JOB SUMMARY

Post Title	*Information Security Officer*						
Job Family	*Business Support*	**Pay Range**	*10*	**Line Manager to others?**	No	**Role profile ref**	*BS10*
Service Area	*Information Security*						
Line Manager	*Information Security Manager (Deputy-SIRO)*						
Location	*County Hall, High Street, Newport, Isle of Wight, PO30 1UD / Agile*						

Job Purpose

The Information Security Officer (ISO) is responsible for providing assistance with the provision of specialist advice and guidance to support the effective delivery of the Cyber Security Strategy and the wider Information security agenda across the council. Including; completing research, consulting on and recommend improvements and changes to ensure the protection of all data held within the organisation and related third parties. This extends to all physical and electronic data including client and staff information.

The post holder will support the Information Security Manager on ensuring the council maintain systems to relevant standards within the Public Services Network (PSN), Cyber Assessment Framework (CAF), Data Security and Protection Toolkit (DSPT) and Payment Card Industry Data Security Standards (PCI DSS). or other related compliance regimes relating to information security and be responsible for the council's conformance with ISO 27001.

Job Context - (key outputs of team / role to provide some specific examples of role profile accountabilities)

- Contribute proactively in providing an effective support for senior managers and stakeholders with identification, prioritisation and development of key Cyber Security and Information Security risks and risk mitigation activities.
- Contribute proactively in providing an effective support for senior managers and stakeholders with identification, prioritisation, and development of Cyber Security Projects to meet the Cyber Security Strategy goals and that will bring significant benefit to the council.
- Assist in providing an effective support to the strategic leadership team, senior managers, Councillors, and other key stakeholders who provide services based on sensitive information, with advice and examples of best practice, compliance, and innovation.
- Provide specialist advice and support to colleagues, customers and stakeholders. Advise on Information Security risks and risk mitigation activities as required.
- Work pro-actively to with council wide services such as Legal Services and Comms to build strong relationships with senior managers improving Cyber Security practices and facilitating cultural change by identifying opportunities to streamline, improve and adapt existing and future Cyber Security and Information Security processes and systems functionality.
- Assist in providing an effective support to the Information Security Manager who is the specialist for the council. As and when required; undertaking research, coaching, training and guidance to services and content contributors that maintains compliance

with statutory obligations.

- Challenge customers' practice where appropriate and support them to develop / improve services, processes and best practice in order to minimise risk, referring concerns to line manager.
- To assist in delivering the Cyber Security Strategy Programme Board and activities to achieve the Cyber Security Strategy ambitions. Supporting the work of the Information Security Team by working in partnership with the Corporate Information Unit (CIU) team ensuring that Information Security is integrated into the corporate agenda.
- Assist in providing reports to the Internal Information Governance Group (IIGG) and CSSPB senior members of management (e.g. a Director, SIRO / Information Asset Owners (IAO's) or equivalent) who has responsibility for Information Governance.
- Assist in providing regular information security risk assurance reports to the Senior Information Risk Owner (SIRO) and, CSSPB, Corporate Management Team and Councillors when required.
- Work in partnership with all the ICT teams ensure Information Security is integrated into the ICT work programme.

Knowledge, Skills and Experience

Role Profile requirements.	**Job specific examples.** (if left blank refer to left hand column)	**Essential**	**Desirable**
Relevant experience within the service area / profession, with evidence of appropriate specialist knowledge.	*Relevant experience of working in an ICT service area / profession, with evidence of specialist knowledge of all of or a combination of the below:*		
	Relevant experience in strategy review, management risk reviews, and policy review.		*D*
	Understands the importance of digital accessibility and can demonstrate previous experience.		*D*
	Strong operational awareness of Cyber Security and Information Security policy, process and systems delivery.	*E*	
	Experience of working in an ICT service area / profession, with evidence of detailed specialist knowledge of Information Security systems, policies, regulations, professional guidelines and legislation. *e.g. ITIL, ISO 27001, Public Secure Network (PSN), Cyber Assessment Framework (CAF), Data Security and Protection Toolkit (DSPT) and Payment Card Industry Data Security*	*E*	

	Standards (PCI DSS).		
Good knowledge of other areas of the authority relevant to the service.	*Information Security impacts every area of the IWC, a good understanding of the departments within a Unitary authority and the information systems required.* *Knowledge in Information security systems design that meet requirements for PSN, CAF, DSPT, PCI DSS, ISO 27001 and ITIL.* *Knowledge in Information security systems governance processes for ensuring continued approval for PSN, CAF, DSPT and PCI DSS.* *Knowledge in Information security systems procedures and ability to create professional level guidelines and training materials for areas of expertise.*	E E	 D D
Authoritative knowledge of the specialist work practices, systems, policies, procedures and professional guidelines relevant to the work area.	*Defining potential projects and proposing future strategic direction for areas of Information Security that specialisms are in.*	**E**	
Excellent communication and interpersonal skills with the ability to engage effectively with a range of audiences and explain specialist information in a way which a non-specialist can understand. Proven ability to build relationships and engage successfully with the stakeholder community.	*Experience of supplier liaison including issue resolution.* *Experience of Stakeholder liaison including business area managers and users.* *Experience of end user training and knowledge transfer.* *Experience of working as part of an Information Security, Cyber Security, Risk Management or Information Governance team.*	 E E	D D
Good literacy, numeracy and report writing skills. High level of technical expertise in analysis, data manipulation.	*Experience of supplier liaison including quotes for work required and arranging for orders to be raised.* *Experience of maintaining comprehensive up-to-date and accurate details of all systems and services within the remit of the post including knowledge items relating to fixes for known issues.*	E E	

	Able to ensure that high standards of data quality are maintained using a variety of tools. *Experience of carrying out data analysis, cleansing data to address anomalies found, and amending data pro-actively, with the agreement of or at the request of business managers.* *Able to demonstrate the ability to undertake logical analysis and investigation of customer information security risks and recommend potential solutions. Escalate complex issues as appropriate.*	E E E	
Good planning and organisational skills, with proven ability to prioritise and co-ordinate workloads, monitor and evaluate work, to ensure standards, outcomes and deadlines are achieved.	*Working on multiple projects within your workload, balancing this with many incidents, problems and events. Ability to appropriately prioritise your own workloads between them.* *Able to demonstrate the ability to undertake logical analysis and investigation of customer information security risks and recommend potential solutions. Escalate complex issues as appropriate.*	E E	
Excellent ICT skills - including use of Microsoft applications and specialist systems which support procedures and record keeping.	*Strong working experience of all or a combination of the below:* *Office 365 Pro Plus, Microsoft Teams, UTM security systems, E-Mail filtering, Web filtering, security system monitoring, Firewalls and perimeter Security Systems.*	**E**	
Experience of contributing to project delivery as part of a team.	*Working on projects in an Information Security environment; demonstrating an understanding of project management.* *Demonstrate an understanding of PRINCE2 project management principles.* *Understanding of the ITIL Framework*	**E** **E**	**D**
Qualifications			
Role Profile requirements.	**Job specific examples.** (if left blank refer to left hand column)	**Essential**	**Desirable**
Educated to level 4 up to first degree standard or equivalent		E	

experience in a relevant subject.			
Relevant professional / vocational qualification.	*Certified Information Systems Security Professional (CISSP)*	E	
	ISO 27001 Information Security Management Standard		D
	PRINCE 2 Foundation or equivalent experience	E	
	ITIL Foundation		D

Other Requirements
Deliver the provision of “Emergency Services Provision Cover”, to provide a twenty four–hour, seven days per week cover to participate in a Cyber Incident Response Team (CIRT). The post holder will attend to all emergencies as necessary and liaise with suppliers as required or deal with personally. The on-call allowance payable for the provision of these services shall include the taking of all telephone calls, and taking the appropriate actions. To liaise appropriately with the relevant customer and keep all records of call-outs received and actions taken.
Maybe required to undertake additional duties as commensurate with the role and grade.
Highly self-motivated
Good interpersonal and communication skills
Willing to challenge existing practices
Organisation Structure

Strategic Manager for ICT and Digital Services (SIRO)

Information Security Manager (Deputy-SIRO)

Information Security Officer (This role)