Job Description

Job descriptions should be no more than four pages when complete.

Where you are amending an existing job description you must make the changes using Track Changes.

Once you have decided what role you require within your team / department structure, you need to articulate this into a job description. This needs to be a specific description of the role, including the responsibilities that the job-holder will carry out as well as what qualifications and skills they will require to fulfil the role. Please note: job description should not be based on an individual but on the role the business requires.

Job descriptions must be accurate and created before the recruitment process.

A Post Details

Job Title: Cyber Security Compliance Manager	Grade: Only state the grade if this an existing role otherwise leave blank
Department: Technology	Division: A
Reports to: Head of Cyber Security	Contract Type: Select Contract Type
Level of Vetting:**Management Vetting**	Numbers in Post: 1

B Purpose of the Post

The Cyber Security Compliance Manager is responsible for the confidentiality, integrity, and availability of all our assets whilst continuously improving compliance within these areas. You will be the subject matter expert on all things related to information security risk management and assessment, providing assurance for compliance requirements to ensure adherence with our Technology policies.

The scope of the role encompasses the implementation of compliance management procedures, performing Security assessments and providing Security expertise and support for the monitoring of compliance and associated remediation activities. The role will take responsibility for delivering compliance metrics and tracking key remediation/improvement of Security to ensure they are delivering for the force.

The postholder will also offer specialist advice and guidance to stakeholders as well as upskilling team members and assist in maturing the existing cyber security function.

BTP operate a flexible working policy, including the ability to work from home. The role will be based at our Force Head Quarters (FHQ) in Camden and will require at least 2 days in the office.

Travel to sites may be required and flexibility in working hours to manage/resolve high priority incidents.

C Dimensions of the Post

Financial – Direct or Non-Direct Direct: No Direct Financial Responsibility. Non-direct: None Staff Responsibilities – Direct or Non-Direct Direct: None. Any Other Statistical Data: The role will involve being on call and part of an on-call rotation for the provision of support services during outage, compromise or incident response / recovery

D Principal Accountabilities

- Lead in maintaining the Technology Information Security Risk Register, holding key individuals accountable for remedial action
- Collaborate on Technology projects to ensure that security policy/risk issues are addressed throughout the project life cycle
- Manage the ISO 27001 ISMS implementation, from scoping, risk assessment, documentation to controls design, implementation, and external audit
- Ensure the ISO 27001 ISMS is maintained and updated
- Perform security controls testing across the scope of ISO 27002 and NIST, including design & operational effectiveness testing and remediation test activities
- Perform supplier due diligence, security assessments, and ISO27001 aligned security audits of suppliers
- Monitor third-party risk assessments and assist in performing internal risk assessments
- Develop key performance metrics to track and ensure compliance with established security policies and standards (ISO27001/NIST)
- Create security performance dashboards and provide regular reporting to the Head of Cyber Security and BTP forums on security internal audits, progress and compliance status
- Provide Technology project teams with requirements and design input regarding security compliance
- Act as a go-to technical resource for compliance matters.
- Lead on compliance assurance assessments (e.g. annual ITHC, Control Assessments, Third Party Vendor Assessments.)
- Development and publishing of BTP Cyber Security policies and standards and procedures
- Drive Security maturity through metrics and evidence-based findings
- Support Cyber Security training and awareness activities and initiatives

E Decision Making

- Incident management priorities related to Cyber Security
- Proactive Cyber Security health-checks and infrastructure/services security monitoring
- Access management controls and best practices in place to manage the access of BTP
- employees.
- Specific recommendations affecting Cyber Security projects (SOC, SIEM, Accreditations,
- Threat Intelligence)
- Key input to the Change Authority Board (CAB) and associated Cyber Security planned
- works.
- Develop and implement a strong risk management regime, ensuring Cyber Security controls are adequately applied to all relevant infrastructure and services

F Contact with Others

Internal:

- Contact with domains across the Technology function (Infrastructure, Applications, Service

Desk)

- Engagement with management across the Technology organisation.
- Engagement with wider BTP functions including Digital Policing, Information Management

CCTV, SSU, CCU

G Essential Criteria

- Strong knowledge and experience with security policies and standards
- Technical aptitude and knowledge across the spectrum of cyber security solutions and operations
- Experience in providing advice on data protection, cyber security, and business continuity
- Experience of implanting and supporting security control frameworks, such as NIST and ISO27001/2.
- Knowledge and experience of cyber security maturity frameworks such as NIST CSF and its Implementation Tiers, Cybersecurity Capability Maturity Model (C2M2) and NCSC CAF
- Strong experience in measuring compliance of an organisation or digital systems against a given set of security criteria
- Strong stakeholder engagement skills, detail-oriented, delivery-focused, and able to manage multiple work streams simultaneously
- Ability to prioritise workload based on the severity of impact and risk to BTP
- Strong interpersonal skills, able to communicate across a broad spectrum of users, building relationships with senior internal and external stakeholders
- Excellent oral, written and presentation communication skills

Qualifications and Training:

- Educated to degree level or equivalent experience
- Experience of risk management methodologies, frameworks and standards such as ISO27001, ISO31000, ITIL, COBIT, NIST Cyber Security Framework (CSF)
- Recognised industry qualification e.g. CISSP, CISM, CEH, CISA, Security+

Experience:

- Significant experience of creating mature cyber security environments aligned to the usage of industry best-practice frameworks such as ISO-27001/NIST/CIS
- Experience reviewing compliance evidence and communicating findings to owners
- Experience collaborating cross-functionally to identify and implement best practice Security, across all aspects of Security.
- Experience working with industry and regulatory frameworks and standards.
- Demonstrable evidence of effective problem-solving skills in complex support BC & DR, including experience relating to Cyber Security, Compliance, or Assurance.
- Significant experience in leading third-party assessments and running third-party assurance activities, preferably against a recognised framework.
- Significant experience of conducting compliance reviews, including creation of GAP analysis reports and remediation plans.
- Demonstrated ability to analyse and coherently present complex threat risk information relevant to the audience that clearly articulates business impact(s)

Skills:

- Strong analytical, reasoning, and organisational skills are essential
- Strong verbal and written communications skills are essential
- Ability to prioritise and handle multiple tasks simultaneously
- Ability to work in collaboration with colleagues across technology around incident and problem management
- Exceptional communication and collaboration skills with proven success to influence, inspire and support a diverse Tech community
- Ability to build relationships at all levels with excellent interpersonal skills and evidence of ability to influence decision-making.
- Proven track record of cyber technical security experience and to be seen as a subject matter expert for BTP
- Ability to demonstrate an exceptional analytical skill set and knowledge of current and evolving Cyber threats

Knowledge:

- A good knowledge of Cyber Essentials and experience of preparing and working towards successful accreditation is important along with experience of Securing Cloud Technologies (Microsoft Azure & Office 365)
- Good knowledge of frameworks such as Cyber Essentials, Minimum Cyber Security Standards, National Cyber Security Standards (NCSC) 10 Steps, and National Institute of Standards and Technology Controls Security Framework (NIST CSF).
- Authoritative knowledge of risk methodologies and experience applying these in assessments.
- Knowledge of cyber security threats, risks and an ability to explain their observations to team members.
- An Expert understanding of security compliance & detailed knowledge of a control framework such as NIST CSF, SP800-53, SP800-37, and ISO270001/2
- Strong knowledge of risk management frameworks such as ISO27005 and 31000
- An Expert understanding of security maturity & detailed knowledge of a security maturity frameworks such as NIST CSF and its Implementation Tiers, C2M2 and NCSC CAF.
- Strong knowledge of threats, risks and impacts associated to cyber security

Desirable criteria:

- Experience implementing cyber risk management and compliance methodologies and processes.
- Experience managing subcontractors providing technical risk consulting teams.
- An industry recognised certification in Information Security and/or Risk Management

H Additional Information

- Flexible to travel across the UK as required
- On call requirement within the role supporting the function

For Panel to complete only:

Line Manager Approval: (this is only signed off when the line manager has approved the final version)

Panel Approval: (this will only be signed off once the job has gone through the Job Evaluation Panel)

Date: Click or tap to enter a date.

Email the Job Evaluation submission form together with supporting documentation (organisational charts, job descriptions) to **People & Culture Policy & Reward inbox**

You will be advised of a panel date following receipt of the submission