



## AFP National Guideline on risk management

### 1. Disclosure and compliance

This document is classified **UNCLASSIFIED** and is intended for internal AFP use.

Disclosing any content must comply with Commonwealth law and the [AFP National Guideline on disclosure of information](#).

#### Compliance

This instrument is part of the AFP's professional standards framework. The [AFP Commissioner's Order on Professional Standards \(CO2\)](#) outlines the expectations for appointees to adhere to the requirements of the framework. Inappropriate departures from the provisions of this instrument may constitute a breach of AFP professional standards and be dealt with under Part V of the [Australian Federal Police Act 1979](#) (Cth).

### 2. Acronyms

<b>AFP</b>	Australian Federal Police
<b>AS/NZS ISO</b>	Australian Standards/New Zealand Standards International Organization for Standardization
<b>CO2</b>	AFP Commissioner's Order on Professional Standards (CO2)
<b>RM</b>	Risk management
<b>SES</b>	Senior Executive Service
<b>SLG</b>	Senior Leadership Group

### 3. Definitions

**Appointee** - is defined in s. 4 of the [Australian Federal Police Act 1979](#) (Cth).

**Control** - a measure modifying a risk. Controls may include any process, policy, device, practice, or other actions which modify risk. A control is something that is currently in effect, as opposed to a risk treatment, which is a control not yet implemented.

**Control rating** - a rating designed to describe the perceived effectiveness of a control in managing a risk.

**Consequence** - the outcome of an event affecting objectives.

**Event** - occurrence or change of a particular set of circumstances. In the AFP context an event is the actual occurrence of a risk.

**Likelihood** - the chance of something happening.

**Probability** - a measure of the chance of occurrence.

**Required actions** - the minimum actions to be taken based on the risk rating.

**Risk** - the effect of uncertainty on objectives. Risk is often measured in terms of likelihood and consequences.

**Risk appetite** - the amount and type of risk that the AFP, as an organisation, is willing to pursue or retain.

**Risk assessment** - the overall process of risk identification, risk analysis and risk evaluation (refer [AFP Risk Management Toolkit](#)).

**Risk Champion** - a position or appointee that has a role secondary to their substantive role focussed on promoting awareness, understanding and compliance with the AFP Risk Management Framework.

**Risk management** - the coordinated activities to direct and control an organisation with regard to risk.

**Risk Management Framework** - the set of components that provide the foundations and AFP arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

**Risk Management Plan** - the scheme within the Risk Management Framework that specifies the approach, management components and resources to be applied to manage risk. For AFP purposes it is this guideline and the AFP Risk Management Toolkit.

**Risk owner** - person or entity with the accountability and authority to manage a risk. For AFP purposes, this is the person notified of the risk in accordance with the 'required actions' process listed in ss. 10.9 and 10.10 of this guideline.

**Risk register** - the record of information about identified risks which also identifies whether a risk requires treatment (refer to the [AFP Risk Management Toolkit](#)).

**Risk treatment** - a process to modify risk. In the AFP risk assessment process, a risk treatment is something proposed or planned, typically to reduce the likelihood and/or consequence of a risk. A risk treatment can also be designed to share or avoid the risk, or remove the risk source.

**Risk tolerance** - the AFP or a stakeholder's readiness to bear a risk, after treatment, to achieve its objectives.

**Risk treatment schedule** - a document containing strategies to reduce risk.

**Security assessment** - an assessment of threat, countermeasures effectiveness, vulnerabilities and security risks relating to a business area's concept of operations and current practices.

**Senior Executives** - a collective term for all AFP manager and above positions throughout the AFP.

**Strategic risks** - those risks that could prevent or severely disrupt achieving the AFP mission, Portfolio Budget Statement key outcomes and Ministerial Direction key strategic priorities, or bring into question the AFP's ability to do so. These risks are typically whole-of-organisation type risks, or Function/program risks of such significance as to warrant Strategic Leaders Group oversight.

**Strategic risk profile** - a description of strategic risks relating to the AFP, used to inform AFP senior management decision making.

**Threat assessment** - an assessment of those entities (persons or organisations) that have an intent and capability to cause harm to AFP information, resources, people, assets and reputation.

## 4. Guideline authority

This National Guideline was issued by the National Manager Policy and Governance using power under s. 37(1) of the [Australian Federal Police Act 1979](#) (Cth) as delegated by the Commissioner under s. 69C of the Act.

## 5. Introduction

This guideline and related risk management advice (e.g. the Risk Management Toolkit) is a Risk Management Plan as defined by the Australian, New Zealand and International Standard on risk management (AS/NZ ISO 31000:2009).

This guideline outlines the obligations, policies and procedures for a common approach by all appointees to managing risks that may impact upon the AFP achieving its objectives. The guideline is supplemented by a more detailed [AFP Risk Management Toolkit](#).

In addition to the provisions contained within this guideline, appointees must note legislative risk management obligations, such as those dealing with occupational health and safety and fraud control.

Any deviation from this National Guideline requires clearance from the owner of this National Guideline - the National Manager Policy and Governance. Deviation will only be granted in exceptional circumstances dictated by specific business needs (for example, when working in collaboration with other Australian Government or International agencies).

## 6. Policy

The AFP risk management policy is:

- the AFP will provide the necessary tools, techniques and training to undertake risk assessments
- all appointees are responsible for managing risks
- appointees have specific responsibilities to ensure timely and successful implementation of risk management processes
- the risk management process involves self-assessment, based on the premise that individual Functions and business or operational areas are best placed to identify, evaluate and prioritise relevant risk treatments
- specific projects (e.g. those managed under the Prince2 methodology) are subject to additional reporting or project management governance (consistent with this National Guideline) as determined by project managers or respective project Boards of Management in accordance with Program Management Office requirements
- all key risk exposures, current controls and respective risk treatments must be recorded in risk registers and treatment schedules
- AFP risk registers and risk treatment schedules must demonstrate clear accountability for accepting risks and risk treatments
- escalating individual risks or risk categories to relevant committees or individuals with specific risk management roles and responsibilities allows for informed and coordinated decision making

## 7. Risk management principles

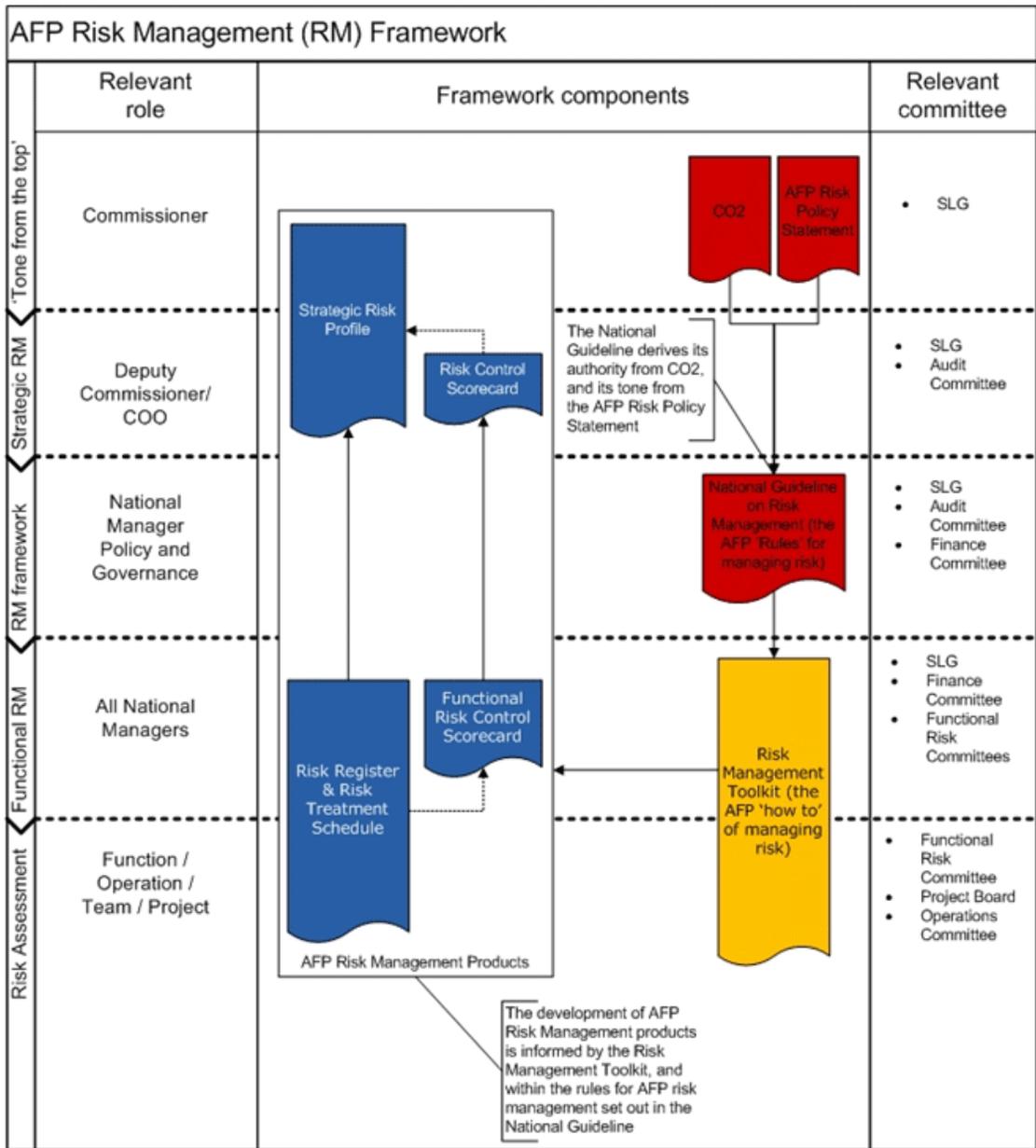
The AFP Risk Management Framework is based on key principles that the AFP will:

- apply risk management practices across the AFP in a systematic, consistent and cost effective manner
- identify and manage all reasonable risk exposures

- integrate risk management practices with business planning and other whole-of-AFP activities including business continuity, fraud control and internal and external audits
- ensure risk management adds value to the AFP by enabling evidence-based decision making and strategic direction setting
- have risk management processes at all levels that will be able to withstand internal and external scrutiny.

## 8. Risk management framework

The AFP's Risk Management Framework is the set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. For example, it includes risk management policy, procedures, templates, responsibilities, culture, training and awareness. The main components of the Framework are depicted diagrammatically below:



## 9. Roles and responsibilities

The Commissioner is ultimately accountable and responsible for managing AFP risk.

All appointees are accountable for, and have a responsibility to, identify, communicate and respond to risks relevant to their specific areas of work. They must:

- proactively assess and document identified risks to the achievement of key business outcomes
- promptly act to manage and communicate identified risks per the principles in this guideline.

## 9.1 Senior Executives

All Senior Executives must establish and maintain an effective risk management culture and set expectations in managing risk throughout the AFP.

## 9.2 Strategic Leaders Group

The Strategic Leaders Group (SLG), by way of inclusion of risk on the SLG agenda, must monitor and assess the AFP's Risk Management Framework by:

- ensuring existing and emerging key risks have been identified and treated appropriately
- reviewing the AFP's strategic risk profile to ensure it remains current and focused on the areas of greatest risk
- monitoring the risk appetite of the AFP.

## 9.3 National Managers

All National Managers must:

- contribute to the AFP risk management culture through modelling adequate risk awareness and compliance
- approve Functional risk registers and risk treatment schedules
- clearly document overall responsibility for accepted risks and the implementation of functional risk treatments
- establish a Functional Risk Committee or at a minimum ensure an alternative Functional committee maintains a standing agenda item of risk management
- ensure the Function contributes to the AFP risk management culture through adequate risk awareness and compliance
- ensure alignment of Functional risk registers and treatment schedules with Functional business plans
- ensure risk reporting obligations are met, including escalation to Deputy Commissioner's as set out in s. 10.9 of this guideline
- identify a suitable SES-level Functional risk champion.

## 9.4 Managers and supervisors (including Office Managers, Airport Police Commanders, Station Managers and International Deployment Group Mission Commanders)

All managers and supervisors must:

- contribute to the AFP risk management culture through modelling adequate risk awareness and compliance
- manage risks through periodic risk assessment of key objectives or activities, including new initiatives
- support and encourage staff to manage risks by documenting risk identification, assessment and treatments to maintain audit trails
- ensure there is active participation in the risk management process by a wide cross-section of stakeholders
- establish a Risk Management Committee for office, station, mission or operation, or ensure that risk matters at this level are considered by a Function-level Risk Management Committee
- ensure formal risk assessment processes are completed as required (e.g. for major investigation plans, standard tactical plans, fraud control, occupational health and safety, etc.)
- approve relevant risk registers/treatment schedules (e.g. at the office, station, mission, operation or team level) and assume

- responsibility for monitoring accepted risks and implementing risk treatments
- ensure risks are escalated in accordance with the relevant risk rating and subsequent required actions.

Supervisors must ensure their staff, including independent contractors and consultants, are aware of and adhere to this guideline.

## 9.5 AFP Audit Committee

Per the Audit Committee Charter, the Audit Committee must:

- review whether management has in place a current and comprehensive risk management framework, and associated procedures for effective identification and management of AFP's financial and business risks, including fraud
- review whether a sound and effective approach has been followed in developing strategic risk management plans for major projects or undertakings
- review the impact of AFP's risk management framework on its control environment and insurance arrangements
- review whether a sound and effective approach has been followed in establishing AFP's business continuity planning arrangements, including whether disaster recovery plans have been tested periodically
- review the AFP's fraud control plan and satisfy itself the AFP has appropriate processes and systems in place to capture and effectively investigate fraud related information.

## 9.6 Risk management committees

Risk management committees or equivalent committees must:

- monitor and review alignment between risk registers/risk treatment schedules and Functional business plans or Office action plans
- ensure Functional risk registers/risk treatment schedules reflect key corporate, operational and project risks within the Function
- report quarterly to the relevant National Manager and/or Operations Committee on risk management and as required for Performance and Budget Monitoring Committee reporting.

## 9.7 Strategic Risk Management Team

The Strategic Risk Management Team must:

- promote risk management awareness and facilitate communication, training and development of appointees on risk management
- independently monitor the AFP's risk management environment, including continuous improvement and value-adding
- review adherence to, and effectiveness of, risk management policies, framework and reporting
- advise and direct AFP risk management to ensure consistency with this guideline
- conduct quality assurance checks on risk assessments as required to ensure consistent application of risk management and high quality products throughout the AFP
- manage non-compliance issues
- engage risk champions to facilitate Risk Management Framework continuous improvement
- provide risk management reports to the Audit Committee and the SLG as required.

## 9.8 Project managers

Project managers must:

- be actively involved and accountable for the delivery of the risk management framework within their respective project areas
- maintain a project risk register and, where treatments are required, a risk treatment schedule in accordance with this National Guideline
- pay particular attention to dependent projects and programs, and if part of a program, meet regularly with other project managers to review existing and emerging risks and treatments
- escalate project risks in accordance with the relevant risk ratings and subsequent 'required actions'
- ensure risk management is an integral component of the project management process and regularly reviewed for the life of the project
- promote a strong risk management culture within their project area and ensure project members are familiar with the requirements of this National Guideline
- proactively monitor and review the effectiveness of controls and implementation of treatments
- adhere to other project-specific risk related activity that may be defined by the Portfolio Management Office, such as reporting to project Boards of Management and/or program managers.

## 9.9 Risk Champions

SES-level Risk Champions must:

- integrate and promote risk management within relevant high-level fora, such as operations, business and risk committees
- oversee Functional compliance with the AFP Risk Management Framework.

Non SES-level Risk Champions must:

- be the Functional point of contact for risk management advice
- raise awareness of, and ensure participation and involvement in risk management activity
- liaise with the Strategic Risk Management Team on risk management issues.

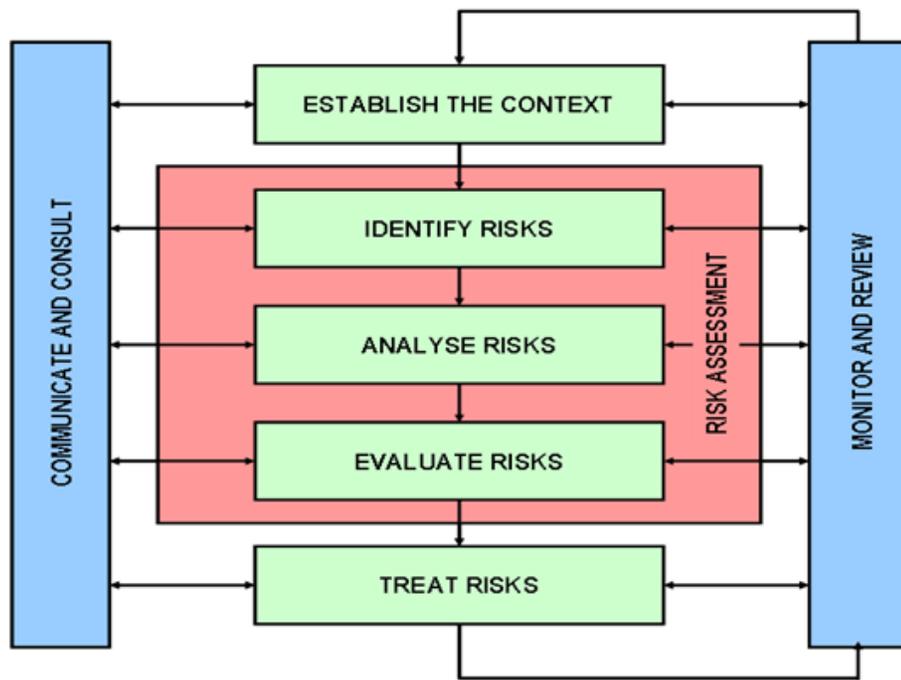
## 10. Risk management process

Procedures and practices for managing risks in the AFP must be:

- consistent with the Australian, New Zealand and International Standard 31000:2009 series (AS/NZS ISO 31000)
- compliant with the steps shown in the flowchart below and specific information and action requirements, such as the use of likelihood and consequence ratings, the AFP risk matrix, and taking the stipulated required action based on the risk rating.

Appointees must refer to the Risk Management Toolkit (AFPHUB) for detailed advice on process steps.

### **Risk management process**



### 10.1. Communicate and consult

Risk assessments must include detailed communication and consultation with internal and external stakeholders. All relevant stakeholders, including those accountable for implementing the risk management process or who are affected by it must be consulted.

The 'communicate and consult' element exists in parallel with all other steps of the risk management process.

### 10.2. Establish context

The context of the risk assessment must be clearly defined in risk management documentation. The documentation must clearly state:

- objectives or goals threatened by risk
- scope of the risk assessment
- specific assumptions or limitations.

### 10.3. Identify risks

Identifying risk is the first step of the actual risk assessment phase, which includes risk identification, risk analysis and risk evaluation.

Appointees conducting the risk assessment must:

- describe the risk (what can happen that could prevent, degrade or delay the achievement of objectives)
- detail for each risk, the potential causes/sources (how/why can the risk occur)
- detail for each risk, the potential impacts (what will be the impact if a risk event does occur, or why this is a risk).

Risk impacts can be used from the 'Description of impacts scale' or developed separately depending on the context of the risk assessment. Risk impacts will influence the consequence rating.

## 10.4. Analyse risks

Appointees must use the controls, probability/likelihood, and consequence ratings and risk level matrix in this section. The risk level matrix applies to risks irrespective of whether risks relate to operations, projects, and non-operational (or administrative type) activity, programs, portfolios, or the organisation as a whole (see also the probability/likelihood and consequence descriptors).

Appointees must analyse risks by first identifying and evaluating existing controls (typically what is either in place to prevent the risk event occurring or to reduce the impact of a risk event).

Some avenues supporting this analysis include:

- focus group discussions
- post-event reports
- expert judgement
- structured interviews
- available data or intelligence.

Appointees must consider the strength of controls as an integral component of the risk analysis phase because:

- they will influence likelihood and consequence ratings
- weak or incomplete controls may not reduce the probability/likelihood of a risk occurring, or not reduce the consequences if a risk event does occur.

Appointees must document the strength of controls for each risk and use the following control ratings:

### Control ratings - Assessment of effectiveness

Rating	Description
Unknown	Risk author does not have sufficient knowledge to determine the strength of a control.
Weak	Low control of risk or significant improvement required on newly identified risk.
Incomplete	Actions already established to address known control weaknesses but not fully implemented.
Adequate	Control is effective in mitigating risk, but further improvement may be desirable.
Strong	Control is believed to be operating effectively with no further improvement required.
Over-controlled	Room for efficiency improvements/cost reduction opportunities.

## 10.5. Determining risk probability/likelihood

Appointees analysing risk must:

- after assessing control effectiveness, consider the probability or likelihood of the risk occurring
- use the following scale:

### Probability/likelihood scale

Measure	Description
Almost certain	<b>Probability:</b> There are indicators that the event is imminent or the event may already be happening, and/or high level of recorded incidents and/or strong anecdotal evidence, and/or a strong likelihood the event will reoccur <b>Likelihood:</b> Is expected to occur in most circumstances.
Likely	<b>Probability:</b> There are indicators to suggest that this event is likely to occur if current conditions remain or data/intelligence predictions are accurate, and/or regular recorded incidents, and/or considerable opportunity, reason or means to occur. <b>Likelihood:</b> Will probably occur in most circumstances.
Possible	<b>Probability:</b> There are indicators to suggest that the potential for this event to occur may increase if not managed effectively, and/or few, infrequent or random recorded incidents. <b>Likelihood:</b> Might occur at some time.
Unlikely	<b>Probability:</b> No or minimal indication of potential occurrence under current conditions, or as shown by available data/intelligence. <b>Likelihood:</b> Not likely to occur.
Rare	<b>Probability:</b> No indication of potential occurrence under current or foreseen conditions or as shown by available data/intelligence. <b>Likelihood:</b> May occur only in exceptional circumstances.

## 10.6. Determining event impacts

After rating the risk probability/likelihood, appointees must list the potential impacts if a risk event occurs.

s47E(d)

s47E(d)

s47E(d)

s47E(d)

s47E(d)

s47E(d)

s47E(d)

## 10.8. Assigning a risk level rating

Appointees must, based on probability/likelihood and consequence ratings use the risk level matrix below to assign a risk level for each risk.

### Risk level matrix

<b>L I K E L I H O O D</b>	<b>ALMOST CERTAIN</b>	<b>Low</b>	<b>Medium</b>	<b>Significant</b>	<b>High</b>	<b>Critical</b>
	<b>LIKELY</b>	<b>Low</b>	<b>Medium</b>	<b>Significant</b>	<b>High</b>	<b>High</b>
	<b>POSSIBLE</b>	<b>Low</b>	<b>Medium</b>	<b>Medium</b>	<b>Significant</b>	<b>Significant</b>
	<b>UNLIKELY</b>	<b>Low</b>	<b>Low</b>	<b>Medium</b>	<b>Medium</b>	<b>Medium</b>
	<b>RARE</b>	<b>Low</b>	<b>Low</b>	<b>Low</b>	<b>Medium</b>	<b>Medium</b>
		<b>INSIGNIFICANT</b>	<b>MINOR</b>	<b>MODERATE</b>	<b>MAJOR</b>	<b>SEVERE</b>
<b>CONSEQUENCE</b>						

The risk level determines responsibility for managing risks and escalation/accountability through 'required actions' as shown below.

## 10.9. Evaluate risks

Risks must be assessed as either acceptable or not acceptable. If a risk is unacceptable, it must be treated.

The risk owner or higher authority ultimately determines whether a risk is acceptable or not. A risk may be considered acceptable if, for example:

- the risk is sufficiently low that treatment is not considered cost effective
- a treatment is not available (e.g. a project terminated by a change of government)
- a sufficient opportunity exists and outweighs the potential level of risk.

Appointees must, dependant upon the context of the risk assessment and the risk rating (i.e. the sum of likelihood and consequence levels), take the required escalation/briefing action as shown in the following table.

This table does not limit escalation. 'Required actions' can be further escalated as required.

s47E(d)

s47E(d)

s47E(d)

## 10.11. Treat risks

Risk treatments must be balanced against expected benefits and cost-effectiveness.

Risk treatments must be documented in the risk treatment schedule.

Treatments and resulting monitoring must be included for risks assessed as 'Medium', 'Significant', 'High' or 'Critical'. Where it is determined that treatments will not be implemented (for example where a treatment is not available or not cost effective) the reasons for non-implementation must be documented.

## 10.12. Documenting risk management

Appointees must document the AFP risk management processes sufficiently to demonstrate compliance with AFP process and principles including:

- identifying the risk assessment objective and context
- listing the stakeholders consulted
- assessing the sources and impacts of risks, and likelihood, consequence and risk levels
- documenting a schedule of controls in place and any necessary strategies or options to treat risks, including responsibilities for implementation and monitoring.

The level of documentation maintained should reflect the nature and formality of the risk management process.

Risk management documentation (e.g. risk registers and risk treatment schedules etc.) must clearly identify risk assessment approval, including:

- acceptance of residual risk levels
- overall responsibility for determining and implementing the most appropriate risk treatments.

The Risk Management Toolkit contains templates for AFP risk registers and risk treatment schedules.

Given the sensitivity of some risk assessments, all documentation must be handled in accordance with records management and security requirements (refer [AFP Practical Guide on the Security Classification of information](#)).

## 11. Further advice

Queries about the content of this guideline should be referred to the Coordinator Planning and Governance, Team Leader Risk Policy or Team Leader Risk Implementation.

## 12. References

### Legislation

- [Australian Federal Police Act 1979](#) (Cth)

### AFP governance instruments

- [AFP Practical Guide on the Security Classification of Information](#).

### Other sources

- AS/NZS ISO 31000:2009 - Australian/New Zealand Risk Management Standard
- [Fraud Control and Anti-Corruption in the AFP](#) (AFPHUB).

## 13. Attachments

- [AFP Risk Management Toolkit](#).