Job Description:
Senior Information Security Compliance Officer

Function:	TDDI Manager
Job:	Sodexo Information Security GRC
Position:	Senior Information Security Compliance Officer
Job holder:	
Date (in job since):	N/A
Immediate manager (N+1 Job title and name):	Head of Security Governance, Risk & Compliance
Additional reporting line to:	N/A
Position location:	Homeworker

1. Purpose of the Job – State concisely the aim of the job.

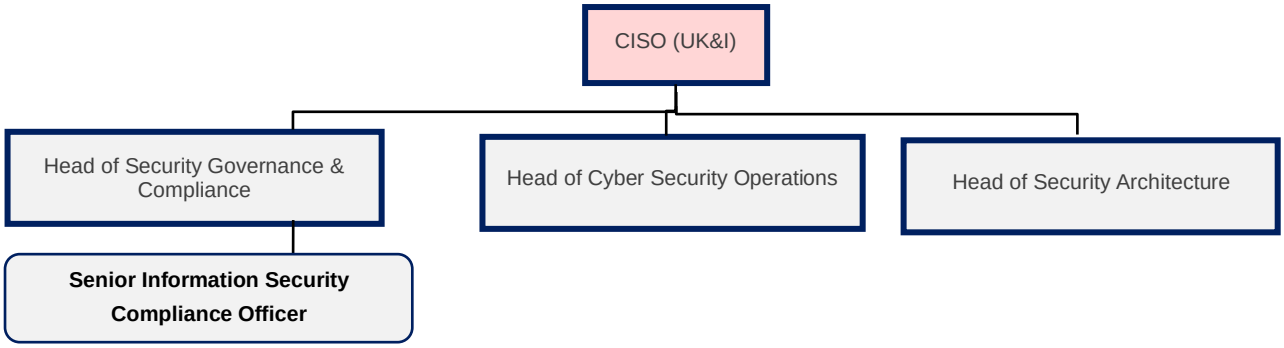
- Accountable for managing IT and Security risk process and associated mitigation and control management.
- Accountable for managing Sodexo's Information Security Management System (ISMS) to maintain ISO27001 certification
- Accountable for managing the delivery of Information Security Compliance activities to maintain Sodexo's compliance with Cyber Essentials +
- Accountable for managing the delivery of ISO22301 and the coordination of IT Business continuity and IT Disaster recovery requirements
- Support the delivery of Information Security compliance activities in the UK & Ireland to support Sodexo's PCI DSS programme
- Responsible for managing Information Security Third Party Assurance on Sodexo suppliers to mitigate Risk throughout the lifecycle of supplier relationships
- Responsible for enabling the Legal teams to ensure appropriate Information Security clauses are in contracts

2. Dimensions – Point out the main figures / indicators to give some insight on the "volumes" managed by the position and/or the activity of the Department.

Characteristics

- Complex Compliance & Regulatory Landscape
- Complex Client Requirements
- 100+ Third Party Suppliers
- 100+ systems

3. Organisation chart – Indicate schematically the position of the job within the organisation. It is sufficient to indicate one hierarchical level above (including possible functional boss) and, if applicable, one below the position. In the horizontal direction, the other jobs reporting to the same superior should be indicated. Please show the job titles not the actual people doing the role, i.e. Finance Manager, Project Manager



4. Context and main issues – Describe the most difficult types of problems the jobholder has to face (internal or external to Sodexo) and/or the regulations, guidelines, practices that are to be adhered to.

- Deliver technical compliance audits across a complex technology landscape, manage and communicate re-mediation activities and coordinate compliance programme
- Influence stakeholders to develop timely and appropriate action plans and to mitigate risk to within appetite t
- Maintain the UK & Ireland ISMS, whilst expanding the scope of ISO27001 coverage
- Deliver CE+ whilst expanding the scope and coordination of remediation activities

5. Main assignments – Indicate the main activities / duties to be conducted in the job.

- Build an annual consolidated Information Security Compliance Programme that provides the business, IT of visibility of internal and external Audit & Assurance activity to allow appropriate demand & resource planning
- Deliver effective Security Compliance reporting to inform Risk & Issue reporting to the CISO, IT & Business Senior Leadership
- Ensure Audit & Assurance actions are managed, tracked, and reported through to mitigation

ISO27001

- Ensure the ISMS is managed and maintained in alignment with the Statement of Applicability and ISO27001/2 framework
- Define requirements for the ISMS, document and implement security policies to develop and maintain the ISMS
- Manage and maintain the ISMS documentation
- Conduct and supervise Sodexo UK and Ireland regular audits and review the implemented controls covered by the ISMS scope to align to the business need
- Develop a plan to scale up ISO27001 practices to a wider scope to improve overall security maturity
- Explore opportunities for consolidation of ISMS where practical and appropriate
- **ISO22301** Maintain ISO22301 compliance and coordinate annual testing requirements
- Build and maintain IT business continuity and the disaster recovery plan aligned to business needs
- Ensure annual recovery testing coordination of IT environment and revise requirements for critical recovery strategy aligns with business requirements

Cyber Essentials +

- Build and maintain a CE+ compliance framework that provides prioritised and targeted assurance activities
- Support CE+ compliance efforts in performing and/or coordinating targeted CE+ compliance monitoring across applicable segments and related Sodexo infrastructure
- Work with internal and external stakeholders to deliver CE+ certifications and recertifications

Information Security Third Party Assurance

- Manage and maintain questionnaires within the Third Party Risk Management platform used by internal and external stakeholders, enhancing the product and supporting processes where applicable.
- Conduct risk-based information security due diligence activities against vendors to provide appropriate levels of assurance to key stakeholders
- Enhance Information Security Third Party Assurance processes and engagement activities across IS&T, transversal functions and the wider business

PCI DSS

- Support the delivery of PCI DSS compliance programme to provide direction and assurance of operational controls and meet Sodexo's compliance requirements
- Support PCI-DSS compliance efforts in performing and/or coordinating information security audits across payment channels / business segments
- Coordinate and support the PCI-DSS Audit Activity to ensure delivery of the ROC and the AOC

6. Accountabilities – Give the 3 to 5 key outputs of the position vis-à-vis the organization; they should focus on end results, not duties or activities.

- Ensure Risk management processes are followed and support TDDI through the UK&I Risk Framework
- Ensure ISO27001 certification is maintained to comply with contract and client requirements
- Ensure ISO22301certification is obtained and maintained with compliance requirements
- Ensure CE+ certification is obtained and maintained to comply with contract and client requirements
- Develop, track and report audit actions through to remediation to improve security compliance controls and reduce information security risk
- Identify Third Party Supplier Risk and deliver reporting to the CISO, TDDI team and business stakeholders

7. Person Specification – Indicate the skills, knowledge and experience that the job holder should require to conduct the role effectively

- 6+ years of experience in Information Security and related fields
- Expert knowledge and practical experience of ISO27001 certification requirements and ISMS documentation
- Expert knowledge and practical experience of Cyber Essentials + certification requirements
- Experience of leading and performing internal or external IT audits
- Experience of dealing with third party supplier audits
- Experience of negotiating with stakeholders in designing relevant action plans
- Experience of comprehensive IT internal audit program design and development
- General knowledge of IT environments and technologies
- General Knowledge of Security Architecture or Enterprise Architecture
- Desirable Certifications: CISA, CRISC, QSA, ISO27001 LI, ISO27001 LA.
- Ability to communicate effectively to a wide range of people from various horizons, both written and verbally
- Analytical and problem-solving capabilities
- Strong minded
- Rigorous and organised
- Ability to gain Government Security Clearance

8. Competencies – Indicate which of the Sodexo core competencies and any professional competencies that the role requires

▪ Business consulting
▪ Rigorous management of results
▪ Innovation and Change
▪ Learning & Development

9. Management approval

Version	2.2	**Date**	06 January 2025
Document Owner	Chief Information Security Officer (UK&I)		