Department of
Education

GOVERNMENT OF
WESTERN AUSTRALIA

Job Description Form

Cyber Security Specialist - GRC

Position number	00045039
Agreement	Public Sector CSA Agreement 2022 or as replaced
Classification	Level 7
Reports to	Cyber Security Manager
Direct reports	Nil

Context

Education Business Services (EBS) is the key provider of professional business services and support for Western Australian public schools, statutory boards and divisions of the Department. These highly valued services are delivered through the areas of finance, information and communication technologies (ICT), and infrastructure. We continually strive to enhance the capability and responsiveness of our staff, systems and processes across the organisation to deliver high quality education.

We are committed to contemporary work practices and adhere to the following service delivery principles:
Responsive: We respond to and reflect the needs of our customers.
Flexible: We are flexible and understand that our customers are not all the same.
Transparent: We are clear and open about our services, processes and decision making.
Accountable: We hold ourselves to high standards and deliver on our commitments.
Collaborative: We work in partnership with our customers.

Delivery of Information and Communication Technology (ICT) services provides support for the Department's educational outcomes by developing initiatives and technical support strategies to ensure all 800 Western Australian public schools can be individual, distinctive and responsive to their local communities while still benefiting from being part of a system.

The ICT Operations and Customer Service Directorate is part of the ICT Division and is the primary entry point to ICT for any responses to operational issues, requests or problems customers of ICT may have. As the highest frequency contact point for customers in many respects it is the 'face' of ICT.

The ICT Cyber Security, Security Operations Centre (SOC) supports the Department with ongoing improvements to cyber security governance, risk, and compliance, while providing expert knowledge, leadership and advice in cyber security matters to protect the assets of the Western Australian Department of Education.
Visit education.wa.edu.au to find out more information about the Department of Education.

Key responsibilities

Specialist Services

- Be the primary point of contact for cyber security policies, procedures, standards, guidelines, strategies, frameworks, plans and roadmaps applicable to the secure operation of systems within the Department.
- Lead and manage cyber security compliance risk and audit activities and ensure they comply with legislation, policy, process, regulations and standards.
- Establish, implement and continually improve the Department's cyber security governance and management framework, its associated policies and assurance compliance processes to ensure their currency and effectiveness.
- Coordinate the development, implementation and maintenance of cyber security policies and practices within the spectrum of governance, risk, compliance and audit for the Department.
- Work with senior management to determine acceptable levels of risk for the organisation and take responsibility for establishing and maintaining a corporate-wide information security management program to ensure that information assets are adequately protected.
- Review and report on security issues together with measures that reduce the likelihood of data breaches.
- Seek and obtain feedback from technology stakeholders and industry as relating to security best practices and fit-for-purposes solutions.
- Develop, collate and present reporting metrics, dashboards and evidence artifacts to show compliance progress with risks and audits.
- Participate in emergency or critical event response management duties, as required.

Branch Support

- Contribute to the development of cyber security strategic plans and translates these into Branch level business plans.
- Contribute to the development of ICT policies, standards and procedures, and monitors compliance where relevant.
- Identify corporate level (operational and strategic) information and technology risks and escalate issues and establish plans to manage actions to an agreed remediation level.
- Monitor performance against Key Performance Indicator’s (KPIs), action plans and other targets, taking necessary action to continuously improve performance.

Client and Stakeholder Support and Liaison

- Partner with business stakeholders across the department to raise awareness of cyber and Information Security risk management concerns.
- Develop relationships with customers to facilitate a customer focused, collaborative and partnership approach to cyber security and service delivery ensuring cyber security and resilience efforts are informed by understanding the Department’s core business functions.
- Work directly with department business units to facilitate risk assessment and risk management processes.
- Represent the Department on committees and working groups as appropriate, with a view to strengthen the Department's security and business continuity ethos and ensure it is appropriately aligned with broader government mandates and initiatives.
- Prepare reports, briefing notes and correspondence for internal and external stakeholders, where required.
- Work within corporate policies and procedures, act with integrity and demonstrate ethical behaviours aligned with the Department Code of Conduct.

Selection criteria

1. Demonstrated extensive understanding and knowledge of Australian Government policies and frameworks, and in particular, the ACSC’s Essential Eight, NIST CSF, and the ADS’s ISM.
2. Demonstrated experience in a cyber security GRC role, including policy development, risk management, and compliance assessments.
3. Demonstrated proven ability to present clear, concise, and articulate information and advice in relation to compliance, risk and audits which encourages and assists key stakeholders in achieving practical and business-focused outcomes.
4. Demonstrated proven ability to design, develop, implement, monitor, and evaluate frameworks, and tools and processes to ensure effective compliance with risks, audits and relevant policies and procedures.
5. Demonstrated skills and experience in achieving outcomes and delivering quality products and service. Remains flexible and responsive to changes in requirements and takes personal responsibility for meeting objectives and progressing work.
6. Demonstrated strong work ethic and the ability to manage own workload and tasks to deliver outcomes as part of a small, dynamic team.

Eligibility and training requirements

Employees will be required to:

- hold a tertiary qualification in information technology/cyber security, relevant industry qualifications or equivalent extensive experience
- consent to a Nationally Coordinated Criminal History Check and obtain a current Screening Clearance Number issued by the Department of Education’s Screening Unit prior to commencement of employment
- complete the Department’s induction program within 3 months of commencement
- complete any training specific to this role required by Departmental policy
- complete the Department’s training in Accountable and Ethical Decision-Making within 6 months of appointment and every 3 years thereafter
- complete the Department’s Aboriginal and Torres Strait Islander cultural awareness online course within 3 months of commencement.

Certification

The details contained in this document are an accurate statement of the responsibilities and other requirements of the position.

ENDORSED

Date 15 August 2024
Reference D24/0591047