Position Description

Job title:	Information Security Officer
Department:	IT
Work type:	Fulltime

About the organisation

au Domain Administration Limited (auDA) is Australia's Country Code Top Level Domain (ccTLD) administrator and self-regulatory policy body, which oversees the operation and management framework of the .au domain of the Internet.

auDA is a not-for-profit public company limited by guarantee and endorsed by the Australian Government and the global Internet Corporation for Assigned Names and Numbers (ICANN). Its job is to provide a safe, secure and operational namespace for more than 20 million Australian Internet users.

Role Purpose

The Information Security Officer is responsible for the security of auDA's systems and processes, including throughout the supply chain, that maintain and promote the operational stability and utility of the .au ccTLD. The role aligns with auDA's objective of maintaining world's best practice in information security as it relates to the .au domain name system. As security policies are developed and refined, the approach for achieving compliance with these policies by auDA staff and registrars will consist of three steps: communicate and educate, guide and facilitate, and enforcement (using automation where possible).

The role should also act in accordance with the following terms of endorsement from the Australian Government:

- ensure stable, secure and reliable operation of the .au domain space

The role will actively contribute to the ongoing development of an organisational culture that embodies auDA's values and promotes a positive and safe environment for staff.

About the role

Key accountabilities:

Enterprise Risk Register

- Identify IT, operational and organisational risks. Present for review by the executive-level committees.
- Assess and prioritise risks and assist developing strategies for managing or mitigating the risk.
- Work with all functional areas to ensure consistent use of the Enterprise Risk Management Framework.

Audit and Compliance

- Manage auDA's Information Security Management System (ISMS) maintaining ISO 27001 compliance, and compliance with the Australian Signal Directorate's Essential 8.
- Manage and maintain auDA's Governance, Risk and Compliance (GRC) platform (eramba).
- Ensuring system compliance with system hardening policies and standards.

Communicate and Educate

- Drive cultural change to ensure IT security is an important consideration of every team member within auDA.
- Implementing a continuous improvement program for cyber security awareness training for staff and registrars.
- Lead risk workshops and discussions with registrars and stakeholders

Guide and Facilitate

- Review registrar security assessments provided by third parties.
- Provide guidance to registrars on practical steps to address security weaknesses.
- Develop and maintain relationships with registrar security teams and conduct regular meetings to track execution of initiatives to meet minimum security standards.

Enforce the rules

- Arrange regular ISO 27001 audits and baseline security assessments for auDA registrars.
- Monitor usage of IT systems and ensure that are being used in compliance with auDA security policies.

Enterprise Security

- Assisting in reviewing and updating auDA's Enterprise Security Policy.
- Examine impacts of new technologies on auDA's overall information security.
- Establish annual and long-range security and compliance goals and a roadmap for continual program improvements.

Business Continuity

- Develop and review disaster recovery and business continuity plans that meet organisational goals.
- Run regular business continuity testing exercises with both internal and external stakeholders.

Physical and Logical Security

- Management and implementation of end-point security.
- Cyber incident response planning and overseeing/performing investigation of reported security breaches.

- Manage Security Information and Event Management systems (SIEM) including alert management
- Service procurement and security review of third-party applications.

Skills and Experience

Key selection criteria

- Minimum 5 years' experience in Information Security with a good understanding of security operations.
- Previous employment in the domain name industry.
- Significant knowledge of Risk Management Frameworks and Vulnerability Management.
- Proven experience implementing and managing a Governance, Risk and Compliance program.
- Extensive knowledge of ISO 27001 standard and requirements.
- Proven experience in developing Information Security strategies.
- Experience with Data Loss Protection (DLP).
- Proven experience and strong understanding of SIEM (Security Incident and Event Management).
- Experience running cyber-security exercises.
- Demonstrated ability to work on security projects as a team lead.
- Proven ability to communicate technical issues with non-technical and non-security focused people.
- Experience in leadership / mentoring team members.
- Ability to perform analysis of security risks and develop mitigation strategies.
- Excellent written and verbal communication skills - proven effectiveness in documenting IT environments.
- Strong organisational skills allied to good time management and high attention to detail.
- Ability to manage and motivate self, work with minimal direction and to exercise initiative and discretionary judgement.
- Self-starter and able to operate autonomously, but also able to be a successful team player.
- High attention to detail.

Qualifications and experience

- Tertiary qualification in Information Systems, Technology, Engineering or related discipline.
- Domain Name industry experience with a registry operator, registrar or large reseller.
- Relevant certifications such as CISSP, CISM, CRISC, SABSA, SANS.
- Demonstrated experience in implementing, maintaining and improving information security risk. management systems in alignment with ISO 27001/27002.
- Knowledge of Australia government Information Security Manual (ISM), Essential 8 and Protective Security Policy Framework (PSPF).
- Linux/Unix operating system experience.
- TCP/IP Networking fundamentals.
- Australian citizen.

Important Information

Must be able to obtain Australian Government Security clearance of Negative Vetting 1 (NV1) or higher.

National Police Check, Right to Work and National Personal Insolvency Information Check will be conducted as part of the selection process.

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

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

Supporting our employees balance their work and life commitments

All roles at auDA can be worked flexibly, 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.

Last Updated

9 June 2021