Position Description

Job title:	Security Assurance Manager
Department:	Security
Work type:	Full time
Reports To:	Chief Information Security Officer
Position Reports:	None
Position Contact:	Chief Information Security Officer

About the organisation

.au Domain Administration (auDA) is the administrator of the .au domain name system (DNS), which is Australian critical infrastructure relied on by internet users in Australia and around the world. We are a not-for-profit endorsed by the Federal Government.

Our purpose is to administer a trusted .au domain for the benefit of all Australians and champion an open, free, secure and global internet.

We support the needs of Australian internet users by:

- Delivering a stable, secure and reliable .au DNS
- Implementing .au policy rules that are transparent, responsive and efficient
- Investing in the Australian internet ecosystem to improve the utility of the .au domain.

We also participate in global internet governance processes. Through our work, we strive to uphold the multi-stakeholder model of internet governance and the social and economic benefits that flow from it.

Further information about auDA is available at www.auda.org.au.

Our values

Leadership

We are committed to communicating openly, and adding value to our multistakeholder community, locally, regionally and globally

Collaboration

We work together as one auDA in the service of Australian, regional and global internet users

Accountability

We honour our commitments, are responsible for our decisions, actions and performance, and deliver excellence

Curiosity

We seek to grow our knowledge, including of emerging practices, be adaptive and improve our understanding of our stakeholders and their viewpoints

Role purpose

The Security Assurance Manager plays a critical role in strengthening auDA's cybersecurity posture and ensuring the ongoing resilience of our information assets, services and the .au domain supply chain. This position is responsible for developing, implementing, and overseeing robust security assurance frameworks, policies, and procedures. The manager will lead efforts in supply chain security risk assessments, and the continuous improvement of security controls, ensuring alignment with industry best practices, regulatory requirements, and auDA's strategic objectives. This role is pivotal to auDA's objective to provide a cyber resilient .au that builds trust, enables innovation and builds the capabilities needed into the future.

This role will contribute significantly to auDA by safeguarding critical infrastructure, sensitive data, and maintaining the trust of its stakeholders. By proactively identifying and mitigating security risks, the Security Assurance Manager will help prevent security incidents across auDA's supply chain, support ongoing compliance to industry security standards, and protect auDA's reputation. The role will report directly to the Chief Information Security Officer and will be instrumental in translating security into actionable strategies, supporting auDA's mission to operate a secure and stable domain name system for all Australians.

This role will suit a candidate with a strong background in information security, risk management, and compliance, possessing excellent communication and stakeholder management skills. The ideal candidate will be a proactive, detail-oriented individual with the ability to communicate complex technical concepts effectively to both technical and non-technical audiences. They should demonstrate a proven track record in leading security assurance initiatives, managing stakeholder relationships, and driving continuous improvement in a dynamic environment.

Key accountabilities

The primary responsibilities of the Security Assurance Manager include:

Security Assurance

- Developing and maintaining auDA's security assurance framework, policies, standards and processes in line with relevant regulations and industry best practices (e.g. ISO 27001, NIST, Essential 8)
- Managing and overseeing a Security Assurance Program, engaging with the key stakeholders across the .au Domain Name System supply chain and conducting ongoing security assurance activities.
- Performing security outreach and education activities to support improved security assurance outcomes both internally within auDA and across the .au domain supply chain.

Risk Management

- Conducting regular security risk assessments, identifying vulnerabilities, and recommending appropriate mitigation strategies to reduce auDA's risk exposure.
- Assessing, monitoring and managing auDA's supply chain security risks, including vendor third-party risks, and security risks across the whole .au domain supply chain.
- Reviewing contracts to ensure any security risks are highlighted, raised and appropriately manged.

Compliance

- Supporting internal and external security audit activity to ensure compliance with security policies, regulatory requirements, international standards, and contractual obligations.
- Driving the continuous improvement of security controls and processes through performance monitoring, incident reviews, and emerging threat analysis.
- Monitoring changes to the regulatory, standards and contractual obligations compliance landscape to ensure new or emerging obligations are captured and addressed by auDA.

Other responsibilities

- Participate in and support good procurement practices, enabling security contribution and input in procurement processes.
- Support security governance activities and forums, including developing executive level briefings and reporting.
- Support execution and delivery on auDA's Cyber Security Strategy and associated Cyber Security Program as it relates to Governance, Risk & Compliance.
- Other activities as directed by the Chief Information Security Officer and Chief Operating Officer to support the delivery of auDA's Strategy and the Security strategic goals.

Key selection criteria

Security Assurance

- Demonstrated expertise in developing, implementing, and managing security assurance frameworks, policies, and standards.
- Demonstrated experience conducting security assurance activities in line with industry standards including: ISO27001, NIST CSF, NIST 800.53, ACSC's Essential 8, ASD Information Security Manual.
- Proven experience in conducting comprehensive security risk assessments, vulnerability identification, and recommending effective mitigation strategies.
- Strong background in supporting internal and external security audits, with a focus on compliance and continuous improvement.
- Ability to drive and implement improvements in security controls and processes, utilising performance monitoring and threat analysis.

Connection and collaboration

- Strong analytical and problem-solving abilities, with a proactive and detail-oriented approach to information security.
- A proven track record of fostering a security-conscious culture and building strong relationships within an organisation.
- Experience working with a diverse range of stakeholders, including industry, government and non-government organisations.
- Ability to work independently as well as part of a multidisciplinary team.

Communications

- Excellent communication and interpersonal skills, with the ability to provide expert security advice and guidance to diverse stakeholders.
- Ability to articulate complex concepts effectively with to a range of stakeholder audiences, verbally and in writing.

Project management

- Strong organisational, planning and coordination skills.
- Ability to plan and prioritise work and manage multiple tasks concurrently.

Other

- Proactive and self-motivated attitude.
- Analytical and problem-solving skills.
- Ability to model auDA's workplace values.
- Occasional work outside business hours will be required. Occasional domestic travel and potentially international travel may be required.

Qualifications and experience

- A minimum of 5 years' experience in a dedicated Security assurance role.
- At least 10 years of experience in technology or security related roles.
- Background in a regulated industry, such as financial services or critical infrastructure, is advantageous.
- A degree in a technology or security related field is advantageous.
- Experience working in organisations of varying sizes will be highly regarded.

Important information

Background checks

A National Police Check, Right to Work and bankruptcy will be conducted as part of the recruitment process. An *AusCheck Critical Infrastructure Background Check* will need to be conducted and there may be a need to obtain Government security clearances as part of this role. Where applicable, international background checks may also be required.

Privacy collection information

.au Domain Administration Limited ACN 079 009 340 collects your personal information for the purpose of assessing and responding to your application. All personal information is collected in accordance with the *Privacy Act 1998* (Cth) and our Privacy Policy.

We, or our third-party tools or platforms, may disclose some of your personal and sensitive information to our payroll, invoicing and data storage and records management services located overseas, including in the USA, United Kingdom, New Zealand, Singapore, Malaysia, Vietnam, and the Philippines. You agree to this disclosure and acknowledge that such recipients may use de-identified employee data for that recipient's commercial purposes. We will ensure that all arrangements with third party tools or platforms or third-party service providers will contain appropriate controls (which may be contractual or operational) to protect your personal information.

If you have any questions or would like to access your personal information held by auDA, please contact us at privacy@auda.org.au.

Occupational Health and Safety

In the context of OHS policies, procedures, training and instruction, as detailed in Section 25 of the *Occupational Health and Safety Act 2004* (Vic), employees are responsible for ensuring they:

- Follow reasonable instruction
- Cooperate with their employer
- At all times, take reasonable care for the safety of themselves and others in the workplace.

Flexible working arrangements

We believe in supporting our employees in balancing their work and life commitments. All roles at auDA can be worked flexibly by mutual agreement. This underpins a diverse, adaptive and high-performing workforce. The nature and scope of flexible options available will depend on the nature of the position. Applicants are encouraged to discuss flexible arrangements with the hiring manager during the recruitment process.

Please note that the role may require you to work the hours which are reasonably necessary to fulfil the requirements of the position, or as required by auDA, including monitoring, reading and responding to business-related communications from auDA or customers outside of usual office hours, where reasonable. The remuneration for this role includes compensation for all hours you would be required to work, including reasonable availability out of hours

Last Updated

13/08/2025