Security Assurance Manager

Basic information

Band: C
Job family: Technical
Terms: Permanent
Location: Cheltenham

Reports to: Service Assurance Manager
Team: Service Assurance
Business unit: Technology

Role purpose:

The Security Assurance Manager supports the Service Assurance function in implementing the IT security vision, model and principles across all of UCAS, **ensuring compliance with ISO 27001, PCI DSS**, **DPA 1998,** and other appropriate industry standards, to support the organisational strategy. The Security Assurance Manager works with the Technology department to guide the selection and deployment of technical controls to meet specific security requirements, and defines processes and standards to ensure that security configurations are maintained.

Key duties and responsibilities:

Support the Head of Technology Service Management, Service delivery managers, Security Architect and Information Security Manager with the following:

- To complete information security operations documentation.
- To develop strategies and plans to enforce security requirements, and address identified risks.
- To proactively develop and improve the Security Operations Centre, in partnership with our outsource provider.
- To report to management concerns about residual risk, vulnerabilities, and other security exposures, including misuse of information assets and non-compliance.
- To assess security requirements and controls, and ensure that security controls are implemented as planned during application development or acquisition.

- To collaborate on critical IT projects to ensure that security issues are addressed throughout the project life cycle.
- To identify, select, and implement technical controls.
- To develop security processes and procedures, and support service-level agreements (SLAs) to ensure that security controls are managed and maintained.
- To advise security administrators on normal and exception-based processing of security authorisation requests.
- To research, evaluate, and recommend information security-related hardware and software, including developing business cases for security investments.
- To develop a common set of security tools. Define operational parameters for their use, and conduct reviews of tool output.
- To perform control and vulnerability assessments to identify control weaknesses, and assess the effectiveness of existing controls, and recommends remedial action.
- To define testing criteria for systems and applications.
- To perform risk assessments and analyse the result of audits (performed by other groups) to produce recommendations of acceptable risk and risk mitigation strategies.
- To develop and validate baseline security configurations for operating systems, applications, and networking and telecommunications equipment.
- To provide support and analysis during and after a security incident, as necessary.
- To assist the resolution of reported security incidents.
- To participate in security investigations and compliance reviews.
- To assure monitoring of daily or weekly reports, and security logs for unusual events, is being done effectively and efficiently.
- To assist in the development of security architecture and security policies, principles, and standards.
- To research and assess new threats and security alerts, and recommend remedial actions.

Accountabilities:

Primary customers and stakeholders
Internal:

- Other internal IT functions
- All non-IT business units
- Corporate Governance and Performance Team
- Outsource provider

External:

- Core IT Partner (CITP)
- Crisis management teams for HEPs
- Awarding bodies
- External auditors, Customer Experience and Marketing, UCAS Media, and Technology and Operations

Person specification:

- Certified Information Systems Security Professional (CISSP) and/or Certified Information Security Manager (CISM) preferred, or demonstrated technical capability at this level.
- IT security management or analysis experience mandatory.
- ISO 27001 experience and qualification highly desired.
- PCI DSS experience mandatory.
- Understanding of security monitoring and testing processes such as vulnerability scanning, penetration testing, SIEM, IDS.
- Experience working with Cloud, Big Data and Open Data architectures.
- Knowledge of third party security assurance highly desired.

This role profile sets out the scope and main duties of the post at the date when it was drawn up. Such details may vary from time to time without changing the general character of the post or the level of responsibility entailed. Such variations are a common occurrence and cannot of themselves justify a reconsideration of the level of the post. All UCAS employees are expected to be flexible in undertaking the duties and responsibilities attached to their role and may be asked to perform other duties, which reasonably correspond to the general character of their role and their level of responsibility.

Our values in action

Customer – We always look through the customer lens. The logic of the customer is the logic of UCAS.
Commitment – When we commit, we deliver on time, quality, and budget, or we negotiate changed commitments for good reason. We never leave commitments uncovered.

Team – We work collaboratively. When we commit, we commit as an individual and as a team. We strive for and support team success as well as individual success.

Outcomes – We plan and do things to achieve outcomes. We define them, aspire to them, and deliver them.

Agility – We know we need to be agile when we look through the customer lens, when we make commitments, when we work in teams, and strive for the right outcomes.

Extraordinary – We are ambitious for our customers, for UCAS, and for our teams. We want more than ordinary outcomes – we strive to achieve extraordinary outcomes, extraordinary customer focus, and an extraordinary culture of high performance and quality of focus.