Job Description

A Post Details

Job Title: Governance, Risk & Compliance Manager	Grade: B004
Department: Information Management Unit	Division: A Division
Reports to: Head of Information Management Unit / dotted line to SIRO	Contract Type: Permanent
Level of Vetting:**Management Vetting**	Numbers in Post: 1

B Purpose of the Post

Policing is inherently information-led, and information assurance is critical to maintaining operational effectiveness in the face of evolving threats. This role leads the strategic direction and operational delivery of British Transport Police's Governance, Risk and Compliance (GRC) function, ensuring the organisation upholds a robust Information Security Management System (ISMS) aligned with national policing standards, including the National Community Security Policy (NCSP), Police Cyber Assurance Framework (PCAF) and Secure by Design (SbD) principles, and industry standards such as the National Institute of Science & Technology (NIST) and ISO 27001.

The postholder will oversee risk management for projects, suppliers and contracts, policy governance, third-party assurance, monitoring and audit, and incident management. They will lead a team of GRC Officers, providing direction, coaching, and oversight, and will escalate or accept risk as appropriate to the Head of Information Management (HoIM). This role is central to embedding a culture of compliance, continuous improvement, and proactive risk mitigation across the organisation.

C Dimensions of the Post

Financial – Direct or Non-Direct
N/A

Staff Responsibilities – Direct or Non-Direct
Direct: Line management responsibility for Governance, Risk & Compliance Officers x 3.

Any Other Statistical Data
Provide quarterly and annual statistics on risk management and assurance work, incident management & compliance with policy and processes, to force governance boards as required.

D Principal Accountabilities

Strategic Leadership & Governance

- Lead the development, implementation, and continuous improvement of BTP's ISMS in line with ISO 27001, the National Policing Cyber Security Strategy (NPCSS), and the NCSP.
- Act as the senior lead for information assurance governance, risk appetite, and assurance strategy, ensuring alignment with the National Police Information Risk Management Framework (NPIRMF).
- Provide expert, risk-informed advice and briefings on compliance, risk, and governance across the organisation.

Third-Party Assurance (TPAP)

- Oversee third-party risk management using the NPCC TPAP framework, ensuring due diligence, assessment completeness, and compliance through BTP's assurance platform.

- Ensure external suppliers meet BTP's information security and compliance standards, with regular reporting to governance boards.

Policy & Compliance Oversight

- Lead the development, review, and governance of information security and assurance policies, ensuring clarity, consistency, and compliance with national standards and legislation (e.g. GDPR, DPA 2018).
  - Ensure policies are accessible, regularly reviewed, and aligned with the NCSP and SbD standards.
  - Monitor compliance through internal audits and assurance activities, reporting findings to governance boards.
- Ensure team processes are documented, maintained, and continuously improved.

Team Leadership

- Lead, coach, and develop the GRC team, fostering high performance and professional growth.
- Promote collaborative working, agile practices, and continuous improvement.
- Support self-management and cross-functional working by removing barriers to team performance.

Risk Management

- Oversee the identification, assessment, mitigation, and documentation of information risks across the force, including those related to projects, suppliers, and national systems.
- Maintain and evolve the organisational risk register, ensuring risks are escalated appropriately in line with the National Police Information Risk Management Framework (NPIRMF) and national appetite thresholds, setting and regularly reviewing the force risk appetite.
- Promote a risk-aware culture and embed risk-based decision-making across all GRC activities.

Incident Management

- Lead the force-wide incident reporting and response process, ensuring incidents are logged, triaged, investigated, and reviewed in accordance with national guidance.
- Ensure incidents are logged, investigated, and reviewed, with lessons learned integrated into policy and training.
- Report regularly to internal boards and national policing bodies.
- Coordinate with the National Management Centre (NMC) for significant incidents.

Cryptography

- Perform role of BTP's designated Crypto Custodian and maintain the Force's Crypto Account to enable BTP to exchange encrypted information with appropriate external organisations and agencies.

Security Assessment for Policing (SYAP)

Ensure the force information assurance posture is continually assessed, monitored and improved through:

- Regularly updating control maturity ratings in conjunction with colleagues in Cyber and Technology
- Ensuring consolidated SYAP data is submitted quarterly to the Police Information Assurance Board (PIAB)
- Escalating risks that exceed local appetite to HoIM
- Supporting the production of the annual Senior Information Risk Owner (SIRO) report
- Acting as primary liaison between BTP and Police Digital Services (PDS)

Prepare strategic position papers and advise the HoIM, and relevant governance boards on the development, implementation and compliance with information security policies, guidelines and procedures.

E Decision Making

F Contact with Others

Stakeholder Engagement (Internal & External)

- Build and maintain strong relationships with internal departments across the force including colleagues at all levels, national policing bodies (e.g. PIAB, NIRMA), and external regulators (e.g. ICO, NCSC).
- Represent BTP in national forums and working groups, ensuring alignment with emerging cyber security and assurance developments.

G Essential Criteria

Qualifications and Training:

- Educated to degree level or equivalent in a relevant discipline, or significant equivalent experience in Information Assurance
- ISEB Qualification in Information Security Management (CISMP)
- CISSP and on-going affiliation with relevant industry body
- Crypto-custodian training from a nationally-recognised training provider
- GDPR/Data Protection certifications

Experience:

- Significant experience in information security, risk management, and compliance within a complex or regulated environment—ideally policing or public sector.
- Demonstrable experience in designing and implementing enterprise-wide governance frameworks.
- Excellent communication and influencing skills, with the ability to engage senior stakeholders and translate complex regulations into actionable guidance
- Experience in managing third-party assurance programmes.
- Experience in regulatory compliance and industry standards.
- Proven track record in developing and implementing security policies and procedures.
- Experience of devising and performing audits for a variety of subject areas to provide assurance
- Experience of accrediting systems and assuring against Codes of Connection for national policing
- Experience of Cryptographic control measures and accounting

Skills:

- Demonstrable skills in engaging, influencing and negotiating with a range of internal and external stakeholders at a senior level.
- Analytical skills and ability to present a logical argument.
- Preparation of technical reports and policies with the ability to communicate these simply and succinctly to a non-technical audience.
- Preparation of risk assessments for the confidentiality, availability and integrity of information assets.
- Skilled in developing policies, planning audits, and monitoring compliance to ensure organisational adherence to regulatory standards.

- Proven ability to lead, develop and create high-performing teams.
- Skilled and experienced in leading change and embedding new ways of working.

Knowledge:

- E Strong knowledge of ISO/IEC 27001, GDPR, and national security standards (e.g. NCSC, Cabinet Office, NPCC).
- Extensive working knowledge of relevant Information Security legislation
- Solid working knowledge of information security standards and best practice / ISO27001
- Understanding and empathy with managing large volumes of confidential information
- Sound up to date knowledge of best practice initiatives in Information Management
- Knowledge and opinion on issues relating to physical, procedural, and technical (ICT) aspects of Information Security.
- Knowledge of cryptographic standards and best practice
- Knowledge of accreditation processes and assurance methodologies

Desirable criteria:

H Additional Information

This is a specialist position which can significantly affect the Force. Failure of the Force to comply with ACPO policy and code of connection for Information Assurance and Security could result in BTP being disconnected from national policing systems such as PNC/PND. Police vetting must be attained.

For Panel to complete only:

Line Manager Approval: Helen Edwards 23/07/25

Panel Approval: Jodie Childs (3661)

Date:23/07/2025