JOB DESCRIPTION

Function:	IS&T
Position:	**SENIOR INFORMATION ASSURANCE MANAGER**
Job holder:	
Date (in job since):	
Immediate manager (N+1 Job title and name):	CIO
Additional reporting line to:	
Position location:	Salford

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

To be responsible for the management of Information Assurance with regard to the business objectives set out by Sodexo UK and ROI; providing data management leadership, advice, support and guidance to all levels of the organisation.

To ensure through proactive and reactive tasks, that information security risks to the business are mitigated, and where possible reduced by continual improvement of the Sodexo UK and ROI Information Security Management System.

To liase with external bodies to ensure Sodexo maintains compliance with:

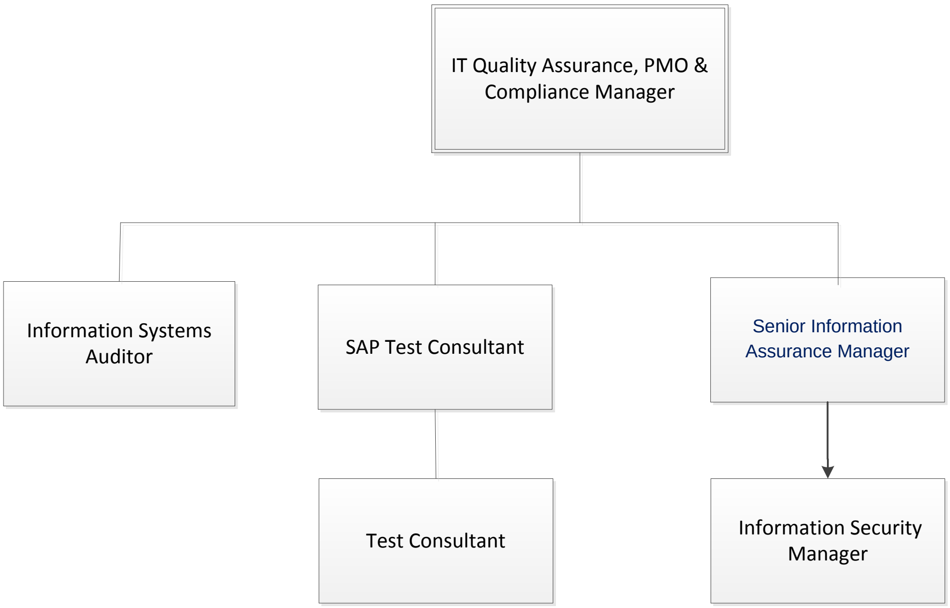
- Information Security requirements of ISO 27001, PCI-DSS and Cyber Essentials
- Information Security requirements of HMG client at upto Official Sensitive
- Relevant legislation and practises such as the Data Protection Act, Freedom of Information Act, Regulation of Investigatory Powers Act

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.

Revenue FY13:	€tbc	EBIT growth:	tbc	Growth type:	n/a	Outsourcing rate:	n/a	Region Workforce	tbc
		EBIT margin:	tbc						
		Net income growth:	tbc			Outsourcing growth rate:	n/a	HR in Region	tbc
		Cash conversion:	tbc						
Characteristics		▪ Financial - No responsibility for budget ▪ Staff - One direct report ▪ Scope covers IS&T for UK&ROI							

STOP HUNGER
A Sodexo Initiative

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


IT Quality Assurance, PMO & Compliance Manager
Information Systems Auditor
SAP Test Consultant
Senior Information Assurance Manager
Test Consultant
Information Security 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.

- Drive the Information Assurance programme for activities at up to IL3/Official Sensitive for HMG clients
- Work directly with senior management and external bodies to grow a culture of quality, prevention, protection and compliance that is driven by effective leadership and accountability; Develop and manage the Information Security Working Group and associated ISMS Forums.
- Drive and manage the InfoSec team and programmes dynamically
- Support multiple project engagements providing estimation, planning and tracking of security requirements.
- Ensure security requirements are established, documented and met by external suppliers.
- Be a recognised subject matter expert for ISO27001 and PCI-DSS Accreditation
- Support ITT / PQQ and contract bid opportunities through customer facing engagement and the completion of security questionnaires.
- Expected to comply with the Company's Policies and supporting documentation in respect of Data Protection, Information Security and Confidentiality

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

- Develop, implement and maintain information security policies, standards, guidelines and procedures, ensuring on-going achievement of information security objectives based on Industry best practice.
- Develop, implement and maintain Information Assurance Accreditations in line with business strategy, global standards and policies, and the requirements of audit bodies and Clients (including National Security Standards, HMG Security Policy Framework (SPF) and Defence Manual of Security (JSP440) etc).
- Create security documentation in accordance with appropriate standards (e.g. JSP440, HMG National Security Standards and guidelines (HMG IAS1-2, etc.), SPF, ISO 27001) including Technical Risk Assessment, RMADS, SyOps and Codes of Connection.
- Deliver legislative update training programmes and raise awareness of information assurance, using a variety of communication methods
- Support the definition, delivery and management of the ICT Business Continuity Management System to ISO 22301 and the requirements of the Corporate BCMS.

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.

- Role holder uses strong stakeholder management and communication skills to work effectively with IS&T and Business team members to ensure that all employees have a good awareness of information security that is relevant to their role and the Information Security Policy is aligned to business objectives and strategy.
- Information security risks are identified in a timely manner and managed according to the Information Security risk management process within the ISMS Manual.
- Information security considerations are a key part of all IT projects / initiatives; appropriate information security requirements are identified and implemented as necessary.
- Information security incidents are reported and managed according to the Information Security Incident Management Policy.
- ISO27001 certification and Accreditations are achieved and maintained for the agreed scope.

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

- Role holder is regarded as an Information Security Subject Matter Expert and acts as a champion for information security best practice; they are able to sensitively articulate the link between information security, risk management and tangible business advantage, in uncluttered language.
- CESG Certified Professional (CCP) in one or more role at practitioner level
- Qualified to one of : CISSP; CISM; and / or CLAS membership
- Excellent communication & influencing skills; able to demonstrate successful engagement with HMG Accreditors
- Customer-focused, acting as an ambassador with all security stakeholders and able to engage with internal and external clients, in both the public and private sector.
- Ability to work to work collaboratively, as well as develop, coach and mentor other colleagues and team members

- Ability to act as Lead to a number of resources providing Information Assurance capability into a project/programme
- Understanding/expertise of : ISO27001; ISO22301; PCI-DSS
- Knowledge and understanding of the characteristics, vulnerabilities and risks relating to IT infrastructure (operating systems, applications, web applications, IT networks, wireless LAN, firewalls, switches, routers etc) and the relevant mitigating controls (encryption, protective monitoring , anti-malware etc).
- Eligible to live and work in the UK and either possess or be able to obtain UK Security Clearance to SC level or equivalent level as defined by HMG.
- Candidates must already have a UK/European Union passport and the right to work in the UK without restrictions/sponsorship.

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

Growth, Client & Customer Satisfaction / Quality of Services provided	Leadership & People Management
Rigorous management of results	Innovation and Change
Employee Engagement	Business Consulting
Learning and Development	

9. Management Approval – To be completed by document owner

Version	1.1	Date	3rd Sept 2016
Document Owner	M. Mitchelson		