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 information management.

This instrument is part of the AFP's professional standards framework. The AFP Commissioner's Order on Professional Standards (CO2) outlines the conduct expected of AFP Appointees. 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. Guideline authority

This guideline was issued by the Chief Counsel 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.

3. Introduction

This guideline outlines the obligations, policies and procedures for a common approach by all AFP Appointees in managing risks that may impact the AFP achieving its objectives.

This guideline forms part of the AFP's overall risk management framework, based on the Standard AS/NZS ISO 31000:2018 Risk Management – Guidelines, and conforms with the Commonwealth Risk Management Policy and the *Public Governance, Performance and Accountability Act 2013* (Cth) (PGPA Act).

Further to the provisions contained within this guideline, AFP appointees must comply with legislative and regulatory risk management obligations (e.g. protective security in accordance with the Australian Government Protective Security Policy Framework, fraud control and work health and safety in accordance with the *Work Health and Safety Act 2011* (Cth)).

4. Key risk management concepts

Risk is defined as 'the effect of uncertainty on objectives', therefore effective risk management is not possible without a clear understanding of the intended objectives.

When planning to achieve objectives, there is likely to be some level of uncertainty, stemming from unknown or incomplete information, unpredictable circumstances, changing parameters, or factors which may not be easily understood nor controlled. These factors have the potential to cause our outcomes to deviate from our intended or expected objectives.

At its core, risk management is the structured, coordinated process to understand and address this uncertainty, which should facilitate better decision making and contribute to the successful delivery of AFP outcomes.

5. Leadership and commitment

Tier one (Tier 1) and two (Tier 2) Committees and the Chief Risk Officer (CRO) will ensure risk management is integrated into all AFP activities and will demonstrate leadership and commitment by:

- promoting effective risk engagement and management within the AFP
- assigning authority, responsibility and accountability at appropriate levels within the AFP
- promoting the systematic monitoring of risks
- aligning risk management with the AFP's objectives, strategies and culture
- ensuring the risk management framework remains appropriate to the corporate objectives of the AFP.

The Committees will be required to understand the risks facing the AFP in the pursuit of its objectives and ensure these are considered when setting the AFP's corporate objectives. The Committees will make certain there are systems to manage these risks and they are implemented and operating effectively. Information about these risks and their management will be properly communicated to the appropriate audiences.

6. Risk management framework

The risk management framework includes an integrated top-down and bottom-up approach to the assessment and management of risks for successful achievement of AFP outcomes that are set out in AFP's primary plans, strategies and operational procedures.

AFP Appointees must comply with the AFP's risk management framework to ensure a consistent risk managed approach is applied across the AFP. The Framework includes:

- this guideline
- the AFP Risk Management Policy
- the AFP Risk Matrix.

All AFP Appointees must also comply with risk management requirements in accordance with legislation, and other Commonwealth or AFP-specific governance relating to:

- work, health and safety
- operational planning
- fraud control and anti-corruption
- projects and programs
- finance
- procurement and contracting
- protective security, in accordance with the Australian Government Protective Security Policy Framework and the AFP Security Governance Framework
- business continuity management
- conflicts of interest.

7. Roles and responsibilities

The risk management roles and responsibilities for all AFP appointees, including supervisors, senior executives and those on key committees are detailed below:

Role	Responsibilities
AFP Appointees	All AFP 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 risks to achieve key business outcomes • document risk assessments including identified risks, controls and treatments in accordance with the AFP's risk management framework • promptly act to manage and communicate risks using the escalation process outlined in the Risk Management Matrix • contribute cooperatively to achievement of the risk management responsibilities of committees of which they are members.
Commissioner	The Commissioner is the accountable authority and is ultimately responsible for managing AFP risk. The Commissioner determines the AFP's risk appetite and tolerance.
Senior Executives	AFP Senior Executives have responsibility for establishing and maintaining an effective risk management culture in high-level forums and setting expectations in managing risk throughout all levels of the AFP.
Chief Risk Officer (CRO)	The CRO will champion risk awareness and bring a risk lens to strategic and enterprise level conversations at Executive Board meetings and other fora. The CRO will: • oversee the AFP's Framework and promote engagement • actively seek to enhance the maturity of all elements of the AFP's Framework, as prescribed by the PGPA Act and Commonwealth Risk Management Policy • champion integration of risk engagement and management into the AFP's risk culture, thinking and business processes.
Executive Board (tier one committee)	The Executive Board is responsible for the endorsement of the AFP Risk Profile.
Tier two committees (Finance, Capability, Operational and People)	Tier two committees will maintain oversight of the effectiveness of the AFP's risk management framework by: • ensuring existing and emerging key enterprise risks have been identified, analysed, rated, delegated and treated appropriately • regularly reviewing the AFP Risk Profile to ensure risks relating to the committee's responsibilities remain current and focused on the areas of greatest risk • engaging risk as a core element of decision making processes • considering shared risks and facilitating cross-committee engagement to manage risk holistically.
Audit Committee	The Audit Committee assures risk oversight in accordance with its charter, including ensuring the: • AFP has a sound risk management framework and associated processes for the effective identification and management of the AFP's business and financial risks, including those associated with individual projects, program implementation, and activities

	• processes for engaging and managing risk through the AFP Risk Profile are effective in facilitating high level understanding of the overall level of risk being carried by the AFP, and can be used to support strategic decision making.
Tier three committees	Tier three committees will engage risk where it relates to their charters and terms of reference.
National Managers	National Managers are responsible for: • contributing to the AFP risk management culture through modelling risk awareness and compliance • commissioning and approving functional risk assessment and treatment plans (RATPs) • clearly documenting all decisions and assuming responsibility for retained risks and the implementation of functional RATPs • effectively managing risk within their function, through establishment of a functional risk management committee or ensuring an alternative functional committee maintains a standing agenda item of risk management • ensuring the function contributes to the AFP risk management culture through adequate risk awareness and compliance • ensuring alignment of functional RATPs with functional business plans and the AFP Risk Profile • ensuring risk treatment and reporting obligations are met as set out in the in the AFP's Risk Matrix • appointing a suitable AFP Appointee(s) as their function's risk champion(s) • when identified as a Risk Lead for an enterprise level risk in the AFP Risk Profile, coordinating the overall treatment strategy (or strategies) and reporting obligations for that risk • considering enterprise risks through the National Managers' Forum and Senior Leadership Group.

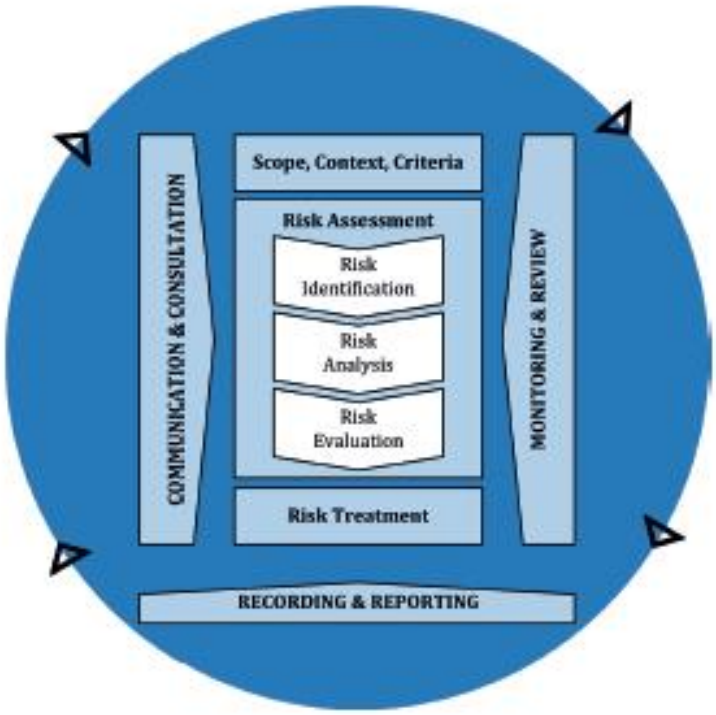
Managers and supervisors (including state managers, airport police commanders, station managers and IDG mission commanders)	Managers and supervisors will be responsible for: • contributing to the AFP risk management culture through modelling risk awareness and compliance • managing risks through regular risk assessment of key objectives or activities, including new initiatives • supporting and encouraging staff to manage risks by documenting risk identification, assessment and treatments to maintain audit trails • ensuring there is active participation in the risk management process by a wide cross-section of stakeholders • ensuring regular risk consideration at a risk management committee for office, station, mission or operation, or ensure that risk matters at this level are included in a standing agenda item of an appropriately placed committee • ensuring formal risk assessment processes are completed as required (e.g. for major investigation plans, standard tactical plans, fraud and corruption control, projects, procurements, work health and safety, etc.) • approving relevant RATPs (e.g. at the office, station, mission, operation or team level) and assuming responsibility for monitoring retained risks and implementing risk treatments • ensuring risks are escalated in accordance with the relevant risk rating and subsequent required actions as specified in the Risk Matrix • ensuring their staff, including independent contractors and consultants are aware of, and adhere to, this guideline.
Functional risk management committees or equivalent committees	Functional risk management committees or equivalent committees will be responsible for: • monitoring and reviewing alignment between RATPs and business plans • ensuring functional/state RATPs are aligned with the AFP Risk Profile and reflect key corporate, operational and project risks within the function/state • ensuring development and review of functional/state RATPs considers all risks which may relate to activities within the function/state including security, fraud and corruption, information management and security, WHS, compliance, etc • reporting at least every six months to the relevant National Manager and/or Operations Committee on risk management and as required to other committees and for updating the AFP Risk Profile • considering shared risks.
Control Owner	A control owner must effectively implement, monitor and maintain the control, and be able to provide assurance to oversight committees as to the effectiveness of the control as required.
Strategic Risk team	The Strategic Risk team is responsible for: • maintaining and improving the AFP risk management framework in accordance with legislation, ISO standards and better practice (it should remain tailored to AFP organisational needs) • building the risk management capability of AFP Appointees through guidance, targeted training, raising awareness and networking activities

	• maintaining the AFP Risk Profile including analysis of strategic and enterprise risks and monitoring risk treatments for appropriate consideration and clearance • monitoring the AFP's risk management environment • monitoring and reporting on the effectiveness of AFP risk management to the relevant AFP committees including the Audit Committee and Comcover • identifying and monitoring emerging risks.
Project managers	Project managers must: • be actively involved and accountable for adherence to 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 guideline • consider 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 is reviewed regularly 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 guideline • proactively monitor and review the effectiveness of controls and implementation of treatments.
Risk champions	Risk champions must: • be a functional or office point of contact for risk management information and advice • raise awareness of, and ensure participation and involvement in, risk management activity • integrate and promote risk management within relevant fora, such as operations, business and risk committees.

8. Risk management process

The steps in the risk management process identified in the flowchart below are articulated in the international standard ISO 31000:2018 and described in the risk management guidance material on the risk management hub page. Effective risk management utilises this process.

Risk management process



The AFP Risk Matrix must be utilised to undertake risk assessments for project, business and operational planning activities.

AFP Appointees should consider enterprise risks, including fraud and corruption, work health & safety, workforce planning and business continuity when undertaking any risk assessment.

8.1 Treatment of risks

Risks must be assessed as either acceptable or unacceptable using the AFP Risk Matrix. If a risk is unacceptable it must be treated.

Risk treatments must be balanced against expected benefits and cost-effectiveness. Taking this into consideration, there will be instances where the risk owner or higher authority may determine a level of risk can be retained but closely monitored as an appropriate risk treatment.

9. Documenting risk management

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

Risk management documentation, should clearly identify the risk assessment approval by the risk owner or higher authority including:

- controls and treatments to bring the risk(s) to an acceptable level
- acceptance of residual level of the risk(s)

- overall responsibility for determining and implementing the most appropriate risk treatments.

Given the sensitivity of some risk assessments, all documentation must be handled in accordance with the AFP National Guideline on information management, the Australian Government Protective Security Policy Framework and the AFP Security Governance Framework.

Dynamic risk assessment is the continuous cognitive process to identify and assess risks. It is not a formally documented process; however, it should be recorded in an official record of the event (case notes, official notebook or diary etc.) as soon as practicable. The record should articulate the thought process regarding the risk likelihood, consequence, treatments and controls along with the proposed course of action. Notes of dynamic risk assessment may subsequently form part of the justification for decisions or actions.

10. Shared risk

A shared risk is a risk where more than one entity is exposed to, or can significantly influence, the risk.

The AFP undertakes a number of law enforcement activities/operations in partnership with other Commonwealth and/or jurisdictional agencies, which may have different risk assessment requirements and documentation.

Where a single risk management approach is required, the lead agency should determine the risk assessment process and documentation for the joint activity/operation.

However, AFP Appointees must still comply with this guideline, as far as practicable, for managing risk within the AFP's own area of responsibility in joint activities/operations and include reference to shared risks.

11. Maintaining risk management capability

The AFP will maintain an appropriate level of risk management capability in order to implement the risk management framework and to manage identified risks.

The AFP does this through:

- equipping AFP Appointees to effectively manage risk via defined responsibilities and learning and development
- ongoing risk management training
- a fit-for-purpose risk management framework and associated processes
- clearly defined risk responsibilities and accountabilities
- integrated storage of risk information
- dissemination and sharing of risk information including status and compliance reports
- consistent information and messaging which is unambiguous and sufficiently enduring allowing risk to be measured and communicated to all stakeholders.

12. Review and continuous improvement

The risk management framework must be formally reviewed every two years in accordance with the AFP Commissioner's Order on Governance (CO1). Individual amendments are considered as needed.

The effectiveness of the AFP's risk management framework and performance is measured by:

- benchmarking against Commonwealth agencies and better practice through participation in the annual Comcover Risk Management Benchmarking Survey
- analysis of function, office and other RATPs to assess the quality and effectiveness of risk assessment and treatment and compliance with the framework
- internal audit program which informs, and is informed by RATPs, and the AFP Risk Profile
- other internal compliance reporting processes
- analysis of external reports and audits which have relevance to risk management in the AFP, for example ANAO performance reports, court or regulatory body findings
- feedback received from AFP Appointees, Senior Executives or AFP Committees.

13. Further advice

Queries about the content of this guideline should be referred to strategic-risk@afp.gov.au.

14. References

Legislation

- *Australian Federal Police Act 1979* (Cth)
- *Public Governance, Performance and Accountability Act 2013* (Cth)
- *Work Health and Safety Act 2011* (Cth)

AFP governance instruments

- AFP Commissioner's Order on Security (CO9)
- AFP National Guideline on business continuity management
- AFP National Guideline on procurement and contracting
- AFP National Guideline on work, health, safety and rehabilitation management arrangements
- AFP National Guideline on information management
- AFP National Guideline on information security
- AFP National Guideline on personnel security
- AFP National Guideline on physical security

Other sources

- AS/NZS ISO 31000:2018 – Risk management principles - guidelines
- ISO Guide 73:2009 Risk Management – Vocabulary
- Commonwealth Risk Management Policy, 2014
- Department of Finance Resource Management Guide 211 – Implementing the Commonwealth Risk Management Policy – Guidance, 2016

- Protective Security Policy Framework (Australian Government policy)
- Commonwealth Fraud Control Framework, 2017
- AS/NZS HB 167:2006 – Security risk management

15. Acronyms

AFP	Australian Federal Police
AS/NZS ISO	Australian Standards/New Zealand Standards International Organisation for Standardisation
RATP	Risk Assessment and Treatment Plan

16. Definitions

Accountable authority – as per the *Public Governance, Performance and Accountability Act 2013* (Cth), the AFP's accountable authority is the Commissioner.

AFP Appointee – means a Deputy Commissioner, an AFP employee, special member or special protective service officer and includes a person:

- engaged overseas under s. 69A of the *Australian Federal Police Act 1979* (Cth) (AFP Act) to perform duties as an AFP employee
- seconded to the AFP under s. 69D of the AFP Act
- engaged under s. 35 of the AFP Act as a consultant or contractor to perform services for the AFP and determined under s. 35(2) of the AFP Act to be an AFP appointee.

(See s. 4 of the AFP Act.)

AFP Risk Profile (ARP) – is the document detailing the AFP's strategic and enterprise level risks which represent the most significant risk exposure to the AFP. It articulates the overall level of risk carried by the AFP, and facilitates senior executive oversight of the effectiveness of AFP risk management, informing strategic discussion, prioritisation and decision-making.

Chief Risk Officer (CRO) – means the AFP Appointee undertaking the role of AFP Chief Risk Officer (CRO). The CRO is a risk advocate at the Executive Board and tier two committees, and promotes effective risk engagement and management within the AFP.

Control – means a measure (e.g. any process, policy, device, practice, or other action) that maintains or modifies a risk. A control is a measure that is currently in effect.

Control effectiveness – is the total effectiveness of all controls that act upon a particular risk.

Control Owner – means the AFP Appointee responsible for the effective implementation or ongoing management or monitoring of a particular control. The Control Owner may be required to provide assurance to oversight committees as to the effectiveness of the control.

Control rating – means a measure or estimate of the effectiveness of a particular control that acts upon a risk.

Consequence – means the outcome of an event affecting objectives. A consequence can be certain or uncertain and can have positive or negative effects on objectives. A consequence may escalate through cascading and cumulative effects.

Emerging risks – are the newly developing or changing risks which may have a major impact on the AFP and/or its outcomes.

Enterprise risks – means those risks which could prevent or severely disrupt achievement of the AFP's overall objectives and desired outcomes, or bring into question the AFP's ability to do so. Enterprise risks are typically enterprise-level risks or function/program risks of such significance to warrant attention and oversight by the senior executive. Enterprise risks may be internal or external risks.

Event – means an occurrence or change in a particular set of circumstances.

Key control – means a control that:

- is essential to preventing the risk event or mitigating the consequences of the event
- would significantly increase the risk if it were absent or failed, despite the presence of other controls, and
- controls more than one source of risk, consequence or risk event.

Likelihood – means the chance of something happening. May be defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Required actions – means the minimum actions to be taken based on the risk rating.

Risk – means the effect of uncertainty on objectives, where effect is a deviation from the expected. Risk is often characterised in terms of likelihood and consequences.

Risk appetite – means the amount and type of risk the AFP, as an organisation, is willing to pursue or retain. The AFP's risk appetite determines the level of risks that must be treated in accordance with the AFP Risk Matrix.

Risk assessment – means the overall process of risk identification, analysis and evaluation.

Risk assessment and treatment plan (RATP) – means the plan specifying the approach, management components and resources to be applied to the management of risks which could impact on achieving the objectives of an AFP business activity, a function or the whole organisation. There is a template for preparing a RATP on the risk management page of the Hub.

Risk champion – means the AFP Appointee, appointed by a National Manager, whose responsibility it is to promote awareness, understanding and compliance with the AFP's risk management framework within their own work area, or across the AFP.

Risk lead – means the AFP Appointee responsible for coordination of the overall management of a risk. Where a risk is beyond the authority of a single owner to manage, appointment of a Risk Lead rather than a risk owner may be appropriate. Enterprise level risks typically have Risk Leads.

Risk management – means the coordinated activities to direct and control an organisation with regard to risk.

Risk management framework – means the set of components providing the foundations and AFP arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk management process – means the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Matrix – is the guidance for selecting the likelihood and consequence of an identified risk and for determining the risk rating. The Risk Matrix also includes details of risk rating, required action and reporting after risks have been rated. This forms part of the risk management framework.

Risk owner – means the person or entity with the accountability and authority to manage a risk.

Risk source – means an element which, alone or in combination, has the intrinsic potential to give rise to risk. A risk source can be tangible or intangible.

Risk steward – is a term used in the Protective Security Policy Framework, and is equivalent to an AFP risk lead / risk owner as defined in this section.

Risk tolerance – means the AFP's readiness to bear a particular level of risk after risk treatment, in order to achieve a specific objective or manage a category of risk.

Senior executive – means an AFP manager or above.

Shared risk – means those risks extending beyond a single entity which require shared oversight and management. Accountability and responsibility for the management of shared risks must include any risks that extend across entities and may involve other sectors, community, industry or other jurisdictions. Shared risks defy allocation of a single risk owner, and may affect and/or be affected by multiple stakeholders.

Strategic risks – means those risks that the AFP faces which, if they eventuate, may lead to a change in strategic direction for the organisation. Strategic risks do not focus on operational activities, but rather reflect the external threats over which the AFP, on it's own, has limited ability to affect the likelihood of the risk occurring. There may be a requirement for new or amended high-level strategies to protect from the consequences, or to consider as a shared risk. Given the limited control over strategic risks' likelihood, it may be more appropriate to manage strategic risks using other metrics such as vulnerability, impact and velocity.

Treatment plan – means the treatment actions to reduce the level of risk(s), the priority of each treatment action and documented progress of implementation.

Treatment owner – means the AFP appointee responsible for the effective implementation and ongoing management or monitoring of a particular treatment.