



ROLE PROFILE

Role Profile			
Job Title	Information Security Manager		
Section	Cyber and Data Protection	Department	Infrastructure and Operations
Reports to (Job Title)	Head of I & O with a dotted reporting line to CEO		
Location	Post will be based in Plymouth but can also work on a regular basis from home.		

Job Purpose	<p>Leads the information security function that enables Delt and our clients to safely and securely, do amazing things by assisting in the development and implementation of a strategic information security strategy and roadmap that goes beyond a 'compliance only' view and becomes a business differentiator.</p>
Key Competencies and Output	<p>Works with our customers to develop their information security strategies and roadmaps, helping ensure they can deliver not only compliance against sector specific infosec requirements but aspire to become best in class.</p> <p>Owns operational risk management for the company ensuring a consistent application of the process and effectiveness. Ensures appropriate operational risks are reported in a timely manner to the senior leadership team.</p> <p>Identifies, evaluates and reports on information security risks, practices and projects to the Senior Leadership Team and provides subject matter expertise on security standards and best practices.</p> <p>To ensure that appropriate relationships are fostered and developed with internal services and external partners, and that the IT security function works in collaboration with all areas.</p> <p>Engages with our clients at multiple levels to provide assurance in the security of the Delt offering.</p> <p>Sets the direction and priorities for the information security staff and develops, mentors and manages their performance to ensure key objectives are met.</p> <p>Leads the development of information security policies, procedures, standards and guidelines, and oversees their approval, dissemination, and most importantly, maintenance.</p> <p>To regularly review the effectiveness of the IT Security Management Service performance, in line with agreed SLAs, KPIs, and KRIs.</p> <p>To ensure that the corporate risks for the IT Security Management Service are identified, managed and mitigated.</p> <p>Ensures that the Delt security management program is in compliance with applicable laws, regulations, and contractual requirements including: DPA, GDPR, GPSOC, PSN PCI DSS and DSP Toolkit.</p> <p>Manages the annual Cyber Essentials+ submission to ensure ongoing certification.</p> <p>Performs the role of Data Protection Officer (DPO) with specific focus on:</p> <ul style="list-style-type: none"> Informing and advising the organisation and its employees about our obligations to comply with the GDPR, Data Protection Act and related data laws

	<ul style="list-style-type: none"> • Monitoring compliance with Data Protection law and related organisational policies, including managing internal data protection activities such as raising awareness of data protection issues; training staff; conducting internal audits; advising on and monitoring Data Protection Impact Assessments (DPIAs); ensuring the Record of Processing Activities (ROPA) and Privacy Notices are accurate and maintained • Cooperating with the supervisory authority; and being the first point of contact for supervisory authorities and for individuals whose data is processed by Delt. <p>Oversees the evaluation, selection and implementation of information security solutions that are innovative, cost-effective, and minimally disruptive.</p> <p>Manages regular intrusion detection and vulnerability reporting, internal and external IT audit groups reviews, and the coordination of resolving discovered issues.</p> <p>Monitors the industry and external environment for emerging threats and advises relevant stakeholders on appropriate courses of action.</p> <p>Owens Delt's business continuity and disaster recovery planning, ensuring that Delt can continue supporting its customers as seamlessly as possible following any business interruption event. Provides advice to customers on technical elements of business continuity planning.</p> <p>Provides advice to the organisation on IT security (including managing physical), technical aspects of information governance and IT risk management.</p> <p>Develops commercial cyber security consultancy offerings (potentially including partnerships with other suppliers) to enable Delt to share its expertise in the cyber arena.</p> <p>To ensure that all staff have the necessary information security and risk management training appropriate for their role.</p> <p>To promote excellent IT Security practice throughout Delt.</p> <p>The accountabilities listed here are not an exhaustive list. The post holder will be required to work in any area of the business and deliver ad-hoc duties as and when directed.</p>
<p>Experience, Knowledge, Skills and Qualifications</p>	<p>An experienced senior leader in IT with a proven track record of managing people and risks.</p> <p>Knowledge of business management, information security risk management, data protection and cybersecurity technologies including common information security management frameworks, such as ISO/IEC 27001, ITIL, COBIT.</p> <p>Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate information security and risk-related concepts to both technical and nontechnical audiences.</p> <p>A proven track record and experience in developing policies and procedures, as well as successfully executing programs that meet the objectives of excellence in a dynamic business environment.</p> <p>A passionate leader and builder of both vision and bridges, able to energize and motivate not just our information security team but both the wider Delt workforce and those of our clients.</p> <p>Excellent analytical and project management skills with the ability to manage multiple projects under firm timelines, as well as the ability to work well in a demanding, dynamic environment.</p> <p>A professional security management certification is desirable, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) or other similar credentials.</p> <p>Excellent stakeholder, contract and vendor negotiations skills.</p>

Corporate Standards	<p>In accordance with Delt's organisational policies and guidance on information management and security, it is the personal responsibility of all employees to ensure data protection, client confidentiality and appropriate information governance.</p> <p>All employees must always act in accordance with appropriate legislation and regulations, codes of practice and Delt's policies and procedures.</p> <p>All employees must work with the requirements of our Health and Safety policy, ensuring safe systems of work and procedures.</p> <p>Undertake all duties regarding the Delt equalities policy and relevant legislation.</p> <p>In a 'people first' environment, the post holder must both be aligned and aspire to Delt's values and expected standards of behaviour for them and their team(s).</p>
----------------------------	---