



Australian Government

Australian Financial Security Authority

afsa.gov.au

Position Description



Position title / number	Assistant Director, Cyber Governance, Risk and Compliance
Classification	Executive Level 1
Location	Adelaide, Brisbane, Canberra, Melbourne, Sydney
Division / section	Technology Services / Cyber Security
Reports to	Head of Cyber Security
Position status	Ongoing
Direct reports	Up to 3
FTE / hours	37:30 Full time
Security clearance	Negative Vetting 1

AFSA acknowledge Aboriginal and Torres Strait Islander peoples as custodians of Australia and we pay our respects to Elders, past and present. We also acknowledge the ongoing connection to land, sea and communities throughout Australia, and the contributions to the lives of all Australians. We are committed to advancing reconciliation and recognise the importance of empowering Aboriginal and Torres Strait Islander people to achieve greater equity and equality as a society.

Organisational context

The Australian Financial Security Authority (AFSA) is responsible for managing the application of bankruptcy and personal property securities laws through the delivery of high-quality personal insolvency and trustee, regulation and enforcement, and personal property securities services.

The **Enabling Services Group** is responsible for aligning AFSA's enabling services to better support AFSA's core regulatory functions and achieve the strategic vision of becoming a visible, modern, and contemporary regulator.

The Group plays a key role in shaping AFSA's strategic direction, managing government relationships, providing efficient corporate services, and leveraging and harmonising AFSA's technology to promote organisational delivery and performance.

The **Technology Services Division's** aim is to ensure that cutting-edge technologies are employed in alignment with industry best practices, resulting in a secure, efficient, and innovative IT environment. Our

Position Description – Assistant Director, Cyber Governance, Risk and Compliance

efforts are geared towards seamlessly supporting the organisation's core functions, optimising operational processes, and enabling the achievement of strategic objectives.

Purpose of the position

The **Assistant Director, Cyber Governance, Risk and Compliance** is responsible for the development and implementation of information security policies, standards and procedures, and the development of cyber security risk assessments as well as the provision of cyber security advice to Technology Services Leadership Team. This position leads a small team of APS staff and contractors to ensure risks within the AFSA ecosystems are managed and ICT systems are compliant with relevant Australian Government standards and guidelines.

The **Assistant Director, Cyber Governance, Risk and Compliance** works closely with the Head of Cyber Security, Agency Security Adviser (ASA) and System Owners to ensure comprehensive security documentation is established and maintained, and that comprehensive work plans and auditing and reporting frameworks are also in place. They also provide specialist advice to system and network engineers and support the development of new systems by providing timely, risk-based advice, playing an active role in change and incident management.

Accountabilities

- Ensure a strategic and integrated approach to cyber-security risk management, with a focus on information management, staff development and risk-based decision making.
- Determine security requirements by:
 - evaluating business strategies and requirements;
 - researching global information security standards and emerging technologies;
 - conducting system security reviews, vulnerability analyses and risk assessments;
 - developing and complying with architecture/platform standards;
 - identifying integration issues; and
 - preparing cost estimates for relevant cyber security work.
- Document and analyse risks using the Information Security Manual (ISM) control framework and provide certification documentation (SOA, SSP, SRMP) for accreditation by the Head of Cyber Security or Chief Information Officer (CIO).
- Ensure the development and implementation of plans, policies, work instructions and standard operating procedures to ensure an enhanced level of security compliance within AFSA.
- Maintain security by:
 - monitoring and ensuring compliance to standards, policies, and procedures;
 - supporting incident response and analyses; and
 - providing advice and ongoing education to staff on managing ICT risks and threats.
- Lead and build a team by:
 - establishing clear work expectations, systems and processes
 - encouraging and supporting of ongoing learning and development opportunities
 - providing regular feedback
 - identifying opportunities to enhance team performance in an environment of collaboration, continuous improvement and change.
- Enhance security team competence and undertakings by:
 - mentoring team members and answering technical and procedural questions for less experienced team members; and
 - developing, promoting and coaching staff on improved processes.
- Prepare system security reports by collecting, analysing, and summarizing data and trends.
- Engage and manage contractors and consultants, as required, to contribute to delivery of secure services and projects.
- Lead initiatives as a senior member of the Cyber Security Team and Technology Services Division within AFSA, including providing input to ICT strategies and operational plans and senior management discussions as required.

All duties will be performed in accordance with:

- the APS Values, Code of Conduct and Employment Principles
- WHS obligations, taking responsibility for own health and safety and that of others
- AFSA's risk management framework and relevant legislation, including guiding others to identify and mitigate foreseeable risks.

Core skills and capabilities

Operates efficiently to achieve business outcome

- take a flexible approach to planning in order to meet changing circumstances and consider the impact on others
- Consider the broader, long term, implications of actions including the impact on governance, finance and technology as well as social and environmental considerations

Drives Innovation and continuous improvement

- Constructively challenge and question status quo, with a view to continually improving the way we work
- Explore and work with new ideas that will benefit our stakeholders.

Uses information to make evidence-based decisions

- Identify and integrate different types of relevant evidence towards finding solutions to the problem
- Provide unbiased, comprehensive and accurate advice to others
- Use past experience and organizational/environmental awareness to analyse what information is important and how it should be used in the decision-making process.

Sustains a user-centred approach to design and deliver better services

- Gain an authentic understanding of the stakeholder's experience and needs through collaboration and curiosity
- Embrace ambiguity and work through the solution that works for the stakeholder.

Communicates simply, tailoring messages to audience

- Communicate clearly in plain English, without using jargon
- Demonstrate an ability to convey a message succinctly and with empathy, regardless of medium (written, verbal and digital)
- Understands target audience, and tailors written and verbal messages in a way that appeals to them.

Promotes performance excellence

- Supports development of goals for self and team which align to Future AFSA, focusing on outcomes not outputs
- Role models drive, accountability and achievement orientation, and holds others to the same high standards

Qualifications, accreditations and experience

Mandatory

- VET or Tertiary qualifications in information management, computer science, information systems or equivalent experience
- Certified Information Security Manager (CISM), Certified information Systems Security Professional (CISSP) or equivalent certification
- Demonstrated experience in risk management, policy and strategy development
- Demonstrated capacity to provide timely, compelling and concise advice to inform executive members and senior management to support decision making.

Preferred

- Information Security Registered Assessors Program (IRAP)
- SANS specific security training
- Demonstrated experience leading a team to achieve high performance and meet organisational and business goals.

Delegations exercised:

- AFSA delegations
- *Public Service Act 1999*
- *Public Governance Performance and Accountability (PGPA) Act 2013*

HR use only:

Date last varied	By Who
Date Updated in Aurion by People Assist	