Post Details			Last Updated: 05/09/24
Faculty/Administrative/Service Department	IT Services		
Job Title	Cyber Risk and Assurance Manager		
Job Family	Professional Services	**Job Level**	6
Responsible to	Head of Cyber Risk and Assurance		
Responsible for (Staff)	n/a		

Job Purpose Statement

The Cyber Risk and Assurance Manager is a senior risk professional within IT Services, who will lead on diverse information security assurance activities, working with other cyber security specialists, technical teams and colleagues across the organisation to overlay good practice and security controls in support of business activities. Using your business acumen, you will apply appropriate risk analysis principles to support the University mission.

Key Responsibilities

- Working with the Head of Information Security to develop the University's security and compliance frameworks, maintaining and developing accreditation for IT Services' service catalogue
- Managing the PCI-DSS certification process, supporting all faculties / departments to ensure that their payment solutions are compliant
- Managing the annual certification activities associated with NHS DSP Toolkit
- Managing the annual certification activities associated with Cyber Essentials+
- Lead on assessment of all new regulatory or accreditation requirements as they arise
- Operate and continuously improve risk assessment processes in support of new service design
- As a senior risk professional within Cyber Security, you will operate and continuously improve the cyber risk registers and management information, supporting the successful communication of business risk within the institutional risk framework and University committee structure
- Maintain and develop governance and compliance documentation.
- Provide product ownership for GRC platform(s) and associated relevant tools
- Act in the interests of the University reviewing security clauses in new contracts, advising the business and embedding security by design. Developing and implementing new processes to manage and deliver this workload.
- Leading on information security due diligence processes with key suppliers, developing and maturing existing processes and delivering integration with IT Services pipeline processes as appropriate.
- Developing and maintaining a RACI matrix, or other mechanism as appropriate, to ensure that Information Security Roles and responsibilities are defined as appropriate across the University and in more detail within IT Services.
- Supporting assurance activities in respect of the Cyber Security portfolio working alongside colleagues in specialisms including Internal Audit and Information Governance.
- Supporting academic security attestations related to research funding and data sharing
- Acting as liaison with the data privacy team to dovetail with ongoing GDPR compliance and other information governance activity.
- Assisting the Cyber Security team in delivering the security awareness programmes across the University
- Deputising on behalf of the Head of Cyber Risk and Assurance as required

N.B. The above list is not exhaustive.

All staff are expected to:

- Positively support equality of opportunity and equity of treatment to colleagues and students in accordance with the University of Surrey Equal Opportunities Policy.
- Work to achieve the aims of our Environmental Policy and promote awareness to colleagues and students.
- Follow University/departmental policies and working practices in ensuring that no breaches of information security result from their actions.
- Ensure they are aware of and abide by all relevant University Regulations and Policies relevant to the role.
- Undertake such other duties within the scope of the post as may be requested by your Manager.
- Work supportively with colleagues, operating in a collegiate manner at all times.

Help maintain a safe working environment by:

- Attending training in Health and Safety requirements as necessary, both on appointment and as changes in duties and techniques demand.
- Following local codes of safe working practices and the University of Surrey Health and Safety Policy.

Elements of the Role

Planning and Organising

- The post holder has a wide remit as the Cyber Risk and Assurance Manager and will therefore be expected to plan the use of their time appropriately to match demand, planning to deliver both short-term and long-term activities and projects
- The post-holder is responsible for developing and implementing review processes and frameworks, which will inform the delivery of both their work activities and that of colleagues requiring advice and guidance on information security
- The post-holder will act as a visible and approachable point of liaison for colleagues across the University and will work closely with the Information Governance Team around GDPR compliance. They will therefore be expected to balance demands for their time, while providing an informed, professional service to colleagues
- The role will involve delivery of accreditation reviews that will require advanced planning and a full understanding of resource requirements from IT services and other business units, in order to deliver outcomes to the appropriate standard and to deadlines
- As a specialist in reviewing security contractual agreements, the post-holder is fully responsible for ensuring the delivery of feedback on contract clauses within timescales associated with services going live

Problem-Solving and Decision-Making

- The post-holder will work within, and further develop a framework of processes and policies, and is expected to take a proactive approach to problem-solving. The role has delegated authority to resolve problems using sound judgement and experience. The post-holder will also work alongside colleagues to improve and develop security frameworks and the supporting policy catalogue
- The post-holder will operate within established legal and University frameworks, policies and procedures to ensure that decisions, advice and guidance provided to colleagues and external third parties, are consistent for managing corporate information security risk
- Appropriate and timely decision-making has the potential to influence the successful completion of strategic projects, or impact operations for all staff and students at the University. Timely escalation is therefore expected where the impact of a decision is significant or where it is clear that a significant security threat or incident is present

Continuous Improvement

- The post-holder is expected to maintain their knowledge of security and regulatory frameworks and laws impacting on the delivery of services, to ensure the advice they provide is up-to-date and accurate.
- The post-holder will bring to the attention of the Head of Cyber Risk and Assurance any proposed improvements to the security protocols and procedures identified as part of their reviews and accreditation processes.
- The post-holder will be expected to draw upon the knowledge, skills and expertise of information security colleagues to develop their own knowledge and skills while discharging in the role
- Recommendations for major process and service improvements are encouraged

Accountability

- The post-holder has a high level of autonomy and is expected to act a specialist advisory and key point of contact on information security regulation for the University
- The post-holder is expected to produce accurate and timely reports on behalf of the Cyber Security Leadership team

Dimensions of the role

- The post-holder is expected to provide input into information/cyber security protocols and policies, ensuring that these are relevant and up-to-date
- The post-holder will be expected to monitor regulatory changes and take appropriate, informed action to ensure that the University remains aligned in all key areas
- While the post-holder does not have any direct line management responsibilities, they are expected to matrix-manage colleagues in compliance activities to ensure effective and timely outcomes.
- The scope of the role is University-wide, but resides within the IT Services directorate. The purpose of the role is to provide a focal point for information security assurance, providing guidance and support to colleagues outside of IT Services and matrix management for colleagues within IT Services as appropriate. The role holder must be able to succinctly define, justify and articulate what is appropriate for the maintenance of a proportionate and effective information security culture in support of organisational mission

Supplementary Information

- N/A

Person Specification

Qualifications and Professional Memberships	
Professionally qualified with a relevant degree/postgraduate qualification, plus several years' broad management experience in similar or related roles OR; Substantial vocational and relevant management experience demonstrating management ability in an appropriate professional or specialist area, and success in similar or related roles, supported by evidence of significant appropriate specialist knowledge	E

Technical Competencies (Experience and Knowledge)	**Essential/ Desirable**	**Level 1-3**
Appropriate IT Security certifications (such as one or more of: CISSP, CISA, CISM, CRISC etc.)	E	3
Experience of working with external parties in relation to their specific information security assurance requirements, such as NHS England (NHS DSP Toolkit); ONS (ONS Secure Research Service)	D	2
Experience of administering vendor risk management processes, and prior experience of risk assessment	D	2
Experience of developing workflows in support of information governance and information security assurance; particularly any service development involving GRC processes and tooling (such as OneTrust)	D	2

Special Requirements:	**Essential/ Desirable**
The post holder must be willing and able to work flexibly. This may include working outside of regular office hours upon occasion where incidents arise.	E

Core Competencies	**Level 1-3**
Communication	3
Adaptability / Flexibility	2
Customer/Client service and support	3
Planning and Organising	3
Continuous Improvement	3
Problem Solving and Decision-making Skills	3
Managing and Developing Performance	2
Creative and Analytical Thinking	3
Influencing, Persuasion and Negotiation Skills	3

Strategic Thinking & Leadership	2

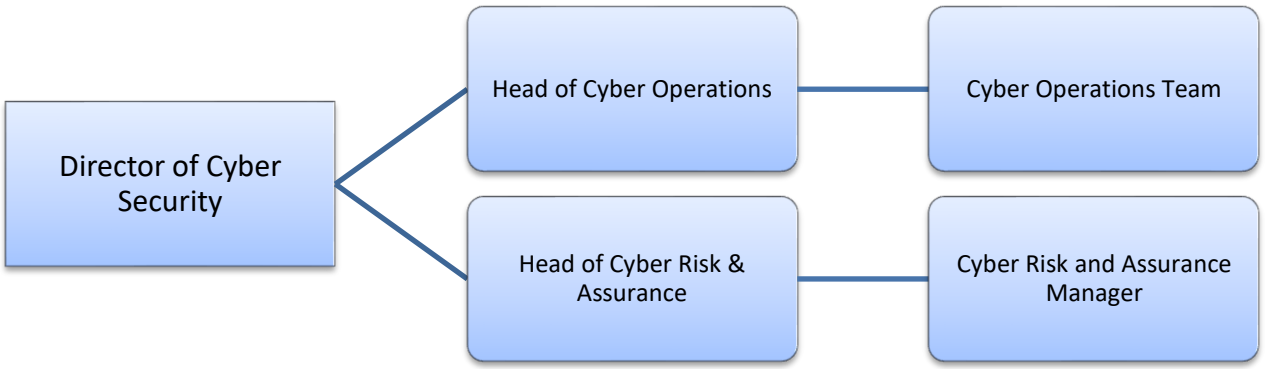
Organisational/Departmental Information & Key Relationships

Background Information

With an operating budget of ca. £10M and complement of approx. 100 staff, the University IT Services department provides a wide range of administrative and academic computing and information services for all staff and students at the University. IT underpins both the operational heartbeat of the University and enables strategic developments. The University Strategic Objectives are:

1. Driving the Student Experience
2. Focusing Research Intensity
3. Creating the Conditions for Success
4. Engaged and Connected

Team Structure Chart



Relationships

Internal

- All IT Services colleagues, especially Contracts / Procurement, Project and Programme Leads
- Staff and students across the University, and in particular the Information Governance team
- Project managers, project sponsors and senior stakeholders across the University

External

- External suppliers and third-party consultants
- Information/cyber security colleagues in other Higher Education institutions and organisations of similar sizes