# Manager Cyber Operations

POSITION DESCRIPTION FORM

**Region / Portfolio:**
Technology

**Directorate / Command / District / Division:**
Enterprise Security and Risk Management Division

**Work Unit:**
Operations

**Position Description Number:**
227506

**Level:**
Level 6

## Employment Conditions

Industrial Agreement/Award: Current PSA PSCSAA and Agency Specific Agreement

Work Pattern: Monday – Friday (Day Work): May be required to work outside normal operating hours
This role may be included in an On-Call roster to support 24/7 cyber security coverage.

Location: Perth

## Position Objective

Leads the operational delivery of security operations by overseeing vendor-provided Security Operations Centre (SOC) services, validating operational performance against Service Level Agreements (SLA) and playbooks, coordinating effective incident prevention, detection and response, and overseeing vulnerability management technology. Supervises Security and Risk Officers, maintains alignment across SOC workflows, internal escalation paths and Security Orchestration Automation and Response (SOAR) tooling, and ensures technical compliance by applying established standards and performing operational assurance activities. Monitors operational metrics and implements process improvements and automation to enhance service efficiency and cyber resilience.

## Role of Work Unit

Security Operations is responsible for the WA Police Force Security Incident Management and undertakes cyber security incident protection and response, administration account management, cyber threat monitoring and governance oversight of the managed security service providers (MSSP).

Enterprise Security and Risk Management is responsible for safeguarding the WA Police Force's information assets, systems, and infrastructure by implementing robust cybersecurity and risk management strategies. This unit plays a critical role in ensuring the confidentiality, integrity, and availability of information essential to the agency's law enforcement operations. It focuses on developing and executing comprehensive security policies, frameworks, and proactive threat management programs while ensuring compliance with relevant Australian regulations and standards.

## Reporting Relationships

This position reports to:

- Executive Manager, Level 7

Direct reports to this position include:

- Security and Risk Officer, Level 3 x 2

Total number of positions under control: 2

## Key Accountabilities

### 1 Delivery and Monitoring (60%)

1.1 Oversees day-to-day delivery of 24/7 SOC services including monitoring, detection and incident response.
1.2 Supervises activities of Security and Risk Officers, providing guidance, support and performance management.
1.3 Monitors vendor adherence to operational SLAs and identifies areas of non-compliance for internal escalation and follow-up.
1.4 Contributes operational insights and service delivery feedback to vendor performance reviews and capability assessments to support continuous service improvement.
1.5 Maintains alignment between SOC workflows, internal escalation paths, and SOAR tooling.
1.6 Evaluates incident handling timeliness, playbook adherence and documents findings for follow up and action tracking.
1.7 Applies established prioritisation criteria when reviewing remediation recommendations.
1.8 Supports the implementation of advanced detection techniques to enhance operational maturity.
1.9 Reviews vendor delivery of detection, response, and vulnerability management activities and reports deviations or emerging issues.

### 2 Cyber Security Monitoring and Reporting (20%)

2.1 Reviews vulnerability scanning processes for accuracy, completeness and follow-up
2.2 Collects, validates, and analyses operational data to support reporting on vendor performance, risk exposure, and KPIs.
2.3 Tracks mean-time-to-detect, mean-time-to-respond, and SLA compliance and produces regular operational summaries.
2.4 Performs technical assurance activities supporting protection, detection, and response capabilities.
2.5 Applies established standards to recommend remediation actions.

### 3 Operational Coordination (15%)

3.1 Coordinates daily operational activities with outsourced providers to ensure the effective security operations function.
3.2 Develops and supports the performance of Security and Risk Officers by providing guidance, feedback, and upskilling opportunities.
3.3 Facilitates communication and workflow coordination between internal teams and vendor personnel to maintain strong cyber resilience and operational reliability and efficiency.
3.4 Contributes to the continuous improvement security technologies and processes, and implements operational improvements and applies automation opportunities to enhance efficiency and SLA performance.

### 4 Other (5%)

4.1 Understands and complies with information security policies and procedures to mitigate areas of information security risk by ensuring the integrity, confidentiality, availability and security of information holdings/systems.
4.2 Demonstrates and advocates a high level of ethics and integrity in accordance with the agency's professional standards and Code of Conduct including reporting wrongdoing.
4.3 Undertakes other duties as directed.

## Specialist Prerequisite(s)

It is a requirement that the position holder is:

- An Australian Citizen prior to the completion of the selection process;
- Successful in obtaining and maintaining a NEGATIVE VETTING **LEVEL 1** security clearance for the duration of their appointment in the position.

## Work Related Requirements

| **Essential** | **Context in which work related requirements will be applied and or general standard expected.** |
|---|---|
| Experience with Security Operations Centre processes, incident response and vulnerability management | Applying operational knowledge of SOC workflows, vulnerability management processes, and incident response practices; managing operational pressures during cyber incidents and executing required actions |
| Technical Skills | Using SIEM/SOAR platforms and applying hands-on technical capability to support cloud security operations (Azure, AWS) and vendor-delivered monitoring services. |
| Technical leadership skills | Leading and supporting the daily work of technical staff and service-provider personnel. Guiding team members to meet operational expectations and deliver consistent outcomes. |
| Communication and interpersonal skills | Engaging with internal and external technical stakeholders, preparing complex operational reports, and explaining technical issues in clear language suited to the audience. |
| Analytical, conceptual and problem-solving skills | Identifying, analysing, and resolving emerging operational issues. Developing practical solutions to improve workflow efficiency and service outcomes. |
| Contract and vendor management | Monitoring operational aspects of vendor performance, reviewing service delivery quality, and documenting issues or risks requiring escalation through appropriate internal channels. |
| **Desirable** | |
| Possession of or progression towards relevant qualifications | Working towards qualifications in Cyber Security, IT or Risk Management; or holding/working towards certifications such as CISSP, CISM, GIAC. |
| Experience implementing frameworks | CSF Applying knowledge of ASD Essential Eight, ISO 27002 and NIST CSF in an operational environment. |

## Capability Framework

The framework is intended to support staff and supervisors through the performance cycle and identify core competencies relevant to the rank and/or classification level.

## Leadership Context

We believe all our people are leaders irrespective of their role. We consider this as critical to our success and, to support this, we have adopted **Leadership Expectations** which provides a common understanding of the mindsets and expected behaviours required of all our employees and the public sector.

The leadership context for this role is **Leading Leaders.**

## Certification

These details are an accurate statement of the duties, responsibilities and other requirements of the position.

| **Position Title and Work Unit** | **Name** | **Date** |
|---|---|---|
| Senior Organisational Design Consultant, Organisational Design and Analysis | Julie Ismail | 19/03/2026 |
| Assistant Commissioner Technology | Marc Smith | 23/01/2026 |