- Service Standard 1.1.28 Injury and Accident Reporting and Investigation
- Service Standard 1.1.32 Fraud and Corruption Prevention
- Policy P5.1.3 Information Security Management
- Policy P7.1.1 Project Management
- Policy P7.1.4 NSW RFS Corporate Planning and Reporting
- NSW RFS Procurement Handbook

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 › Annual Review - 2013/14 › Reviewed to coincide with review of ORM processes › Negative Consequences table added to SOP P7.1.10 – 1
24 August 2015	1.2	› Repealed and remade P7.1.10 v1.1 › Annual Review - 2014/15 › Reviewed to reflect release of updated Treasury Policy – revised from TPP 09-05 to TPP 15-03
30 June 2015		› Annual Review - 2015/16 › No amendments required

AMENDMENT DATE	VERSION NO	DESCRIPTION
11 May 2017	2.0	› Repealed and remade P7.1.10 v1.2 › Annual Review - 2016/17 › Reviewed to reflect changes in the NSW Government policy framework › Reviewed to align with NSW RFS Organisational Risk Management Framework › Refined approach to risk treatment, including links to Business Plans
30 July 2018	2.1	› Repealed and remade P7.1.10 v2.0 › Annual Review – 2017/18 › 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 › Annual Review – 2018/19 › Update of review cycle to normal 3 – 5 year review cycle › Reviewed to reflect the release of AS ISO 31000:2018

SOP P7.1.10 - 1
Risk Assessment and Treatment Process

1 Purpose

1.1 This Standard Operating Procedure (SOP) describes the process to be followed for:

a. Identifying, analysing and evaluating risks;

b. Assigning specific responsibilities for managing risks to the appropriate officers;

c. Deciding whether the risk should be controlled or accepted, by way of informed decision;

d. Treating the risk and taking appropriate steps to do so;

e. Confirming whether risk treatment activities are effective; and

f. Adjusting risk treatments in light of experience.

1.2 All NSW RFS managers are responsible for applying the risk management process as appropriate to the situation.

1.3 All NSW RFS employees are responsible for notifying their manager, or the manager of the area in which they are working, of any identified potential risks.

2 Procedures

Overview

2.1 The NSW RFS risk management process consists of the following steps, shown in Figure 1:

a. Establishing the scope, context and criteria;

b. Risk identification;

c. Risk analysis;

d. Risk evaluation;

e. Risk treatment;

f. Communication and consultation;

g. Monitoring and reviewing; and

h. Recording and reporting.

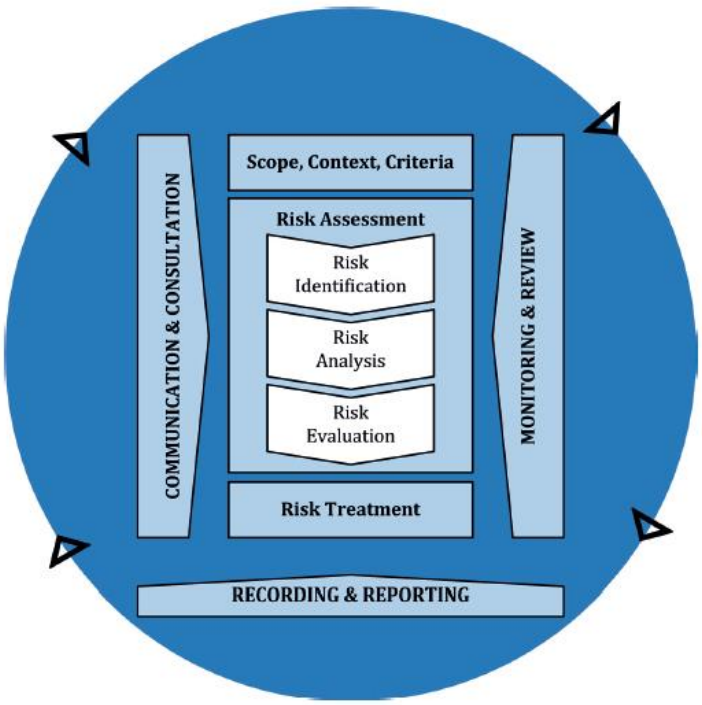

Figure 1: NSW RFS risk management process based on AS ISO 31000: 2018

Establishing the Scope, Context and Criteria

2.2 Prior to undertaking a risk assessment, the scope, context and criteria are to be established. This enables an effective risk assessment. Both the external and internal contexts must be considered and documented.

Risk Identification

2.3 Risks may be identified through a number of means including but not limited to:

a. Examination of organisational functions, plans, policies and procedures;

b. Strategic, business planning and performance monitoring;

c. Projects, new initiatives and developing situations;

d. Assessing compliance obligations

e. Discussion or workshops with internal and external stakeholders;

f. Lessons learned from experience (individual or of others, including other organisations);

g. Audits; or

h. Events occurring.

2.4 Risks must be identified and recorded in the appropriate risk register and given a unique identifier.

2.5 Each risk must be recorded in only one risk register at any time.

2.6 Risks may be moved between risk registers, retaining their unique identifier, with Executive Director approval and agreement.

2.7 When identifying risks, those risks that may affect the objectives of the NSW RFS must be included, regardless of whether they can be controlled by the organisation. Risks to the community should be included if they are in areas of NSW RFS responsibility.

2.8 Risks must be identified even when their control is so effective that they are unlikely to occur or have any significant impact on the NSW RFS. The identification of these risks supports the ongoing resources allocated to these controls.

2.9 Risks must align to the NSW RFS Strategic Plan.

2.10 When changes in the internal or external context occur, these changes must be examined to determine whether they create new risks or alter existing risks.

Describing Risks

2.11 Risks must be expressed in plain English and suggest the broad types of impacts that might result from an event that creates the risk. They are usually expressed in the form:

<*something uncertain may occur*> which leads to <*an effect on objectives*>.

For example:

- × volunteer numbers are inadequate
- ✓ changing community demographics may lead to insufficient member numbers.

2.12 The potential causes and effects of each risk must be considered.

Describing Key Controls

2.13 The key controls, that is, those that influence the consequences or likelihood of each risk and are likely to make a significant contribution to the risk rating, must also be documented in the relevant risk register.

Risk Analysis

2.14 Each risk must be analysed in order to gain sufficient understanding to determine an appropriate risk rating. Risk analysis involves:

a. Identifying the key controls in place used to treat the risk;

b. Assessing the effectiveness of the key controls;

c. Assessing the potential consequences associated with the risk, taking the controls into account;

d. Assessing the likelihood of the risk being realised and leading to the assessed level of consequences (taking the controls into account);

e. Identifying the overall risk rating indicated by the consequence and likelihood ratings; and

f. Assessing the potential exposure of the NSW RFS to the risk.

Assessing Control Effectiveness

2.15 While having risk controls in place is important, the effectiveness of these controls must be assessed. The control effectiveness rating must be documented in the relevant risk register.

2.16 Control effectiveness must be assessed by considering all of the identified key controls together, rather than rating each control individually.

2.17 The following guide (Figure 2) must be used in assessing control effectiveness:

Control Effectiveness Rating	Description / Guide
Fully Effective	Controls are well designed, largely preventive and address the root causes. Controls are effective and reliable at all times. Reactive controls only support the preventative controls. No more to be done except ongoing monitoring and periodic review of the existing controls.
Substantially Effective	Most controls are well designed, preventive and operating effectively. More can be done to improve control effectiveness, pro-activity and/or reliability.
Partially Effective	While the design of the controls may be good, they are not adhered to or effective in practice. Alternatively, controls are effective but not well designed or do not address root causes. There may be an over-reliance on reactive controls.
Largely Ineffective	There are significant gaps in the controls present. The controls may not address root causes, may not be preventive in nature, or may not be effective.
Totally Ineffective	The risk is not controlled. What control, if any, that does exist is ineffective in preventing risk events from occurring or mitigating their effects.

Figure 2: Control effectiveness table

Assessing Consequences

2.18 The potential consequences of each risk must be assessed and the reasonable worst (or best) case consequences are to be identified. When assessing the consequences of a risk event or situation, the existing controls, including their effectiveness, must be taken into account.

2.19 An event or situation can have positive or negative consequences and must be assessed using the NSW RFS five level scales, as shown in Figure 3 and Figure 4 below.

Negative Consequence Table (reasonable worst case)							
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 (>5 yr) significant environmental damage or clean up costs > $5 million	Financial loss or unrecompensed expense of >$30 million Fraud >$1m	Damage to corporate reputation at national or international level Major loss of community support	Parliamentary scrutiny/major government intervention Significant prosecution, fines or class action 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 (1-5 yr) significant environmental damage or clean up costs $1 to $5 million	Financial loss or unrecompensed expense of $10-$30 million Fraud >$500,000	Damage to corporate reputation at state or national level Significant decrease in community support.	Ministerial inquiry/government intervention Requires external legal assistance Prosecution by regulator Litigation 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 or 48 hours	Short term (<1 yr) environmental damage or clean up costs up to $1 million	Financial loss or unrecompensed expense of $1-$10 million Fraud >$50,000	Damage to corporate reputation at state or regional level Moderate decrease in community support	Regulatory breaches with investigation or report to authority with prosecution powers Requires intervention by senior management 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 unrecompensed expense of $100,000 to $1 million Fraud >$5,000	Damage to corporate reputation at regional or local level 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 Fraud <$5,000	Local awareness of an issue exists but there is no public concern	Minor compliance issues

Figure 3: Negative consequence table

*Includes impacts on all members, contractors and the public

Positive Consequence Table (reasonable best case)						
Consequence	**Safety Impact**	**Business Capability**	**Community Impact**	**Environmental Impact**	**Financial Impact**	**Reputational Impact**
5 Extreme	See reputational impact	Major increase in ability to deliver key services or resilience	> 1 week reduction in community impacts	See reputational impact	Saving or benefit of > $30 million	National or international recognition leading to major improvement in community support
4 Major	See reputational impact	Significant increase in ability to deliver key services or resilience	3 - 7 day reduction in community impacts	See reputational impact	Saving or benefit of 10-$30 million	National or state-wide recognition leading to significant improvement in community support
3 Moderate	See reputational impact	Moderate increase in ability to deliver key services or resilience	1 – 2 day reduction in community impacts	See reputational impact	Saving or benefit of $1 - $10 million	State-wide or regional level recognition leading to moderate improvement in community support
2 Minor	See reputational impact	Minor increase in ability to deliver key services or resilience	< 1 day reduction in community impacts	See reputational impact	Saving or benefit of $100,000 - $1 million	Regional or local recognition leading to some improvement in community support.
1 Insignificant	See reputational impact	Inconsequential increase in ability to deliver key services or resilience	Inconsequential reduction in community impacts	See reputational impact	Saving or benefit of < $100,000	No shift in community support

Figure 4: Positive consequence table

Assessing Likelihood

2.20 The likelihood of a risk leading to the assessed reasonable worst (or best) case consequence must be assessed and recorded in the relevant risk register.

2.21 When assessing the likelihood of a risk, the effectiveness of the existing controls must be taken into account.

2.22 Likelihood must be assessed using the NSW RFS five-level scale, as shown in Figure 5 below.

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

Figure 5: Likelihood table

Rating Risks

2.23 The level of risk is a combination of:

a. The assessed level of consequences; and

b. The associated level of likelihood of the reasonable worst (or best) case consequences arising.

The NSW RFS risk tables shown at Figures 6 and 7 below must be used for this purpose.

Note: Figure 6 shows the table for risks with negative consequences and Figure 7 shows the table for risks with positive consequences.

2.24 Using the tables, each risk (whether recorded in a risk register or otherwise identified) must be given a rating of critical, high, medium or low with a letter rating corresponding to the precise combination of likelihood and consequence relating to the risk (e.g. High-H1).

RISK RATING TABLE – NEGATIVE CONSEQUENCES						
	CONSEQUENCE					
LIKELIHOOD		INSIGNIFICANT 1	MINOR 2	MODERATE 3	MAJOR 4	EXTREME 5
	HIGHLY LIKELY 5	Low -L7	Medium -M4	High -H4	Critical -C4	Critical -C1
	LIKELY 4	Low -L8	Medium -M5	High -H5	High -H2	Critical -C2
	POSSIBLE 3	Low -L9	Low -L4	Medium -M3	High -H3	Critical -C3
	UNLIKELY 2	Low -L10	Low -L5	Low -L2	Medium -M2	High -H1
	HIGHLY UNLIKELY 1	Low -L11	Low -L6	Low -L3	Low -L1	Medium -M1

Figure 6: Negative consequence risk rating table

RISK RATING TABLE – POSITIVE CONSEQUENCES						
	CONSEQUENCE					
LIKELIHOOD	INSIGNIFICANT 1	MINOR 2	MODERATE 3	MAJOR 4	EXTREME 5
HIGHLY LIKELY 5	Low +L7	Medium +M4	High +H4	Critical +C4	Critical +C1
LIKELY 4	Low +L8	Medium +M5	High +H5	High +H2	Critical +C2
POSSIBLE 3	Low +L9	Low +L4	Medium +M3	High +H3	Critical +C3
UNLIKELY 2	Low +L10	Low +L5	Low +L2	Medium +M2	High +H1
HIGHLY UNLIKELY 1	Low +L11	Low +L6	Low +L3	Low +L1	Medium +M1

Figure 7: Positive consequence risk rating table

Potential Exposure

2.25 Potential Exposure is the plausible maximum impact on the NSW RFS that could arise from a risk, if controls were not applied or failed completely. It is expressed in terms of a consequence rating (using the negative and positive consequence tables) and, where assessed, must be documented in the relevant risk register or risk assessment.

Risk Evaluation

2.26 Once analysed, risks must be evaluated in order to determine:

a. If the risk is tolerable;

b. The most appropriate level of authority to manage the risk;

c. Whether further action is required to control the risk; and

d. The priorities for implementation of additional risk control actions.

2.27 Risk tolerance and the risk escalation process are described in SOP P7.1.10 – 3 Risk Tolerance and Escalation.

Controlling Risk

2.28 Where a risk is evaluated as not being tolerable to the NSW RFS, or requires further treatment, additional risk treatments must be developed. For those risks rated as “Critical” or “High”, a formal Risk Action Plan must be developed, approved by the Risk Owner (i.e. relevant Executive Director) and implemented. Significant risk treatments should be included in Business Plans, where appropriate.

2.29 Risk treatments should be considered using the following hierarchy:

a. Where a statutory, regulatory, compliance or policy requirement has been, or may be breached, action must be taken;

b. Where there is a risk to health and safety, action must be taken to eliminate or minimise the risk so far as is reasonably practicable; and

c. For the treatment of all other risks, action should be taken to reduce the likelihood or consequence, or both. Priority for attention should be given to risks with higher risk ratings and lower control effectiveness.

2.30 When identifying potential treatment options, further analysis of the risk is required to determine any gaps in the existing controls. The use of detailed risk analysis techniques should be considered e.g. cause and effect analysis.

2.31 Proactive, preventive risk treatments are preferred over reactive risk treatments, provided the benefits/advantages outweigh the costs (both monetary and non-monetary).

Communication and Consultation

2.32 Internal and external stakeholders must be communicated with and consulted. This should occur at all stages of the risk management process to assist in the capture of their experience, expertise and ideas as well as to develop their understanding of the risk.

2.33 This consultation will occur on a regular and ongoing basis.

Monitoring and Review

2.34 Each staff member responsible for managing an area of NSW RFS activity must:

a. Monitor the environment and activities in order to identify trends, changes and emerging issues that may have risk impacts, thus ensuring that all changes to the risk context are known and understood to the extent practicable;

b. Analyse all significant events, incidents, near-misses and related data in order to confirm the accuracy of risk ratings and the control effectiveness, likelihood and consequence ratings; and

c. Monitor controls to ensure that they are operating effectively and efficiently.

2.35 The NSW RFS Chief Audit Executive must use ORM to assist in the development of a risk-based Internal Audit Program and the annual Internal Audit Plan, ensuring that the Program and Plan are based on the NSW RFS Strategic Plan, Organisation Risk Management Plan and assessed risk profile. These Internal Audit plans must be endorsed by the Audit and Risk Committee and take into account organisational activities with higher Potential Exposure, low Control Effectiveness or Risk Ratings rated as Critical or High.

2.36 Additional control assurance processes may be introduced from time to time by Executive Management. These may result from a review of the NSW RFS Assurance Map.

Recording and Reporting

2.37 The risk management process and the outcomes must be documented and reported in order to provide information for decision-making and to inform the key stakeholders of risk management activities.

2.38 Documented information related to risk management activities is to be held in the current corporate approved NSW RFS record management system and in accordance with P5.1.6 Records Management.

2.39 The outcomes of risk management processes must be recorded in the relevant risk register. See SOP P7.1.10 – 2: Risk Registers

2.40 Risk reporting is outlined in SOP P7.1.10 – 4: Risk Reporting

3 Related forms

- None

SOP P7.1.10 - 2
Risk Registers – Format and Maintenance

1 Purpose

1.1 This Standard Operating Procedure (SOP) provides details of the types of NSW RFS risk registers, the relationships between them, the required format of these registers and the responsibilities of relevant officers to maintain these registers to ensure they remain accurate and up to date.

2 Procedures

Types of NSW RFS Risk Registers

2.1 There are three main types of Risk Registers within the NSW RFS: Organisational, Directorate and Business Unit/Specialised. These are interrelated, as shown by Figure 8 below.

2.2 The Organisational Risk Register and its subsidiary registers (Directorate, Business Unit and Specialised Registers) are the official record of NSW RFS risks.

2.3 Risks are recorded on the risk register where they are most appropriately managed. Where it is identified that the responsibility for managing a risk should change directorates, the change to the register must not be considered as finalised until validated by the receiving Executive Director.

2.4 Other risk registers may exist relating to specific purposes (such as fraud and corruption risk assessments) or risks attached to specific projects. These other registers may be used to support the Organisational Risk Register and its subsidiaries in a greater level of detail.

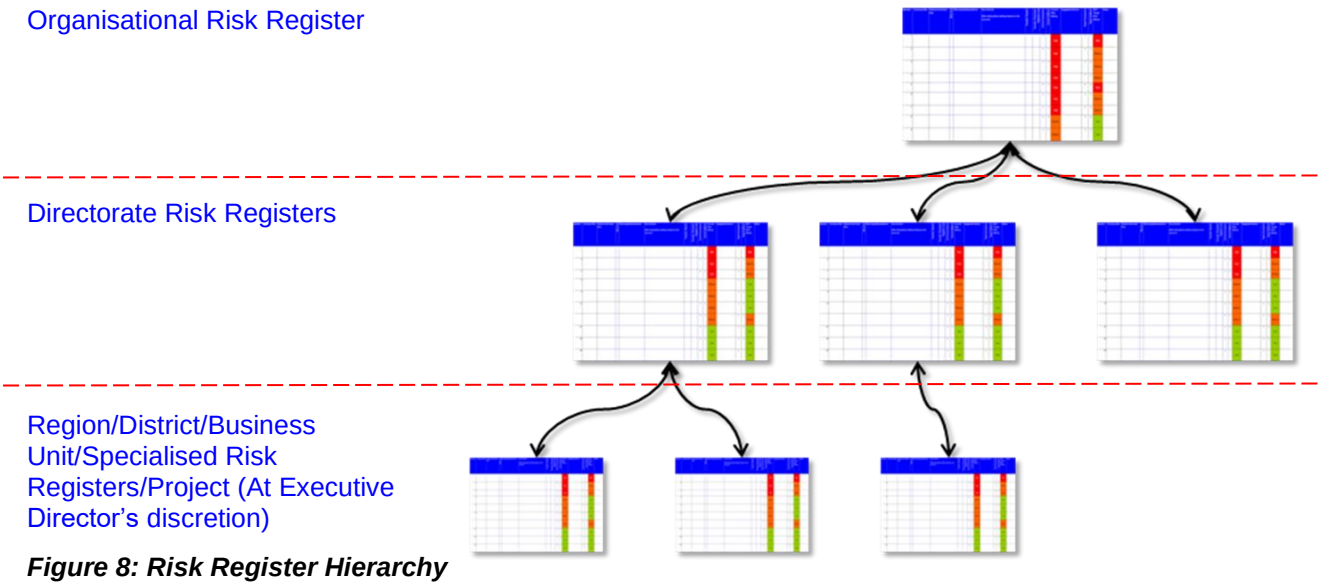

Figure 8: Risk Register Hierarchy

Format of Risk Registers

2.5 All NSW RFS Risk Registers must be maintained in the format determined by the Manager Planning, Risk and Policy in consultation with the Chief Risk Officer.

Organisational Risk Register

2.6 The Organisational Risk Register contains high-level risks with an organisation wide or broader strategic focus. It is the responsibility of the NSW RFS Executive team to ensure a review and update of the risks on this register is undertaken at least quarterly.

2.7 The Organisational Risk Register records the risk owner, usually at Executive Director level, who is primarily responsible for:

a. Ensuring appropriate controls are in place and operating effectively and efficiently;

b. Monitoring these risks; and reporting on the status of the risks and of progress in implementing risk treatment plans (Risk Action Plans).

Directorate Risk Registers

2.8 The Directorate Risk Registers are subsidiary to the Organisational Risk Register. They contain the directorate risks for which each Executive Director is the designated risk owner.

2.9 Where ownership of a risk is shared between Executive Directors, the risk must be recorded in the most relevant Directorate Risk Register. Controls and treatment plans (Risk Action Plans) must be negotiated and agreed by all co-owners and a Risk Action Plan Lead must be designated for the risk.

2.10 It is the responsibility of the relevant Executive Director to ensure that the Directorate Risk Registers are kept accurate and up to date. This will be done through:

a. Identifying and assessing changes in the environment that may affect NSW RFS objectives as they apply to the Directorate;

b. Assessing risks relating to new processes or functions that may affect the Directorate;

c. Assessing incidents, near misses and successes for root causes and lessons learned; and

d. Performing a formal assessment with the Directorate management team of all the Directorate's risks at least annually.

Business Unit and Specialised Risk Registers

2.11 An Executive Director may require an individual business unit to have its own Risk Register. A Business Unit or Specialised Risk Register is subordinate to the relevant Directorate Risk Register.

2.12 Business Unit or Specialised Risk Registers include risks that are applicable to that Business Unit or specialised function or activity, including program/project risks.

2.13 Risks may be recorded in a Business Unit or Specialised Risk Register at a more granular level, reflecting the context of each Register.

2.14 Each risk may be broken down into a set of sub-risks in the Business Unit or Specialised Risk Register if the relevant manager finds such an approach helpful for easier development of risk treatments or recording of controls.

2.15 It is the responsibility of the relevant Director / Manager to ensure that the Business Unit or Specialised Risk Register is kept accurate and up to date. This must be done through:

a. Identifying and assessing changes in the environment that may affect Business Unit objectives;

b. Assessing risks relating to new processes, functions or activities;

c. Assessing incidents, near misses and successes for lessons learned; and

d. Performing a formal assessment of all the unit's risks at least annually.

3 Related forms

› None

SOP P7.1.10 - 3
Risk Tolerance and Escalation

1 Purpose

1.1 This Standard Operating Procedure (SOP) details the readiness of the NSW RFS to bear a specified level of risk in order to achieve its objectives. It also provides the process for managing risk at the appropriate level within the NSW RFS. This includes escalating risk to the appropriate management level as required.

2 Procedures

Risk Tolerance

2.1 Risk tolerance determines, through an escalation process, at what level of accountability a risk is to be managed.

2.2 Where a statutory, regulatory, compliance or policy requirement has been, or may be breached, action must be taken.

2.3 Where there is a risk to health and safety, action must be taken to eliminate the risk or reduce it to as low as reasonably practicable.

2.4 Where a risk is rated as critical or high, a detailed and documented Risk Action Plan must be implemented by the responsible Executive Director.

2.5 Where a risk is rated as medium or low the responsible Executive Director must specify management responsibility for the implementation of appropriate risk mitigation action. For those risks rated as low, the response may be to take no action at this time and continue to regularly monitor the risk.

2.6 Risks, other than health and safety risks, must be treated as long as the benefits exceed the cost unless there is a legislative, regulatory, compliance or policy requirement that overrides this. Making an *informed* decision to accept a risk is also considered a risk treatment.

General Principles

2.7 A hazard may not give rise to a risk and may be eliminated through immediate treatment e.g. remove a trip hazard on a walkway.

2.8 Where a risk cannot be treated at the organisational level where it is identified, it must be escalated to the appropriate management level.

2.9 Taking into account the NSW RFS stated risk tolerance and escalation levels, risks should be managed at the lowest organisational level appropriate to the context and rating of the risk.

2.10 When an officer tasked with managing or monitoring a risk becomes aware of either:

a. A change in that risk's rating so that the risk now exceeds the NSW RFS tolerance and escalation levels that apply to his or her level of delegated authority; or

b. A newly identified risk that is rated at a risk level higher than the NSW RFS tolerance and escalation levels for his or her level of delegated authority,

the officer is required to immediately escalate that risk through the chain of command to the appropriate level of management.

2.11 The NSW RFS expresses risk tolerance levels and the associated escalation process as shown in Figure 9 below:

NSW RFS RISK TOLERANCE AND ESCALATION LEVELS	
RISK RATING	**ACTION REQUIRED**
Critical	**Escalate to Commissioner through chain of command** ▪ Allocate a Risk Action Plan Lead and implement a detailed action plan to address the risk ▪ Include on appropriate business plan as needed
High	**Escalate to Executive Director through chain of command** ▪ Allocate a Risk Action Plan Lead and implement a detailed Risk Action Plan to address the risk ▪ Include on appropriate business plan as needed
Medium	**Specify management accountability and responsibility** ▪ Monitor trends and plan for potential improvements. ▪ Implement a Risk Action Plan if appropriate.
Low	**Manage by routine procedures** ▪ Monitor trends; review costs and effectiveness. ▪ Implement a Risk Action Plan if appropriate.

Figure 9: NSW RFS Risk tolerance and escalation levels

Risk Escalation Procedure - by a NSW RFS Staff Member

2.12 Where a NSW RFS staff member identifies a hazard, potential new risk or a significant change to an existing risk, this risk or hazard must be immediately escalated to the appropriate level of management. This can be done via email to the appropriate level of NSW RFS management through the chain of command.

Risk Escalation Procedure - by a NSW RFS Volunteer Member

2.13 Where a volunteer member identifies a hazard, potential new risk or a significant change to an existing risk, the receiving staff member must immediately report, either verbally or in writing to the relevant District or other manager, through the chain of command. The manager must arrange for a risk assessment to be performed and either treat the risk locally or escalate to the appropriate level of management through the chain of command. Where the notification is reported verbally, the manager must make a record of the notification.

Feedback Procedure

2.14 The NSW RFS staff member to whom a risk is ultimately escalated must provide feedback to the member who originally raised the risk, advising the actions taken to assess and control the risk.

3 Related forms

› None

SOP P7.1.10 - 4
Risk Reporting

1 Purpose

1.1 This Standard Operating Procedure (SOP) details the process for the reporting of risk related activities.

2 Procedures

New or Revised Risks

2.1 All new or revised risks must be reported immediately to the appropriate level of authority as described in SOP P7.1.10 - 3 Risk Tolerance and Escalation.

Reporting Forms and Formats

2.2 In accordance with the Annual Reports (Departments) Regulation 2015, the risk management activities of the NSW RFS must be included in the Annual Report.

2.3 Quarterly corporate reporting of risk management activities must be in accordance with P7.1.4 NSW RFS Corporate Planning and Reporting, using the approved reporting templates.

Annual Attestation Process

2.4 In accordance with NSW Treasury Policy *TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector*, the Commissioner must furnish to the NSW Treasury, and publish in the NSW RFS Annual Report, an attestation statement regarding compliance with TPP15-03.

Annual Reporting to the Commissioner

2.5 The Executive Directors must report annually to the Commissioner on the following matters:

a. Attestation to compliance, in all material respects, with TPP 15-03 within their Directorate;

b. An analysis of any shifts in their Directorate's risk profile, including trends and emerging risks; and

c. An analysis of any significant environmental or major risk events affecting their Directorate or the NSW RFS and relevant lessons learned.

2.6 The Chief Risk Officer must report annually to the Commissioner regarding compliance by the NSW RFS with the core requirements of TPP15-03, relating to risk management.

Annual Reporting to Executive Directors

2.7 Directors and Managers who have the responsibility for managing a Business Unit or Specialised Risk Register must report to their Executive Director annually on the following matters:

a. Attestation of compliance, in all material respects, with TPP 15-03 within their Business Unit; and

b. An analysis of any shifts in their Business Unit's risk profile, including trends.

Annual Reporting to the Audit and Risk Committee (ARC)

2.8 The Commissioner must ensure that a report is made annually to the ARC that includes:

a. Attestations made in accordance with TPP 15-03;

b. Provision of the NSW RFS risk management framework;

c. An overview of organisational risks (inclusive of risks on the Organisational Risk Register, the directorate risk registers, Business Unit and Specialist Risk Registers.

d. An analysis of any shifts in the overall risk profile, including trends;

e. An indication of emerging risks;

f. Analysis of any significant environmental events;

g. Analysis of any significant relevant risk events, both within the NSW RFS and externally, and any lessons learned;

h. The NSW RFS level of risk maturity; and

i. The plans of the NSW RFS to maintain or improve the current risk maturity and the rationale behind those plans.

Quarterly Reporting to the ARC

2.9 The Commissioner must ensure that a report is made to the ARC each quarter that includes:

a. Progress made during the quarter in implementing actions to address all risks rated as critical or high, including all overdue treatment tasks;

b. An indication of emerging risks;

c. An overview of the NSW RFS risk profile from quarter to quarter and year to year;

d. Commentary on, and explanations of, any significant shifts in risks;

e. Notification of significant incidents, risk events and environmental changes; and

f. Notification of significant planned or implemented changes to the risk management framework.

Quarterly Reporting to the Commissioner

2.10 The Executive Directors must report to the Commissioner each quarter, as part of their quarterly performance reporting, on the following matters:

a. Progress made during the quarter in addressing all risks rated as critical or high for which they are the risk owner;

b. Commentary on, and explanations of, significant shifts in other risks;

c. Notification of significant incidents, risk events and environmental changes, if any, affecting or with the potential to affect the Directorate or the NSW RFS; and

d. The results of control assessment activities within their Directorate, including control self-assessments and internal audits.

Quarterly Reporting to Executive Directors

2.11 Directors and Managers who have the responsibility for managing a Business Unit Risk Register or a Specialist Risk Register must report to their Executive Director quarterly as part of their quarterly performance reporting on the following matters:

a. Progress made during the quarter against risk treatments or Risk Action Plans;

b. Any significant shifts in risks included in their risk register;

c. Any new business unit risks identified during the quarter;

d. Notification of significant incidents, risk events and environmental changes; and

e. The results of any control assessment activities within their Business Unit.

2.12 The designated Risk Action Plan Lead must coordinate reporting on the allocated risk to the appropriate Executive Director at least quarterly on the following matters:

a. Progress made against risk treatments or Risk Action Plans;

b. Any significant shifts in the risk; and

c. The results of any control assessment activities for the risk.

3 Related forms

- Quarterly Directorate Risk Reporting Template (stored on HPE)
- Business Plan and Reporting template (stored in HPE)