JOB DESCRIPTION

Job Title:	Information Security and Compliance Analyst	**Grade:**	SG7
Department:	Office of the CIO / Information and Library Services (ILS)	**Date of Job Evaluation:**	July 2023
Role reports to:	Head of Information Security and Compliance		
Direct Reports	None		
This role profile is non-contractual and provided for guidance. It will be updated and amended from time to time in accordance with the changing needs of the University and the requirements of the job.			

PURPOSE OF ROLE:

The Information Security & Compliance Analyst is a vital role that will contribute to the effective and efficient execution of the University's information security governance, risk and compliance programme.

The post sits within the Information Security and Compliance team and will offer a blend of both internal audit activity and involvement in other key information security initiatives.

This role will involve planning and undertaking internal audits against relevant standards, managing remediation of gaps and nonconformities, and preparing relevant audit documentation and reports.

This role will help to foster a positive “security by design” culture, ensuring our users are able to work from anywhere, at any time, safely and in compliance with relevant policies and regulations.

KEY ACCOUNTABILITIES:

Team Specific:

- Be an active member and positive contributor within the department and wider ILS directorate.
- Ensure compliance of high-quality processes in relation to all aspects of work, with a high level of quality assurance and professionalism throughout.
- Liaise with key stakeholders to ensure IT systems and associated processes are fit for purpose and meet the needs of the University.
- Contribute to the delivery of systems and services which are high quality, resilient and secure and meet the core business needs of the University and the aspirations of the Strategic Plan.
- Contribute to the generation of the monthly information security report including key KPIs and security metrics.
- Act as the first point of contact for information security and compliance related queries, escalating to management where necessary.

- Work closely with colleagues from the wider directorate to ensure we are developing and maintaining a high performance, secure and fully resilient infrastructure, whilst protecting the confidentiality, integrity and availability of our information, systems and people.

Generic:

- Maintain an up-to-date knowledge of new developments in information security and the general technology landscape, particularly in relation to its application within a Higher Education context. This includes developments to industry best practices, emerging threats, and regulatory changes.
- From time to time, participate in specific projects not directly related to the main functions of the post.
- Engage in professional development opportunities to keep skills relevant.
- Work closely and collaboratively as required with the Head of Information Security and Compliance, Head of Cyber Security, Head of IT Support, Project Managers, and other senior ILS colleagues.
- Carry out other duties as may from time to time be reasonably required across the service.

Managing Self:

- Assist in the maintenance and continuous improvement of existing security certifications within the teams remit such as ISO27001 and Cyber Essentials (CE).
- Coordinate and perform audit-related activities, in particular ISO27001 internal audits, to assess the effectiveness of the Information Security Management System (ISMS) and to identify areas for improvement.
- Monitor and evaluate compliance with ISO27001 requirements and recommend corrective actions as needed.
- Assist with audit related activities relating to other certifications outside of the team's immediate remit, such as ISO20000-1.
- Manage remediation of gaps and nonconformities identified through the internal audit process, as well as through third-party audits.
- Assist with the coordination of external auditors during ISO27001 certification audits and maintain necessary documentation for compliance.
- Establish and maintain effective relationships with relevant control owners and advise them on audit and compliance activities.
- Ensure manager is kept informed and consulted on key activities.
- Support the development, implementation and maintenance of policies, procedures and controls to ensure the security and integrity of information assets.
- Assist with compliance processes relating to new systems/services, such as third-party/vendor risk assessments and security reviews.
- Assist with the planning and delivery of the University's information security awareness programme including mandatory infosec training, annual simulated phishing campaigns and targeted training for specific user groups.
- Liaise closely with all staff to share and develop best practice and contribute to staff training and development activities.

- Participate in and contribute to relevant external and internal professional, service and University groups.
- Be proactive in promoting the image of the department and directorate within the University, the wider higher education community and the national and international user communities associated with technical and functional use of our corporate systems.
- Proactively and through the application of independent initiative, research industry information to assess suitability of, and advise on the most appropriate information security technologies and processes for use within the University.
- Develop and exhibit excellent organisational, planning and time management skills.
- Display logical thinking with creative problem-solving ability.
- Provide attention to detail.
- Demonstrate excellent communication and negotiation skills.
- Demonstrate good IT skills and willingness to develop them further.

Core Requirements:

- Adhere to and promote the University's policies on Equality, Diversity and Inclusion and Information Security.
- Ensure compliance with Health & Safety and Data Protection Legislation.
- Support and promote the university's Sustainability policies, including the Carbon Management Plan, and carry out duties in a resource efficient way, recognising the shared responsibility of minimising the university's negative environmental impacts wherever possible.
- Adhere to current legal requirements and best practice relating to digital content and accessibility, including Web Content Accessibility Guidelines when creating digital content.

Additional Requirements:

- The post holder will have access to a range of sensitive and key University systems and information. It is therefore essential that they demonstrate a high level of professional integrity and discretion and comply with the University's Policies in relation to Information Assurance and Security.
- They will be expected to use initiative and problem-solving skills and to be able to identify and deliver solutions to requirements.
- The post is critical to the efficient and effective functioning of the University's information system facilities, possessing high levels of responsibility for providing assurance of IT systems and services within the University.
- Attendance at some University committees and informal meetings will be required.
- Travelling between and working at different campuses will be required.
- Undertake any other duties as requested by the line manager or appropriate senior manager, commensurate with the grade.
- This is a professional, demanding role within a complex organisation with an ambitious strategic plan and agenda for change. The role holder will be expected to show flexibility in working arrangements, including working hours, to ensure that the directorate delivers the required level of service.

KEY PERFORMANCE INDICATORS:

Effective execution of the job description, in part measured by;

- Minimal or zero security breaches.
- Reduction in CSIRT notifications from Janet.
- Time taken to respond to security incidents.
- Internal audit outcomes in relation to information security which indicate substantial assurance.
- High system uptime, minimal un-planned outages (target 99.5% or greater).
- Effective monitoring of and analysis of security performance indicators and improvement programmes.
- Progressively improving culture and awareness of information assurance and security throughout the University
- Improvement of existing compliance processes

KEY RELATIONSHIPS (Internal & External):

- Head of Information Security and Compliance
- Associate Director, Office of the CIO
- Head of Cyber Security
- Team and Department Colleagues
- University Senior Management and key University Groups and Committees as required
- University staff within Faculty and Directorate offices, particularly ILS
- Software and managed service suppliers
- University, Partner, Network and Collaborative Centre staff and student
- Colleagues across the sector in related fields
- Relevant sector networks such as JISC, HEFCE, Janet, KPSN, GOETEC
- Partner Universities via the Medway shared service

PERSON SPECIFICATION	
Essential	**Desirable**
Experience • Experience working within IT or Information Security ideally related to server, storage, cloud, and network technologies. • Familiarity with ISO/IEC 27001/Cyber Essentials, relevant good practice, and legislation in relation to information assurance and security. • Understanding and experience of IT audit and review. • Understanding of information security principles, best practices, and emerging threats. • Experience of developing and delivering relevant training and communications programmes. • Experience with Information Security training and awareness tools	**Experience** • Cyber Security incident response experience including post incident reviews, root cause analysis and reporting. • Understanding of technology infrastructures using Firewalls, VPN, Data Loss Prevention, IDS/IPS, Web-Proxy.
Skills • A team member able to work collaboratively but also able to take the initiative, show judgement and lead by example. • Excellent communication skills, both written and verbal, with the ability to convey complex information to technical and non-technical stakeholders. • Ability to contribute to continuous service and process improvement.	**Skills** • N/A
Qualifications • Educated to degree level or equivalent demonstrable experiential learning within a relevant technical, educational management or business discipline.	**Qualifications** • Postgraduate or professional qualification in a relevant technical or management discipline. • ISO/IEC 27001 Lead Auditor and/or Lead Implementer • ITIL certification.

	• Membership of a relevant professional organisation. • CISSP / CISM or similar professional certification. • Clean UK Driving Licence.
Personal attributes • We are looking for people who can help us deliver the values of the University of Greenwich: Inclusive, Collaborative and Impactful	**Personal attributes** • N/A