

Job title	Information Security Manager		
Job family	Technical Systems & Delivery	Band	E

Job purpose

This role supports the Heads of Information Security (IS) in ensuring that data within the BBC is protected in accordance with the needs of the business and according to IS principles of confidentiality, integrity and availability, and to assist to deliver the IS strategy for the BBC. The role will line manage and oversee the day to day working of the IS staff within one of the areas of IS: Development, Governance or Operations.

Key responsibilities and accountabilities

- Manage relationships with teams across the BBC and their third party partners in order to resolve security threats and maintain secure systems.
- Provide technical and tactical advice to IS, BBC and its third party partners and act as the point of escalation for queries and concerns.
- Review the performance of key outsourced suppliers with regard to IS and governance functions.
- Develop and maintain key performance indicators, metrics and operational reports
- Manage the IS specialists, officers and junior officers, providing support, guidance and direction.
- Promote IS across the BBC
- Contribute to the formulation, implementation and maintenance of policies and procedures relating to the specialist area as well as the overarching divisional policies and procedures.
- Ensure that IS policies, related standards and guidelines are applied to requests internally and from the business.
- Deliver IS consultancy to the BBC ensuring that divisional and other local technology plans and solutions are in line with IS policies and standards.
- Manage the timelines, resourcing and delivery of assigned IS strategy projects.

Knowledge, skills, training and experience

Essential

- Experience of IS implementation, development or operations
- Ability to communicate at all levels of the business.
- Understanding of the technologies and architectures used to support IS.
- Record of operating in time critical, diverse corporate environments.
- Experience in management, in particular the ability to lead, support and develop teams of technical specialists within IT security or a related discipline.
- Ability to manage and resolve conflicts between technical and business imperatives.
- Excellent written and verbal communication and presentation skills.

- Highly effective and creative problem-solving skills.
- Experience overseeing multiple projects simultaneously.
- Good understanding of technical systems and processes in use within the BBC or a large corporate environment.

Desirable

- Negotiating and third party management experience.
- Formal IS qualifications or willingness to pursue such qualifications, in particular Certified Information Security Manager (CISM) or Certified Information Systems Security Professional (CISSP)
- Understanding of the guiding principles behind ISO27001 and related standards.
- Ability and confidence to prioritise and balance competing and diverse demands from technical and business perspectives.
- Experience of working with multiple stakeholders.
- Security check cleared or willing to undergo such security clearance.

Job impact

Decision making

- The holder of this post reports to the Head of Information Security. They will be expected to organize their own workload and that of their direct reports within the parameters set by the IS senior management team.
- Manage the relationships with key personnel both within the BBC and third party partners.
- Work closely with the business to ensure projects are supported and the BBC's policies and legal requirements are met.
- Network with peers across the media and security industries to maintain strong awareness of developments within the appropriate fields.
- Undertake/oversee reviews of new project and program requests and ensure that formal risk assessments are carried out as necessary.
- Make recommendations to project teams and sponsors on identified IS risks.
- Ensure all relevant business engagement documentation is reviewed and maintained for use by project teams.
- Ensure that relevant documentation has been completed and assessed before approving project requests.

Scope

- Expected to review and direct the workload of subordinates, and to ensure work is of the standard required, delivered within budget and agreed timeframes.
- Financial decision making against departmental spend up to £20,000.00.

Other information

For Reward team use only

JOB DESCRIPTION



Job Code	
Definition:	Content

This job description is a written statement of the essential characteristics of the job, with its principal accountabilities, incorporating a note of the skills, knowledge and experience required for a satisfactory level of performance. This is not intended to be a complete, detailed account of all aspects of the duties involved.

Appendix

There may be sub-sets of the generic job described above which require additional technical skills. This appendix to the generic job description can be developed to cover such situations.

Advertising Job title	Security Operations Centre Manager		
CPF Job title	Information Security Manager (Operations)		
Division	Design & Engineering		
Job family	Technical Systems & Delivery	Band	E
Location base	MediaCityUK, Salford Quays (Dock House)		

Organisation structure
Chief Information Security Officer Head of Information Security (Operations) Information Security Manager (Operations)

Additional Job Specific Accountabilities
<p>Leadership/Strategic Direction</p> <ul style="list-style-type: none"> Support the Head of Information Security (Operations), Head of Information Security (Development) and the other members of the Information Security leadership team in formulating the strategic direction of the SOC function and executing against the agreed strategy. <p>Programme/Project Roadmap Support</p> <ul style="list-style-type: none"> Support the integration of SOC processes with the overarching Information Security transformation programme, helping to ensure that we actively utilise the domain model to better target delivery of investigative resources to where they mitigate risk. Help define, support and oversee the delivery of projects committed to as part of the strategic roadmap. <p>Protective Monitoring</p> <ul style="list-style-type: none"> Manage the SOC use case development pipeline, prioritizing new use cases in accordance with their risk mitigation value + feasibility given existing log analysis capabilities. Decommission use cases that consume excessive resources for low return on investment. Actively liaise with the Information Security development team, ensuring SOC staff have a clear understanding of the capabilities of the toolset and can relate them to the environment and stakeholders. Understand clearly what is coming down the coverage pipeline and ensure that the SOC are trained and briefed on the organizational context and security utility of new event feeds. Make improvement recommendations to information security leadership team with respect to security monitoring approach (in particularly gaps in visibility that are harming effectiveness of monitoring.) <p>Incident Response</p>

- Act as incident manager for major security incidents, taking the lead on SOC response and actively assuring the delivery of any SOC actions agreed on incident calls.
- Ensure severe / complex incidents are escalated on a timely basis to the Infosec leadership team where additional specialist support is required.
- Ensure the SOC provide support to the Information Security Manager (Forensics) on high priority forensic investigations.

Governance and Team management

- Oversee the career development framework for the SOC team, providing clarity on how staff can achieve progression, and providing career coaching and mentoring to specialists/direct reports.
- Provide direction and guidance to SOC specialists and help them to resolve more challenging issues.
- Ensure rota management is actioned in line with BBC terms and conditions and SOC policies, and manage the resolution of rota conflicts between shifts.
- Ensure SOC investigation quality management procedures are adhered to, and improved over time, to ensure consistent and competent investigation of incidents.
- Develop / review such SOC policies, standards and procedures as are necessary for the efficient operation of the department.

Threat Intelligence and Vulnerability Identification

- Working with Forensics, ensure the timely delivery of threat intelligence information, to relevant teams. Review, and provide feedback on, SOC intelligence outputs to ensure SOC guidance on threat response is appropriate.
- Oversee the vulnerability management and responsible disclosure triage processes within the SOC, working to improve their effectiveness and efficiency over time. Support the timely resolution of any critical issues identified via effective use of influencing skills with business stakeholders.

External Liaison

- Represent the department at internal meetings and present on behalf of the BBC at external conferences, “giving back” to the wider Information Security community by presenting on relevant topics where the BBC SOC has developed expertise.
- Take a lead role on managing the relationships with SOC suppliers, overseeing contract reviews and proof of value assessments.

Approval	
Manager	Andrew Sands
HR Business Partner	Kate Horton