# Security operations SCAD

Manages and administers security measures, leveraging tools and intelligence to protect assets, ensuring compliance and operational integrity.

|  |
| --- |
| **Guidance Notes:**  Activities may include, but are not limited to:   * providing advice and guidance on the implementation and enforcement of security controls, including proactive cloud security measures * using security tools such as Security Information and Event Management (SIEM), Intrusion Detection/Prevention Systems (IDS/IPS), and firewalls, alongside the use of automation to streamline security operations. e.g. automatic patching, vulnerability scanning, and rapid response to common threats * acting on threat intelligence to proactively address potential security threats, and conducting routine vulnerability assessments monitoring and analysing relevant logs, alerts, and events, and responding to incidents submitted via tickets or phone * performing rapid analysis and remediation of security issues * ensuring compliance with relevant legislation, adherence to security policies, and maintaining standard security operating procedures * keeping accurate security records and documentation * implementing, managing, and monitoring cryptographic and certificate management activities to protect data, ensure compliance, and manage cryptographic keys securely * using advanced reporting techniques for comprehensive security oversight and informed decision-making. |

## Level 1

Performs simple security administration tasks.   
Maintains relevant records and documentation, contributing to overall data integrity.

## Level 2

Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken.  
Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques.  
Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.

## Level 3

Investigates minor security breaches using established procedures , incorporating analytical tools and techniques.  
Performs non-standard operational security tasks adapting to evolving technologies and threat landscapes.  
Addresses and resolves a variety of security events to ensure system integrity and operational continuity.

## Level 4

Maintains and optimises operational security processes. Checks that all requests for support are dealt with according to established protocols, including for cloud-based and automated systems.  
Provides advice on implementing and managing physical, procedural and technical security encompassing both physical and digital assets.  
Investigates security breaches in accordance with established procedures using advanced tools and techniques and recommends necessary corrective actions.   
Enables effective implementation of recommended security measures and monitors their performance.

## Level 5

Oversees the adherence to and effectiveness of security operations procedures, including cloud security practices and automated threat responses.  
Reviews actual or potential security breaches and vulnerabilities and ensures that they are promptly and thoroughly investigated. Recommends actions and appropriate control improvements.  
Ensures the integrity and completeness of security records , ensuring timely support and adherence to established procedures.  
Contributes to the creation and maintenance of security policies, standards and procedures integrating new compliance requirements and technology advances.

## Level 6

Develops comprehensive policies, standards, processes, guidelines for organisational security, including automated systems and cloud environments.  
Ensures the ongoing relevance and effective implementation of security policies and standards, adapting to emerging technologies and threats.  
Reviews and advises on security aspects of new business initiatives considering implications in the evolving digital landscape.  
Leads strategic planning for security operations, integrating advanced threat intelligence and automation to enhance organisational resilience.