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 the 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

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

3. Definitions

Appointee – means an AFP appointee as defined in s. 4 of the *Australian Federal Police Act 1979* (Cth).

Control – means a measure that is modifying a risk. Controls 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 potential control that has not yet been implemented.

Control rating – means a rating designed to describe the perceived effectiveness of a control in managing a risk.

Consequence – means the outcome of an event affecting objectives.

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

Impact – means the resulting effect(s) of a risk occurring.

Likelihood – means the chance of something happening.

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

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

Risk appetite – means the amount and type of risk that 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 as per instructions in Table 6 of the Risk Assessment Tool.

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

Risk Assessment and Treatment Plan (RATP) – means the identification, assessment, management and reporting of risks which could impact on achievement of the objectives of an AFP business activity or function. There is a template for preparing a RATP.

Risk Assessment Tool –comprises the tables and risk level matrix for assessment of the likelihood and consequence of individual risks and for determining of the required reporting and management actions after risks have been rated. The tool is included in the RATP template.

Risk champion – means the position or appointee that promotes awareness, understanding and compliance with the AFP Risk Management Framework within their own work area, or across the AFP.

Risk lead – means a National Manager or equivalent that is responsible for co-ordination of the overall treatment of a strategic risk in the AFP's Strategic Risk Profile.

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

Risk management framework – means 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 owner – means the person or entity with the accountability and authority to manage a risk. It is the person notified of the risk in accordance with the Risk Assessment Tool.

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.

Senior executives – A collective term for all appointed AFP Managers and above positions throughout the AFP.

Strategic risks – means those risks that could prevent or severely disrupt achieving the AFP's corporate objectives and desired outcomes, or bring into question the AFP's ability to do so. Strategic risks are typically enterprise level risks or Function/Program risks of such significance to warrant the Strategic Leaders' Group oversight.

Strategic Risk Profile – is the document that details the AFP's enterprise level risks. It facilitates senior executive oversight of the effectiveness of AFP risk management and informs strategic decision-making.

Treatment Plan – is part of a RATP. It lists the treatment actions to reduce the level of risk(s), rates the priority of each treatment action and records the progress of implementation.

4. Guideline Authority

This 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 supplementary risk management guidance on the AFP HUB, 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.

This forms the AFP's overall Risk management framework or plan based on the Standard AS/NZS ISO 31000:2009 *Risk Management: Principles and guidelines* and the *Comcover Better Practice Guide Risk Management June 2008.*

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

6. Risk Management Policy

The AFP's risk management policy is:

- all appointees are responsible for managing risks
- risk management is vitally important to ensure the efficient, effective delivery of law enforcement and also the safety and well-being of employees and the broader community
- in line with the AFPs Leadership Philosophy, appointees are expected to take calculated and innovative risks in the best interests of the AFP's mission and the delivery of valuable service to the Australian people
- appointees have specific responsibilities to ensure timely and successful implementation of risk management processes
- appointees must assess and manage risk in the planning, decision-making and conduct of all AFP business activities and operations
- the risk management process requires:
    - assessment based on the premise that individual Functions and business or operational teams and members are best placed to identify, analyse, evaluate and prioritise their risks and implement relevant risk treatments
    - clear accountability for ensuring the identification, evaluation and treatment of risks
    - escalating individual risks to managers and supervisors and where appropriate to relevant committees or individuals with specific risk management roles and responsibilities allows for informed and coordinated decision making, and
    - where appropriate recording of key risks, controls and respective risk treatments
- the AFP will provide the necessary tools, techniques and guidance for appointees to undertake the risk assessment process

7. Risk Management Principles

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

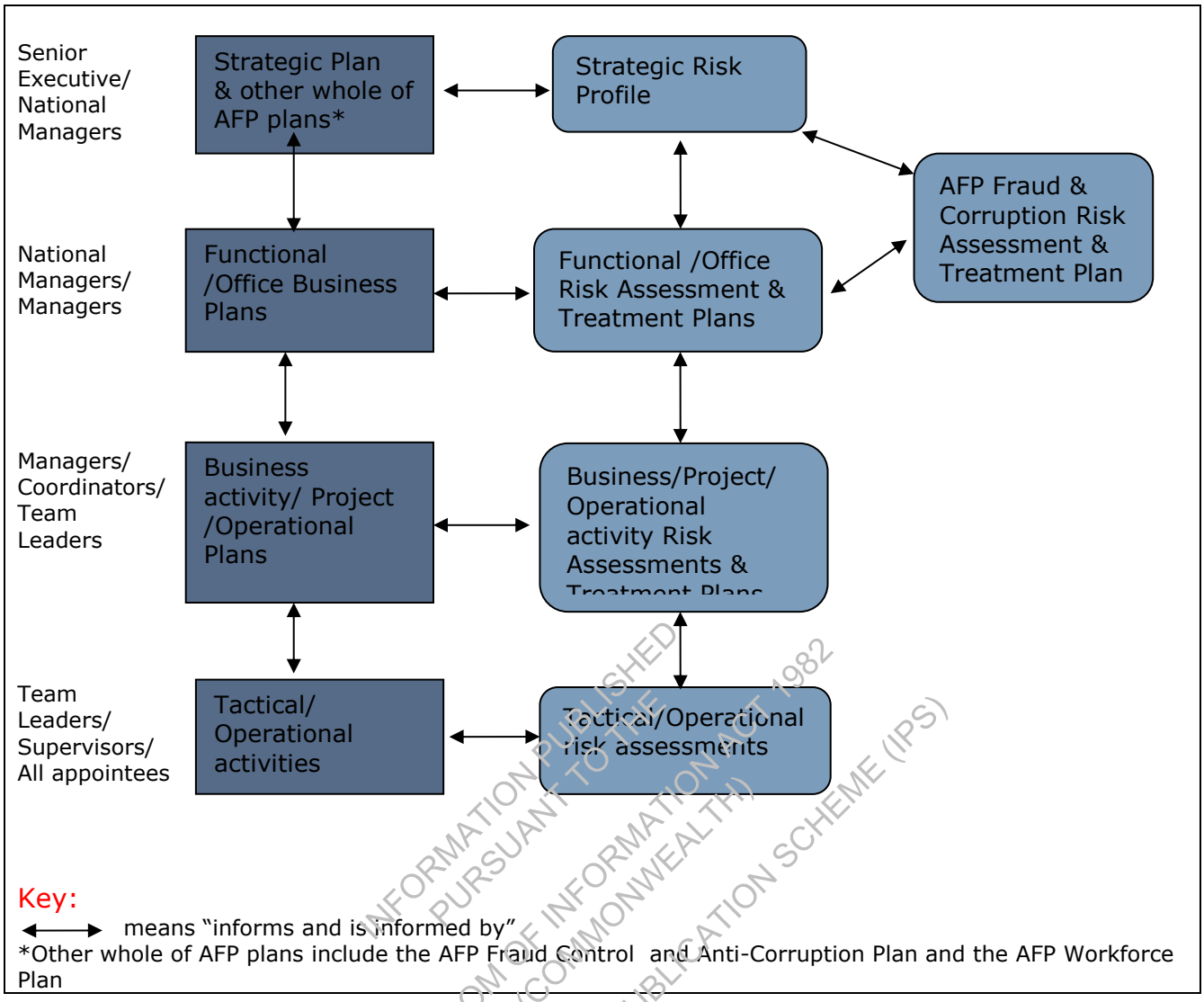
- effectively engage with risk to ensure innovative and effective delivery of AFP outcomes
- apply risk management practices across the AFP in a systematic, consistent and cost effective manner
- identify and manage risks that jeopardise achievement of AFP objectives
- integrate risk management practices 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 planning
- have risk management processes at all levels that will be able to withstand internal and external scrutiny.

8. Risk Management Framework

Appointees must comply with the AFP's Risk management framework to ensure a consistent risk management and reporting approach across the AFP. The framework includes:

- this guideline
- the Commissioner's Risk Management Policy Statement
- the AFP Risk Assessment and Treatment Plan (RAPT) template
- the AFP Risk Assessment Tool
- the AFP Risk Management User Guide, and
- any other risk management requirements in accordance with legislation, or other Commonwealth or AFP-specific guidelines relating to:
    - work and safety
    - operational planning
    - fraud control and anti-corruption
    - projects and programs
    - procurement and contracting
    - business continuity management, and
    - assessment of potential conflicts of interest

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 described in AFP strategic, business and operational plans as outlined below:



The Risk Management framework will be reviewed and updated regularly as part of a continuous improvement process.

9. Roles and Responsibilities

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

Role	**Responsibilities**
Commissioner	The Commissioner is ultimately accountable and responsible for managing AFP risk and determines the AFP's risk appetite and accepts the agency's Strategic Risk Profile.
Senior Executives	All Senior Executives must establish and maintain an effective risk management culture in high level fora and set expectations in managing risk throughout all levels of the AFP.

Strategic Leaders' Group (SLG)	The SLG will maintain oversight of the effectiveness of the AFP's Risk Management framework by: • ensuring existing and emerging key strategic 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.
National Managers	All National Managers must: • contribute to the AFP risk management culture through modelling risk awareness and compliance • approve functional Risk Assessment and Treatment Plans (RATPs) • clearly document all decisions and assume responsibility for retained risks and the implementation of Functional risk treatment plans • establish a Functional Risk Management 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 RATPs with Functional business plans and the AFP's Strategic Risk Profile • ensure risk reporting obligations are met, including escalation to Deputy Commissioners, as set out in the in the AFP's Risk Assessment Tool • identify suitable Functional officer(s) as their function risk champion(s) • when identified as a risk lead for a strategic risk in the Strategic Risk Profile, coordinate the overall treatment strategy/s and reporting obligations for that risk.

Managers and Supervisors (including Office Managers, Airport Police Commanders, Station Managers and IDG Mission Commanders)	All Managers and Supervisors must: • contribute to the AFP risk management culture through modelling risk awareness and compliance • manage risks through regular 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 and corruption control, projects, procurements, work health and safety, etc.) • approve relevant RATPs (e.g. at the office, station, mission, operation or team level) and assume responsibility for monitoring retained risks and implementing risk treatments • ensure risks are escalated in accordance with the relevant risk rating and subsequent required actions as specified in the Risk Assessment Tool • ensure their staff, including independent contractors and consultants are aware of, and adhere to, this guideline.
Risk Management Committees or equivalent committees	Risk Management Committees or equivalent committees must: • monitor and review alignment between RATPs and Functional business plans or Office action plans • ensure Functional/Office RATPs are aligned with the Strategic Risk Profile and reflect key corporate, operational and project risks within the Function/Office • report at least six monthly to the relevant National Manager and/or Operations Committee on risk management and as required for Performance and Budget Monitoring Committee reporting and updating of the Strategic Risk Profile.
Planning & Risk team	The Planning & Risk team must: • maintain and improve the AFP Risk Management Framework in line with best practice and tailored to AFP organisational needs • build the risk management capability of appointees through guidance, targeted training, raising awareness and networking activities. • maintain the AFP Strategic Risk Profile including undertaking analysis of strategic risks and monitoring risk treatments for SLG consideration. • monitor the AFP's risk management environment. • monitor and report on the effectiveness of AFP risk management to the SLG, Audit Committee and Comcover.

Project Managers	Project managers must: • also adhere to additional project and program risk management governance requirements defined by the Portfolio Management Office. • 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 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 (including Business Support Teams or Officers who co-ordinate preparation of Function and Office RATPs)	Risk Champions must: • be a functional or office point of contact for risk management information and advice • raise awareness of, and ensure participation and evolvement in, risk management activity • integrate and promote risk management within relevant fora, such as operations, business and risk committees
Appointees	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 risks to the achievement of key business outcomes • promptly act to manage and communicate risks as per the principles in this guideline • where appropriate document risk assessments including identified risks, controls and treatments

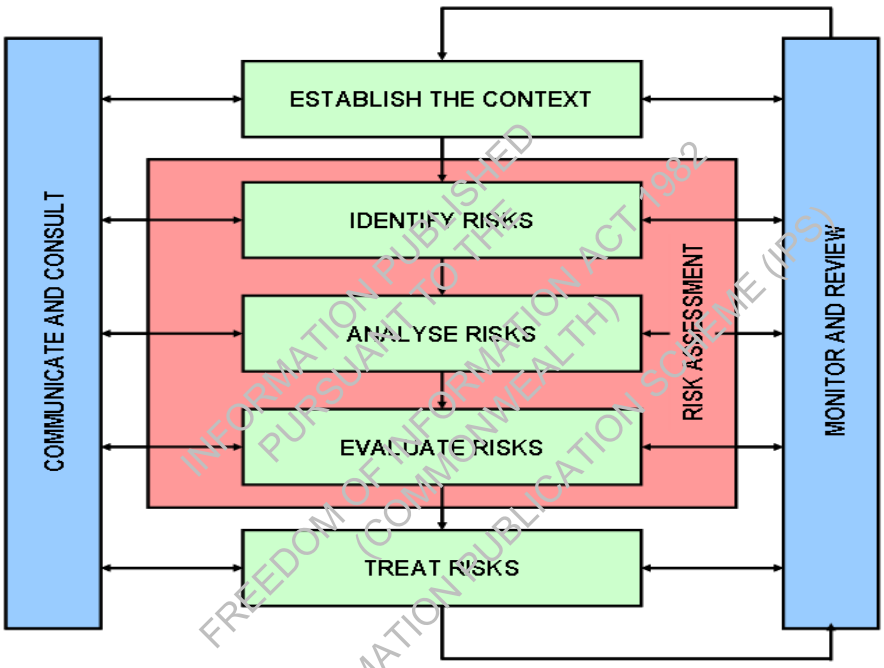
10. Risk Management Process

Appointees must:

- undertake the risk management process steps set out in the flowchart below in accordance with the international standard ISO 31000:2009.
- consider fraud and corruption risks when undertaking any risk assessment
- use the AFP Risk Assessment and Treatment Plan (RATP) template and the AFP Risk Assessment Tool to undertake and document risk assessments for business and operational planning activities

The AFP Risk Management User Guide provides step by step guidance for appointees to prepare RATPs in accordance with these requirements.

Risk management process



10.1 AFP Risk Appetite

The AFP's risk appetite is articulated through the AFP's Risk Assessment Tool and includes the required actions for the communication, escalation and treatment of risk based on the assessed level of risk.

The AFP has endorsed a 'Medium' risk rating as within the confines of business as usual for the AFP. The AFP's 'Medium' risk appetite means any risks rated 'Significant', 'High' or 'Critical' must be treated as per instructions in Table 6 of the Risk Assessment Tool.

10.2 Treatment of Risks

Risks must be assessed as either acceptable or unacceptable using the AFP Risk Assessment Tool. 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 that a level of risk can be retained but closely monitored as an appropriate risk treatment.

11. Documenting Risk Management

Where appropriate appointees must document the AFP risk management processes sufficiently, primarily through completion, review and updating of a Risk Assessment and Treatment Plan (RATP), to demonstrate compliance with the AFP process and principles.

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:

- acceptance of residual levels of the risks
- 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 AFP records management and security requirements.

12. Joint or Multi-agency Law Enforcement activities/operations

The AFP undertakes a number of law enforcement activities/operations in partnership with other Commonwealth and/or jurisdictional agencies, where the agencies 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, 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.

13. Measuring effectiveness of the AFP's Risk Management Framework

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

- benchmarking against best practice, including through participation in the annual Comcover Risk Management Benchmarking Survey
- analysis of function, office and other Risk Assessment and Treatment Plans to assess the quality and effectiveness of risk assessment and treatment and compliance with the Framework
- other internal compliance reporting processes
- feedback received from appointees, Senior Executive and AFP committees, particularly the SLG and Audit Committee.

14. Further Advice

Queries about the content of this guideline should be referred to the Planning & Risk by contacting the Planning-and-Risk@afp.gov.au.

15. References

Legislation

- *Australian Federal Police Act 1979* (Cth)
- *Work Health and Safety Act 2011* (Cth)

AFP governance instruments

- AFP National Guideline on business continuity management
- AFP National Guideline on conflict of interest
- AFP National Guideline on health and safety management arrangements
- AFP National Guide on managing occupation health and safety risk
- AFP National Guideline on operational planning
- AFP National Guide on procurement and contracting
- AFP Practical Guide on applying security classifications and protective markings to information

Other sources

- AS/NZS ISO 31000:2009 – Risk Management Principles and Guidelines
- ISO Guide 73:2009 Risk Management – Vocabulary
- Comcover Better Practice Guide – Risk Management June 2008
- Commonwealth Fraud Control Guidelines 2011