JOB DESCRIPTION

Job Title: Senior Information Security Analyst

Grade: D

Department: Technology

Main purpose of job:
You will support the Information Security Manager in the maturing CAF's security operations and the day to day running of CAF's security programme. This will involve ensuring that the correct security controls are in place, that they are working effectively, and that they are implemented appropriately in technology projects and processes.

The role will support the delivery of the Technology strategy by providing expertise in relation to the secure configuration of managed services and cloud-based IT services, particularly Microsoft Azure, 365, and the associated security stack.

The role sits within a multi-disciplinary security team in which all analysts will work on a mixture of security operations, assurance, and governance activities, with significant cross-training.

To support this model, we are looking for a senior information security analyst with a mixture of hands-on security operations experience using tools such as Microsoft Sentinel and Defender; and understanding of how these relate to risk management at all levels of the organisation. You will be able to effectively triage, prioritise and communicate key activities and mentor junior analysts in how to deliver security value.

Responsible to: Information Security Manager

Budgetary responsibilities: None

Responsible for (staff/jobs): None

Key Job Responsibilities:
- Provide first- and second-line Security Operations support including control health check; triage of tickets, events, and incidents; and support with user queries.
- Undertake investigations of security issues and security incidents, providing a timely and thorough response.
- Support vulnerability management efforts through the effective triage of vulnerabilities across the estate and supporting technology teams with remediation.
- Ensure that processes and guidance reflect industry best practice and developments, balancing risk management with operational effectiveness.

- Assist with the management of the ISMS, coordinating the updates to, and approval of policies and standards.
- Perform security risk assessments, followed by initiating and managing appropriate remedial action, to ensure that IT infrastructure and application systems are adequately protected.
- Provide security and risk assessment consultancy on projects and other formal workgroups and committees, making appropriate recommendations for security design and risk mitigation to ensure that IT and information security is considered in the design of new services or changes to existing services.
- Identify risk management approaches for cloud-based and managed services.
- Support the Information Security Manager in completing all tasks necessary to meet regulatory, legislative and audit requirements such as PCI-DSS, GDPR, Swift, FCA/PRA etc.
- Manage stakeholder queries with a trustworthy, methodical, and timely approach.
- Actively promote Information Security including education and awareness throughout CAF.
- Work as part of a 24x7 support rota.

CAF Values and Behavioural Indicators

The CAF Values and Behavioural Indicators set out in a transparent and consistent manner the explanation of the performance expectations of all CAF People. Through the use of common language and common standard, it combines a set of behaviours with the required technical skills and knowledge needed to effectively perform in any given role in CAF. This is used for the assessment, management and development of performance of all our people across CAF

Please refer to the link: CAF values and indicative behaviours for the CAF Values and Behavioural Indicators.

Dated: August 2025

PERSON SPECIFICATION

Job title: Senior Information Security Analyst

Date: August 2025

Attributes *	Essential ✓	Desirable ✓	How Evidenced†
Experience			
• Significant experience of working in a security related role, with demonstrable experience in the Microsoft Security suite.	✓		A/C
• Experience of working in an environment where PCI or FCA compliance is a requirement.		✓	
Qualifications			
• Degree in information security, or equivalent work experience		✓	A/E
• Certifications from Microsoft covering Azure and M365 security such as AZ-500 or MS-500		✓	
• Certifications from Firewall, Anti Virus, Cisco networking and Network Access control vendors		✓	
• Certificate in Information Security such as CISSP, CCSP or CompTIA Security +	✓		
Specialist Skills/ Ability/Knowledge			
• Good understanding of Risk Assessment framework and methodologies	✓		A/C/T
• Strong understanding of securing Microsoft cloud services		✓	
• Technical expertise (i.e. hands on) with security-related controls, systems and applications.		✓	
• Experience of managing compliance and security programs for applications and technical infrastructure	✓		
• Project lifecycle methodologies	✓		
Communication			
• Good written and verbal communication skills as the role will be expected to produce management information and deal effectively with 3rd party suppliers.	✓		C
• Explain complex security issues in a fashion that could be understood by non-technical people.	✓		

Personal Qualities • Experience of prioritizing and overcoming obstacles to drive through security initiatives. • Strong analytical and problem-solving skills to enable effective security incident and problem resolution • Proven ability to work under pressure in emergencies, with the flexibility to handle multiple high-priority situations simultaneously • Ability to work well under minimal supervision and understand when to escalate with discretion • Strong team-oriented interpersonal skills, with the ability to interface effectively with a broad range of people and roles, including vendors and IT and business personnel • Strong customer/client focus, with the ability to manage expectations appropriately; provide a superior customer/client experience and build long-term relationships • Be tenacious and persistent in ensuring that tasks are completed to the highest possible quality • Using initiative to identify areas for improvement • A willingness to learn and take on new responsibilities	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓		C
Special Conditions Need to be flexible as there may be a requirement to be contacted out of hours in certain situations.	✓		C
Prior to Appointment All posts: • Credit Check • Sanctions Check • Basic DBS Check • Employment References • Medical Clearance • Right to Work in the UK	✓ ✓ ✓ ✓ ✓ ✓ ✓		R/E