Role profile

Role title	Cyber Security Analyst
Department and directorate	Technology Services
Job family level	All BMA Grade 6
Reports to (job title and name)	Chief Information Security Officer (CISO)
Direct reports (job title and name)	n/a

Summary – purpose of the role

Describe as concisely as possible the overall purpose of the job and including the core duties/responsibilities required to be performed in the role (e.g., to provide a full range of administrative support services to the department including x,y,z)

The purpose of this role is to assist the BMA in enhancing and maintaining its Information and Cyber Security posture. Reporting to the Chief Information Security Officer (CISO) and collaborating with the Platforms Infrastructure Team, the post holder will provide technical and operational expertise in the use of security tools, processes, and policies to improve the overall security of the BMA.

Primarily involved with core cyber operations such as incident management, vulnerability management, security monitoring and threat detection, the post holder will also represent security at the weekly Change Advisory Board. Additionally, the post holder will collaborate across the Technology Services teams to identify, assess, and mitigate security risks whilst ensuring adherence to our internal polices and industry standards.

- **Cyber Operations and Incident Response** – Support the Chief Information Security Officer (CISO) in managing and executing measures to detect, respond to, and mitigate cyber threats that impact our digital information assets and operations.
- **Incident Investigations and Remediation** - Lead the response to security incidents, managing containment and resolution according to predefined playbooks, and escalating to the Chief Information Security Officer (CISO) when necessary. Conduct thorough investigations of security incidents, identify root causes, and implement strategies to eliminate vulnerabilities and prevent recurrence.
- **SIEM Expertise** – Optimise and manage the SIEM solution in collaboration with the external Security Operations Centre (SOC). Additionally, design and implement custom playbooks within the SIEM to enhance threat detection and incident response capabilities.

  Participate in the development and enhancement of SOC processes, workflows, and procedures to improve incident response efficiency and effectiveness.
- **Threat Hunting and Analysis** - Proactively seek out advanced threats and vulnerabilities within our environment by leveraging various threat intelligence sources and security tools.

BMA

Summary – purpose of the role

Thoroughly analyse and interpret security data from multiple sources, including our SIEM, network traffic, and endpoint data, to identify emerging threats and attack patterns.

- **Security Assessments and Compliance** - Perform regular vulnerability assessments and assist with penetration testing and remediation activities, including analysis and prioritisation of vulnerabilities across our 'systems, networks and applications' based on exploitability and potential impact.

  Conduct internal security audits to evaluate the effectiveness of security controls in place to mitigate risks ensuring compliance with the Cyber Essentials Plus and ISO27001 security frameworks.

- **Security Engineering and Architecture** - Provide guidance and support to our project and DevOps teams in implementing secure solutions, ensuring the integration of security into CI/CD pipelines and development practices.

  Security Operations – Provide Business as Usual (BAU) Security Operations support to our business processes, ensuring access and changes are in alignment with BMA security policies, standards, and guidelines.

  Optimize BMA Information Security solutions, including SIEM and Vulnerability Management Suite, O365 Security and Compliance, Azure Cloud Tenancy, Email Security Gateway, DLP, anti-malware, firewalls, IPS, VPN, and other technical security controls.

  Assist in the identity and access management process, performing regular privileged account reviews.

  Participate in our weekly change board to evaluate changes for security concerns.

- **Collaboration and Communication** - Effectively communicate with staff, external vendors, and both technical and non-technical stakeholders, translating complex technical concepts into understandable terms.

  Offer security guidance to our Platforms Infrastructure team, including detailed technical advice. For instance, system hardening (such as operating systems and network devices).

- **Awareness** - Assist in the design and delivery of the BMA's cyber security awareness training, fostering a culture of security within the BMA.

  Remain updated with the latest cyber security news, threats, intelligence, tactics, techniques, and vulnerabilities. Research and analyse new threats and vulnerabilities to assess their impact on BMA operations.

- **Reporting** – Produce security updates and reports for the Chief Information Security Officer (CISO) and Head of Infrastructure.

  Support reporting on key performance indicators (KPIs) for Information Security risk management and compliance, through actionable reports and dashboards on risk, compliance status, and key metrics for the CISO and Information Governance Steering Group (IGSG).

BMA

Skill (level and breadth of application)

What relevant experience is necessary to undertake this role? What specialist, technical or professional qualifications are required to be able to perform the job?

How far does the role extend out across the organisation, e.g., confined to own team, involves co-ordination with another department or requires regular negotiation with many other parts of the organisation. Why is this necessary? Describe the range of issues that are involved in this, e.g., resolving people's IT problems, collecting information on key research items, or advising members on a particular issue.

- Broad experience across multiple cyber security domains (protection, detection, response, recovery and resumption of services, situational awareness, testing)
- Experience in security incident management and response, digital forensics, and threat hunting.
- Extensive experience with Security Incident Event Management (SIEM) and security tools in a Security Operations Centre (SOC), contributing to process, workflow, and incident response improvements, resulting in increased efficiency and effectiveness.
- Experience in creating incident response playbooks, including Security Orchestration, Automation, and Response (SOAR)
- Experience with the operation of industry standard vulnerability management tools (e.g. Tenable Nessus, Qualys, Rapid7)
- Knowledge of network security, application security, cloud security, and endpoint protection.
- Experience with security tools and technologies such as firewalls, IDS/IPS, antimalware, SIEM, and encryption.
- Demonstrated experience in Azure Cloud security, including configuring and managing security controls in Microsoft Azure, Azure Security Centre, and Azure
- Experience of advanced email security protection principles (DKIM, DMARC, SPF) and solutions (Mimecast, Microsoft O365 EOP)
- Experience of Microsoft Azure, O365, Entra, (SharePoint, Security and Compliance Centre, Intune MDM, Exchange Online Protection, Advanced Threat Protection, MCAS, Microsoft Secure Score).
- Experience implementing Privileged Identity Management (PIM) and Privileged Access Management (PAM)
- Understanding of conducting security assurance assessments, audits, and managing remediation plans.
- Experience of secure system design architectures and advanced threat analytics at the enterprise level.
- Experience of secure development practices and potential threats in a hybrid cloud environment (OWASP) and the Mitre ATT&CK framework.
- Excellent analytical, written, and verbal communication skills including the ability to effectively communicate technical information to non-technical users.
- Passionate about cyber security, delivering work to a high standard with integrity and accountability.
- Knowledge and experience of working within recognised industry frameworks (e.g. ISO 27001, NIST 800-53, Cyber Essentials Plus, CIS, ASVS)
- Formal Information Security Certifications, including Security+, SSCP, CRISC, Microsoft AZ-900
- Desirable: CESG Cyber Professional (CCP), CEH, ECSA, OCSP, Microsoft AZ-500

Intellectual demands (complexity and challenge)

What sorts of problems, situations or issues are typically dealt with? Give any illustrative examples. How are the problems, situations or issues dealt with (e.g., undertaking original research and analysis or seeking specialist advice)?

To what extent are standard procedures and processes followed when undertaking typical tasks, and how is personal initiative used when solving problems? To what extent is creativity used in solving the problems (e.g., adopting different approaches, trying things that have not been done before within the organisation or improving/changing previous approaches).

- The post holder may need to research innovative security technologies or processes to aid in continual service improvement
- Work closely and daily across the team, BMA and BMJ to ensure all released changes meet sign-off requirements from a security perspective
- Provide regular feedback to the teams on any key cyber security issues.
- Demonstrate Self Learner mindset through alignment of individual skilling to team/area demands and continuous upskilling to align to Tech Services success goals
- Consistently apply "lessons learned" model, personal accountability & teamwork
- Ensure delivery meets/exceeds all operational excellence guidelines and best practices
- Creation of new security systems procedures based on best practice where appropriate

Judgement (independence and level and impact limitations)

What are the typical decisions that are made in the job without reference to any higher authority? What informs/constrains the decisions (e.g., expenditure limits, have to follow clearly laid down procedures or working within broad objectives). What influence upon policy, procedures or resources is there (e.g., giving advice to others)?

Who (or what) is next to be affected by the decisions that are made – for example, supervisor sees them before they leave the team or the whole department sees and has to respond to the change that is made. Give typical example(s) of the consequences of the decisions (e.g., what impact does the decision-making have on the performance of the team/section/department/organisation)?

- The post holder will be required to use their own initiative, to plan and organise their own workload and handle work in accordance with normal office protocols, and organisational policies and procedures.
- On regular basis they will work without direct supervision and deal with routine matters without seeking further advice.
- The post holder will be responsible for bringing potential service affecting issues to the attention of management. These will include security threats that may comprise the integrity of the Associations infrastructure or data.
- Responsible for evaluating and specifying products that will meet business requirements.
- Providing technical lead on projects within any assigned workload.
- Ensure that standard operating procedures exist and are kept up to date.

Use of resources (supervision of resources and influence)

What responsibility is there for managing people, equipment, budgets, resources, customer's welfare, or confidential information? If this is a staff management role describe what is involved, e.g., staff reporting, staff development, appraisal, leading a department or the allocation of work.

How does the role fit within the organisation, e.g., support role, team member, team leader, specialist policy adviser, or leading major areas of core business?

- Work closely with existing 3rd parties and other external bodies to ensure continuous operation and to ensure any problems are dealt with as quickly as possible.
- Work closely and daily across the team, BMA and BMJ to ensure all released changes meet sign-off requirements.

BMA

Communication (level, internal and external demands, and significance)

*What people are typically contacted (regardless of the medium) **inside** the Association, e.g., immediate colleagues, senior managers, or administrators? Committee members are the only members classed as internal communication. Normal non-committee membership and doctors are external (see below)*

*Who is in regularly contact with the role holder **outside** of the Association, e.g., members who are not committee members, suppliers, members of the public? Approximately what percentage of the time is spent on external communications?*

What is the purpose of these contacts, e.g., conveying information, gathering data?

- Most of the internal contact is within the IT technical teams both BMA and BMJ, there is also contact with senior managers across the organisation.
- Regularly contact with industry professionals and specialist outside the BMA, this can occupy 10-15% of the post holder's time.
- Relaying appropriate and relevant information to the relevant team representatives. Providing training and/or training material to ensure the teams are appropriately equipped to administer and support the services used by the Association.
- Providing regular feedback to the teams on any key system issues, briefing senior managers on data security trends. Working with 3rd party contactors, specialists, and consultants on implementation of new products as and when the need arises, also for gathering information on new products and procedures.

Physical demands & coordination (physical effort and mental strain)

Are there any unusual physical or mental demands of the role; for example, lifting heavy objects, standing for long periods, using VDUs extensively or high levels of concentration?

- There are periods throughout the year when the physical demands of the job will be high.
- An elevated level of concentration is required when working on complex problems in situations that could cause catastrophic consequences to the Business if a wrong decision is made, or a process is missed.
- Prolong use of VDUs over and above a standard use due to deploying technology or fixing problems that would require working extended hours.

Working conditions and emotional demands

What are the environmental conditions in which the work is conducted, the social and emotional demands faced by the role and the pressures resulting from these?

- The role also requires occasional travel to other offices to often work out of hours unsupervised these impact on social life as some of these require overnight stays or early starts or late finishes.
- There is a varying amount of stress from the weight of the importance/impact of some of this work.

BMA

BMA competency level required

The post holder is expected to execute their role in line with our five organizational values. These are currently being translated into behavioral indicators that will form part of our new performance management process. The following examples illustrate how we are using our values to inform how we act:

- We are **leaders** because:
  - We strive to always improve.
  - We take responsibility for our actions.
  - We collaborate with each other and work as one BMA for the good of our members.
  - We are proactive and prepared to guide our members and each other.
- We are **experts** because:
  - We understand our members
  - We draw on our collective experience and knowledge to solve problems.
  - We use our insights and research to make decisions.
  - We provide accurate, credible, relevant, and engaging information.
  - We recognise our strengths and act upon them.
- We are **committed** because:
  - We listen to our members and put them at the heart of everything we do.
  - We are respectful, inclusive, open, and honest with our members and each other.
  - We approach everything we do with confidence and sensitivity.
- We are **reliable** because:
  - We deliver on what we say we will do.
  - We are accessible and approachable.
  - We build trust by being consistent and supportive.
  - We are positive and decisive whatever the situation.
- We are **challenging** because:
  - We fight, ethically and fearlessly, for the interests of all our members.
  - We work as a brave, assertive, and effective champion for high quality health. services and the advancement of the profession.

Sign-off

Manager:	Date:
Role holder:	Date: