

Job Description:   
Head of Information Security Governance, Risk & Compliance

|  |  |  |  |
| --- | --- | --- | --- |
| Function: | | IS&T | |
| Job: | | [Enter generic job title] Refer to Invent Position Title Guidance | |
| Position: | | Head of Information Security Governance, Risk & Compliance | |
| Job holder: | | Vacant | |
| Date (in job since): | |  | |
| Immediate manager  (N+1 Job title and name): | | Steve Moran - CISO UK&I | |
| Additional reporting line to: | |  | |
| Position location: | | Home based | |
|  | | |
| 1. Purpose of the Job – State concisely the aim of the job. | | | |
| * Lead the Information Security Governance, Risk and Compliance domain within UK&I IS&T * Establish, monitor, evaluate, report in a professional manner; clearly highlighting the current state of IT and Information & Cyber Security Risks to the Executive committee * Manage the Information Risk Assessment Methodology and associated governance * Lead Sodexo’s professional response to internal and external audits and reviews * Lead the Continuous improvement of the IT control environment * Lead IT Business Continuity and IT Disaster Recovery processes and governance * Lead the develop Sodexo’s Security Compliance requirements (CE +, ISO27001, PCI-DSS, NHS DSPT) * Provide input, and direction, to the Cyber Security strategy * Research and study advancements in educational technologies and threat horizons * Drive cultural change to ensure that IT security is a key consideration for new systems and processes | | | |
|  | | |
| 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 | * Oversee the security governance, risk and control function:   + ~200 projects/security risk assessments/year   + >1,000 suppliers   + ~30 internal controls   + 3 Cyber Essential scopes   + 6 ISO 27001 scopes * Manage a team of 4 expert Information Security Compliance Officers and 1 x IT Risk Analyst * Manage a budget of £500k | | |

|  |
| --- |
| 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. |
| CISO (UK&I)  Head of Cyber Security Operations  Head of Security Architecture  Head of Governance, Risk & Compliance  Security Compliance Officers x 4  IT Risk Analyst x 1 |

Draft. Version: 27-03-2014

|  |
| --- |
| **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 external IT audits, validating and coordinating timely responses to clients and regulators * Influence stakeholders to develop timely and appropriate action plans to mitigate risk and issues * Analyse data and adapt quickly to context * Lead a team with a wide range of expertise * Set up adequate and consistent processes and frameworks across the organisation |

|  |
| --- |
| 5. Main assignments – Indicate the main activities / duties to be conducted in the job. |
| * Lead and drive the evolution of the Governance, Risk and Compliance domain   + Anticipate and identify new people, process and technology needs for the development of the domain   + Contribute to business cases as needed with the support of the CISO’s strategy and roadmap   + Contribute to the IS&T and Information & Cyber Security strategy by providing an accurate view of IT risk and controls   + Establish budget, forecast, and track expenses for the Governance, Risk and Compliance domain   + Advise the CISO and IS&T leadership on future investments   + Build relevant KPIs & dashboards for regular review with CISO, IS&T leadership and regional exec as part of the standard governance reporting framework   + Develop, manage, and communicate all relevant IT and Information & Cybersecurity policies, standards, and processes to maintain Governance Framework   + Develop and maintain a process for horizon scanning to keep up with emerging regulatory changes, threats and technology in the Security Governance, Risk and Compliance domain   + Develop and manage a schedule of a Compliance that meets Sodexo’s regulatory and client contractual requirements   + Manage resource allocation and capacity planning of the team   + Develop and maintain the reputation of the domain as a viable business partner * Support the Governance of the IT and Information & Cyber Security   + Work with the business development, sales and operational teams as appropriate on required client due diligence; help design a more effective process including a self-service process and a library of standard responses   + Manage the Information Security Management System (ISMS) and propose strategies to expand the scope, whilst consolidating certification to reduce compliance overhead, whilst maintaining the ISO27001 certifications   + Maintain and develop the easy-to-use tools and processes to engage with Information & Cyber Security activity; and ensure there are communicated effectively to business stakeholders   + Coordinate CISO and IT leadership reporting to support exec / global risk governance reporting (including the InfoSec SteerCo) * Implement, maintain, and develop the IT and Information & Cyber Security Risk management programme   + Ensure risks are documented, assessed, managed, and tracked in line with Sodexo’s risk appetite   + Ensure risks are surfaced to management and stakeholders when appropriate for formal acceptance   + Ensure appropriate expertise is provided to the CISO and IT leadership in achieving implementation of effective risk management   + Drive the evolution of the various frameworks, procedures, processes, and directives dictating Sodexo risk posture * Implement, maintain, and develop the IT Control management programme   + Ensure internal controls effectiveness are tested and make recommendations to management for improvements to match Sodexo risk appetite   + Direct the work of the team to ensure IT controls are systematically and consistently evaluated, and integrated across the project lifecycle * Implement, maintain, and develop the IT Compliance management programme   + Supervise the definition of the annual internal audit schedule and scoping in conjunction with the Security, Governance, Architecture & Compliance function   + Maintain all Risk, Control, and Business Continuity/Disaster Recovery aspects to ensure we remain compliant with relevant legal and regulatory requirements * Implement, maintain, and develop the IT Business Continuity & Disaster Recovery programme   + Manage the IT Business Continuity Plan and associated IT activities (e.g., Disaster Recovery Plan)   + Ensure adequate testing is completed of plans and any remedial action is documented and tracked |

|  |
| --- |
| 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 the IT and Information & Cyber Security risk posture is accurately established and ensure periodic testing of controls effectiveness to inform exec governance reporting * Ensure regulatory compliance with all relevant IT and Information & Cyber Security standards and frameworks in line with contractual requirements * Ensure appropriate regulatory compliance horizon scanning is in place to inform the IT and Information & Cyber Security strategies and mitigate any issues with client contractual requirements * Ensure processes and tools for engaging with Risk & Compliance activity are in place, communicated and known to business and IS&T stakeholders * Ensure process alignment with the Business Continuity and Enterprise Risk Management functions * Manage budget and spend in line with the annual business plan and the IT & Cyber Security roadmap |

|  |
| --- |
| 7. Person Specification – Indicate the skills, knowledge and experience that the job holder should require to conduct the role effectively |
| * Graduate calibre * Experience of people management * Extensive experience in leading Risk Management * Expert understanding of IT and Information & Cyber Risk and business impact * Proven ability to implement key Information Security and Compliance programmes * Excellent Governance, Risk and Compliance skill set * Effective utilisation, and management, of external suppliers * Effective team leadership and coaching skills * Experience in financial forecasts, budget, and business planning * Proficiency in core information security principles (access control, network security, vulnerability management, etc.) * General knowledge of IT environments and technologies, and data privacy * Expert knowledge of security standards / frameworks (NIST, Cyber Essentials, ISO2700, PCI DSS, etc.) * Diplomatic with the ability to interact successfully with all levels of the business * Ability to work in a matrixed organisation and under own initiative * Ability to translate security requirements and standards into easily understood business concepts versa * Versatile and ability to adapt quickly to changing contexts * Rigorous and organised * Strong-will minded * Analytical and problem-solving capabilities * Knowledge of IT auditing |

|  |
| --- |
| 8. Competencies – Indicate which of the Sodexo core competencies and any professional competencies that the role requires |
| |  | | --- | | * Rigorous management of results | | * Brand Notoriety | | * Commercial Awareness | | * Learning & Development | | * Leadership & People Management | | * Innovation and Change | |

|  |
| --- |
| 9. Management Approval – To be completed by document owner |
| |  |  |  |  | | --- | --- | --- | --- | | Version | 1.1 | Date | 16 October 2023 | | Document Owner | CISO UK&I | | | |