NSW Police Force

NSW Police Force Project Risk Management Guideline

Governance Command

Capability Performance and Youth Command

NSW Police Force Project Risk Management Guideline

The NSWPF Project Risk Management Guideline has been developed to better assist the organisation in understanding and managing project risks and issues.

Risk and issues management are core disciplines that underpin effective project management. They provide the base for effective and active decision-making in programs and projects. The purpose of the NSWPF Project Risk Management Guide is to:

a) Provide project teams with guidance on how to identify, assess, evaluate and manage project risks and issues;
b) Support the application of consistent risk and issue management processes across NSWPF;
c) Enable meaningful reporting and timely decision making on the basis of consistent and comparable data;
d) Improve overall transparency of project risks and issues; and
e) Provide NSWPF projects with greater alignment to the relevant and applicable industry standards and enterprise-wide frameworks (i.e., NSWPF risk management framework and supporting procedures, and Government requirements).

This guide sets the process and approach for managing risks and issues within NSWPF's projects in line with the risk management standard AS/NZS ISO 31000:2018 and defined with consideration to NSWPF's Enterprise Risk Management Framework and the NSW Treasury TPP 20-08 Internal Audit and Risk Management Policy for the General Government Sector.

Document Control Sheet

Document Properties

Title	NSWPF Project Risk Management Guideline
Subject	Project Risk
Command responsible	Governance Command
Authorisation	Commissioners Executive Team
Security Classification / Information Management Markings	Official
Publication date	June 2023
Current version number	V1
Review date	June 2024
Document number	D/2023/1182064 Linked RMS: D/2023/376162
Copyright statement	© Crown in right of NSW through NSW Police Force 2021
Suitable for Public Disclosure	Yes

Modification History

Version #	Version / approval date	Author/Position	Summary of changes
1	June 2023	Governance Command with Ernst & Young	Initial version
1	October 2023	Anning (RN: 30905)	RMS reference number updated.

Table of Contents

1. Purpose and Scope

The NSWPF Project Risk Management Guideline has been developed to better assist the organisation in understanding and managing project risks and issues.

A range of project management methodologies exist to organise and manage a project and each approach has its own principles, practices, and tools. The NSWPF does not have a preferred project management methodology and project managers should select the most appropriate project management methodology based on the nature, size and complexity of the project and their experience with project management.

Irrespective of the project management methodology selected, there are generally five phases in the project management process:

1. Initiation
2. Planning
3. Execution / Implementation
4. Monitoring / Controlling
5. Closure

Risk and issues management are core disciplines that underpin effective project management. They provide the evidence-base for effective and active decision-making in programs and projects. The purpose of the NSWPF Project Risk Management Guide is to:

a) Provide project teams with guidance on how to identify, assess, evaluate and manage project risks and issues;
b) Support the application of consistent risk and issue management processes across NSWPF;
c) Enable meaningful reporting and timely decision making on the basis of consistent and comparable data;
d) Improve overall transparency of project risks and issues; and
e) Provides NSWPF projects with greater alignment to the relevant and applicable industry standards and enterprise-wide frameworks (i.e., NSWPF risk management framework(s) and supporting procedures and Government requirements).

This guide sets the process and approach for managing risks and issues within NSWPF's projects in line with the risk management standard AS/NZS ISO 31000:2009 and defined with consideration to NSWPF's Enterprise Risk Management Framework.

Related Policies, Guidelines, Standards and Documents

- NSWPF Enterprise Risk Management Framework, Policy and supporting Procedure
- TPP 20-08 Internal Audit and Risk Management Policy for the General Government Sector
- TPG 22-12 NSW Treasury Policy and Guidelines: NSW Gateway Policy
- ISO:31000 (2018) - Risk Management Guidelines
- Police Handbook – Project Management

2. Project Risk Management Process

2.1. NSWPF Project Management

Within the NSWPF, a Minor project is a body of work and a planned process to implement a specific service, product, or result, with a budget equal to or less than $10,000. These projects will have a start and end date, a target or objective that will need to be achieved and specific deliverables.

Corporate projects are those meeting a specific criterion relating to strategic alignment (e.g., Our Focus Our Future, corporate sponsor portfolios); stakeholder involvement (e.g., community, other government agencies); organisational impact; resources; existing governance arrangements; and security and confidentiality. Corporate projects must be sponsored by an Assistant Commissioner or equivalent Senior Officer and included on the Corporate Project Register (CoPR), which is maintained by the Governance Command. Projects managed by existing NSWPF governance mechanisms (e.g. ICT Executive Board) will not be added to CoPR.

2.2. Risk Governance

Ownership and management of risk is key to successful project delivery. Project members all play a key role in understanding and identifying risks that impact intended project outcomes. In setting up governance structures and memberships, project teams should have clearly defined accountabilities and responsibilities for managing risks and issues.

2.3. Risk Identification

A **risk** is an uncertain event or set of events that, should they occur, would have an impact on the achievement of program objectives. Risks will always continue to emerge due to the increasing complexity and scope of the program, the changing nature of the environment and relationships with stakeholders.

In order to identify a risk, the internal and external environments need to be scanned to identify the risks to be subject to further analysis. In determining risks to the project, consider:

- Anything that challenge or enhance project objectives;
- Events that are outside the control of the project manager or the project team;
- Risks that are influenced by stakeholders and seek input from stakeholders; and
- Risks arising from external and internal environment characteristics (refer to **Table 1** below).

Table 1 – Project Risk characteristics

Context	Characteristics
External	Business, social, regulatory, cultural, financial and political environments
	Business drivers
	Third-party Supplier/Vendor strengths, weakness, opportunities and threats (from a project's perspective)
	External stakeholders
Internal	Culture

	Structure
	Capacity and Capabilities (pertinent to project scope and complexity)
	Inter-dependencies
	Business continuity and technology resilience
	Compliance
	Internal stakeholders

Mechanisms for identification of project risks

Risk identification can be undertaken in the following ways by the project:

- During periodic Risks status meetings with key project stakeholders
- Individual stakeholder consultation and engagement
- Preparation for Assurance Gateway reviews and other program milestones (e.g., Go/No-Go)
- Program management through day-to-day activities
- Active engagement and participation of the project's Risk Manager in key governance meetings
- Targeted and periodic Risk Workshops over the project delivery lifecycle
- Independent project reviews (e.g., Internal Audit, Assurance gateway reviews etc)

Projects should record the risk and related details in a timely manner including details such as the risk description, owner, risk rating, treatment plan etc, in a centralised project log (ServiceNow) that is maintained and monitored on a regular basis. Refer to the following sections to determine how risks should be assessed and managed, and **Appendix 2** for an Example Risk Register Template

2.4. Risk Assessment

Risk assessment is concerned with assessing the likelihood of the risk occurring, and its potential consequence to the project, should the risk occur. Risk assessment contributes to the development of an aggregated level of risk to a project and assists with prioritising risk management responses and mitigations.

The overall risk assessment process should consider:

- Identification of risks that may impact on the project objective;
- Risk rating - analysis of risk impact (see matrix in appendix) including definition of impacts;
- Risk likelihood assessment including definitions of likelihood (see matrix in appendix);
- Risk impact determined based on an assessment framework (minor, moderate, major); and
- Risk treatment – develop actions to reduce moderate and major risks.

The risk ratings can be calculated according to the assessment of the likelihood and consequence, whilst aligning to the NSWPF Enterprise Risk Management matrix (**Appendix 1**). The overall rating indicates the level of risk.

Risk ratings assist the Risk Owner to determine which risks should be prioritised for treatment, and where Executive level oversight of risks should occur within the project.

2.5. Risk Treatment

Once the risks have been identified and assessed, a response needs to be developed in accordance with the rating determined during assessment. The key steps in this process involve the following:

- **Determine the resolution approach** against the available treatments. Consider the following factors:
  a. Time required to implement the resolution
  b. The cost of the resolution
  c. Target Risk Rating
     - Assessing the possible consequences/impact.
     - Estimating the likelihood of a risk eventuating after considering existing controls and treatments.
- **Prepare treatment plans** in line with the selected treatment option, responsible owner and when the treatment will need to be completed by. For further details on risk treatment options, refer to the **NSWPF Enterprise Risk Management Procedure** 'Evaluate and decide the treatment for the identified risks' section.
- A Target Risk Rating may also be considered by:
  - Assessing the possible consequences/impact.
  - Estimating the likelihood of a risk eventuating after considering existing controls and treatments.

Refer to the **Appendix 1** for the Risk Rating Matrix.

3. Project Issue Management Process

3.1. Issue Identification

An **issue** is a risk or vent that has materialised that may affect achievement of project's objectives, the impact of the issue needs to be assessed to determine the appropriate response.

Issues require management action and treatments to be implemented in a timely manner and with minimal impact on the program.

3.2. Issue Management

Issue ratings should assess the overall impact of the issue and urgency to plan for adequate treatment to resolve and/or minimise impact on the project. Issues should be captured within a centralised Issues Log/Register that is maintained and monitored on a regular basis.

Issues should be assigned an owner, treatment date, rating and action(s) for management.

3.3. Issue Treatment

Once issues have been identified and assessed, a response needs to be developed in accordance with the rating determined during assessment. These responses are known as treatment actions. The key steps in this process should consider:

a) Determining the **resolution approach** and developing treatment options with respect to:
  - Time required to implement the resolution.
  - The cost of the resolution.

b) Preparing **treatment actions** in line with the priority of the issue, who will be responsible, expected outcomes and when the treatment will be completed.

c) Outlining whether or not a **project decision** is required, and whether the decision will be made through relevant levels in the project's governance structure.

4. Monitor and Report

The overall project risk and issues monitoring and review approach should be designed to ensure that risks and issues are being managed and reported at the right level, supported through effective communication and consultation. Key considerations include:

- **Risk owners** – ownership of risks should be clearly defined with clear responsibilities and accountabilities considered i.e.:
  - who will be responsible to monitor the risks and corrective actions
  - how often will the risks be reviewed (e.g., during periodic working group meetings?)
- **Key governance groups** are provided with adequate transparency to enable effective decision-making. Timely and adequate views of project risks and issues should be reported i.e., through existing cadence of project meetings, status reporting or established escalation paths.
- **An integrated project risk and issues log/register** is maintained and updated timely and accurately to facilitate effective risk and issue management and timely decision-making.
- Determining whether internal/external **dependencies** and **impacts** exist for identified issues and risks.
- **Periodic formal risk assessments**, based on the needs of the project.
- **Assurance requirements** – alignment with internal and/or external assurance processes and requirements (e.g., NSW Gateway Policy), where applicable.

As the project evolves, the risk and issues monitoring and reporting processes should be assessed and revised to ensure it continues sufficiently meet the needs of the project.

Minor Project Management templates are available on the NSWPF Intranet – Forms - Project Management (non-ICT), and are designed to guide staff through small, non-ICT related projects. It is recommended staff use RMS to manage all project documentation during this process.

Corporate projects must be recorded on the Corporate Project Register (CoPR). Project Managers will be required to submit monthly project status reports, including risks to the project, until the project is finalised and a closure report is submitted. Projects on CoPR will be monitored by the Governance Command and status updates reported to the Senior Executive.

Appendix 1 NSWPF Risk Matrix and Scales

		Impact				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	Medium	Medium	High	Extreme	Extreme
	Highly Likely	Low	Medium	High	High	Extreme
	Possible	Low	Low	Medium	High	High
	Unlikely	Very Low	Low	Low	Medium	High
	Rare	Very Low	Very Low	Low	Low	Medium

	Likelihood Qualitative (perception, not measured)	Likelihood Quantitive (Probability)
L5 - Almost Certain	Expected to occur during the project	Over 95%
L4 - Highly Likely	Will probably occur during the project	70% - 95% probability of occuring
L3 - Possible	Might occur during the project	30% - less than 70% probability of occuring
L2 - Unlikely	Conceivable but highly unlikely to occur during the project	5% - less than30% probability of occuring
L1 - Rare	Probably won't occur during the project	Less than 5%

Consequence (Impact)					
	C1 - Insignificant	**C2 - Minor**	**C3 - Moderate**	**C4 - Major**	**C5 - Severe**
Scope (Impact on baseline)	Forercasting minor variation in scope and / or functionality w ithout project/program impact	Forecasting minor variation in scope and / or functionality, w ith limited project/program impact	Forecasting variation in scope and / or functionality, requiring project/program re-baselining	Forecasting variation in scope, functionality requiring client / sponsor approval	Forecasting major project variation not able to continue w ithout substantive reduction of scope and / or functionality
Schedule (Impact on baseline)	Forecasting a minor recoverable slippage on a non critical task. Variance< = 1%	Forecasting a minor recoverable slippage on a critical task. Variance over 1%	Forecasting an unrecoverable slippage leading to a delay of planned Phase Exit. Variance over 5%	Forecasting delay of release or deployment. Variance over 15%	Forecasting severe slippage leading to a delay in Program Critical Path. Variance over 40%
Budget (Increase by)	Forecasting a minor cost variance / acceptable impact on financial position of project/program Variance < = 1% of budget	Forecasting a minor cost variance w ithin Program budget / acceptable impact on financial position of Project/Program Variance over 1% of budget	Forecasting a major cost impact requiring project/program re-baselining. Variance over 5% of budget	Forecasting major cost impact leading to project/program re-baselining and draw ing dow n on contingency Variance over 15% of budget	Forecasting a critical cost impact resulting in contingency being exhausted. Variance over 40% of budget
Quality	Forecasting minor variation in quality w ithout Program impact and solution still fit for purpose.	Forecasting minor variation in quality w ith a program impact but solution still fit for purpose.	Forecasting major variation in quality requiring client / sponsor approval due to project/program impact and fit for purpose impact.	Severe quality failure, impacting upon business operations, manual remediation required	Critical quality failure, impacting upon business operations, unable to be remediated.
Benefits	Forecasting minor variation in benefits delivery but still w arrants continuing the project/program.	Forecasting moderate variation in benefits w ith a project/program impact and still w arrants continuing the project/program.	Forecasting major variation in benefits w ith a project/program impact requiring client / sponsor approval.	Forecasting major variation in benefit delivery requiring client / sponsor approval.	Forecasting major variation, project not able to continue w ithout substantive re-baselining of project/program benefits.

Appendix 2 Example Risk Register Template

Risk #	Risk Description	Risk Rating	Risk Responsibility	Planned Treatment Options	Status
	Identify the risk and provide a brief description. What project objectives could this risk hinder or assist? e.g. Outdoor community engagement event – wet weather	★	Who is the person responsible for managing this risk? e.g. Snr Cst Smith	List all activities planned or identified as being required to further control or mitigate this risk. e.g. Hire marquees and advertise contingency plans	Progress and Comments e.g. In progress

Appendix 3 Glossary

Term	Definition
Chief Risk Officer	Chief Risk Officer (CRO) is a person that has designated responsibility for designing the agency's risk management framework and for the oversight of activities associated with coordinating, maintaining and embedding the framework in the agency.
Corporate Internal Audit Director	Is a person within an agency (apart from an approved Shared Arrangement) who heads the internal audit function and is responsible for providing strategic leadership and managing the internal audit function within the agency.
Corporate Risk Assessment & Management System (CRAMS)	Corporate Risk Assessment and Management System
Compliant	Compliant means that the agency has implemented and maintained practices consistent with the Core Requirements of the Policy for the whole of the financial year.
Controls	Controls refers to existing processes, policies, devices, practices or other actions which maintain and/or modify risks.
CoPR	Corporate Project Register (accessed via Blue Portal)
Internal Audit	Internal audit means 'an independent, objective assurance and consulting activity designed to add value and improve an agency's operations. It helps an agency accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.
Mandatory Requirements	Mandatory Requirements are the points listed below each of the Core Requirements and are required to be followed by the Accountable Authority for an agency in order to implement the Core Requirements, with the exception of Practice Notes.
Non-compliant	Non-compliant means the agency has not been compliant with one or more Core Requirements or Mandatory Requirements of the Policy for the whole or part of the financial year.
Project	A temporary undertaking to create a product / service or achieve an objective
Risk	Risk is the effect of uncertainty on objectives. (Note: effect is a deviation from the expected and may be positive and/or negative). Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.
Risk Appetite	Risk appetite means the amount or level of risk the organisation is willing to accept or retain to achieve its objectives
Risk Management	Risk management refers to the coordinated activities to direct and control an agency with regards to risk.
Risk Management Audit Committee (RMAC)	RMAC is a committee established in accordance with the Policy to monitor, review and provide advice and guidance about the agency's governance processes, risk management and internal control frameworks and external accountability obligations.
RMAC Charter	Audit and Risk Committee Charter sets out the roles and responsibilities of the ARC with respect to monitoring, reviewing, and providing advice on the agency's governance processes, risk management and control frameworks and its external accountability obligations.
Risk Management Framework	Risk management framework refers to the set of components for integrating, designing, implementing, evaluating and improving risk management throughout an agency.

Risk Management Process	Risk management process is the systematic application of policies, procedures and practices to the tasks of communication, consultation, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.
Risk Management Plans	Risk management plans identify the strategy, activities, resources, responsibilities and timeframes for implementing and maintaining risk management in an agency.
Risk Treatment	Risk treatment is a process to modify risk.
Risk Tolerance	Risk tolerance refers to the levels of risk taking acceptable to achieve a specific objective or manage a category of risk
ISO 31000	Best practice Risk Management Guidelines