|  |
| --- |
| Information Security Manager - Corporation |
| Information Security Team |
| Risk & Compliance Directorate |

Organisational overview

Nest is a great government delivery success story. Established in 2010, Nest has been a critical pillar of the government’s automatic enrolment programme, with a public service obligation (PSO) to accept any employer wishing to use the scheme to discharge their automatic enrolment duties.

From a standing start, we have delivered a high quality, low cost pension scheme, open to all, which has not only delivered on its mission, but helped to drive up standards and best practice across the industry. Now with over 6 million members, Nest is playing a critical role in helping people save for their retirement many of them low to moderate earners who may be saving for the first time and moving jobs frequently.

Nest now occupies a place in the market as a major Master Trust, a sector that has grown following the introduction of automatic enrolment and that we believe has great potential for delivering pensions to mass market consumers for many years to come, leveraging scale to offer low cost, modernised services in the context of strong Trustee governance.

To best serve our diverse customer base, it’s important that Nest has an equally diverse workforce and
promotes an inclusive culture. This is in line with the organisation’s values and ensures that Nest is a corporation fit for the future.

Nest’s purpose is ‘Building financial peace of mind for all’ and has embarked upon a refreshed corporate strategy to be the best-in-class pension provider delivering the best possible financial outcomes for our members to and through retirement.

Departmental overview

The Risk and Compliance vision is to become a trusted partner for the business. To enable this, the directorate teams’ shared objective is to enable the first line to deliver business objectives in line with agreed risk appetites.

The Information Security team functions as part of the second line of defence in the Risk and Compliance directorate.

It is accountable for the development, implementation and on-going maintenance of the ISMS (Information Security Management System) processes across Nest Corporation and the Scheme Arrangement outsourced providers in alignment with ISO27001.

The Information Security Manager – Corporation reports into the Head of Information Security and is responsible for ensuring that Nest’s Information Security Management System is operated for the Corporation, enabling the first line business teams to deliver business objectives in line with the agreed risk appetite. This role will work across all internal Nest departments, programmes, projects and initiatives, providing oversight, support and challenge.

Scope and deliverables

|  |  |
| --- | --- |
| Key areas | Role deliverables |
| Accountability | The role is accountable for maintaining and improving Nest Corporation’s ISMS through performing ISMS processes including:* Maintaining stakeholder support and buy in of all Nest Corporation 1st line of defence (1LoD) teams including HR, IT, Procurement, Finance, Investment, Facilities, Project Management Office etc.
* Produce corporation reporting based upon relevant metrics and risk indicators.
* Performing incident response for corporation ISMS incidents
* Providing subject matter expert oversight and challenge to 1LoD teams (IT) in processing 3rd party supplier incidents.
* Continually improve the ISMS, Nest’s security policy suite and technical standards.
* Review 3rd party technical security test reports and translate identified vulnerabilities into clearly articulated business risks for non-technical senior management.
* Perform risk assessment of information assets, systems, projects and change affecting the corporation.
* Represent Nest at third party security and service management forums, supporting 1LoD teams in the management of outsourced suppliers.
* Periodically test Information Security controls such as performing phishing tests, clear desk sweeps etc.
* Provide information security expertise to Nest service management teams, programmes, projects and initiatives to ensure they incorporate information security requirements and controls into their processes, analysis and deliverables
* Mentor junior members of the team
* Be required to provide occasional cover for other Information Security team members
 |
| Deliverables | * Maintain an ISO27001 certified ISMS.
* Continually improve the ISMS based on the agreed cyber maturity plan.
* Conduct risk assessments and ISMS based reporting
 |
| Relationships and autonomy | * Interact regularly with all members of Nest delivering and managing Information Security controls for the corporation (including Procurement, HR, IT, Finance, Commercial and delivery etc.) to maintain the quality, effectiveness and alignment of information security controls with business objectives in line with agreed risk appetite.
* Interact with various levels of staff within Nest to communicate changes to policies and requirements
 |

Role requirements

Experience and technical skills

The role holder should be able to demonstrate:

* Practical experience of operating certified ISMS using ISO 27001/2, NIST CSF and other security standards in the design and management of information security controls.
* Practical experience working with third party suppliers to audit and evidence compliance with security policies, standards etc.
* Understanding and experience of various Information Security domains including Security Architecture, Information Security Governance, Network Security, Data Protection, Risk Management, Identity & Access Management, Vulnerability Management, Anti-Malware, Mobile Device Management and Cloud Security
* Experience of working within the Financial Services, whilst beneficial, is not essential

Personal attributes required

The Information Security Manager - Corporation will be able to demonstrate:

* Teamworking skills, capable of collaborating with technical and non-technical senior management, Nest Information Security team members, members of other teams in the organisation and various dynamic resourcing options (e.g. contractors and consultants) when necessary
* Multitasking skills, capable of managing multiple tasks/projects in pursuit of the development and maintenance of the ISMS.
* Communication skills, capable of explaining complex information security requirements using clear and unambiguous language with business audiences, alongside demonstrating influencing and negotiation skills
* Core Risk and Compliance behaviours of being Business focussed, Risk based, Customer centric, Aligned and Collaborative, and Team player
* People-management skills; capable of coaching and mentoring junior team members

**Education, qualification and professional membership requirements**

* The candidate must have appropriate security certifications such as CISSP, CISA, CISM and ISO 27001 Auditor/Implementor certification (or significant recent progress towards such certifications)
* The candidate may be educated to degree level or equivalent (ideally in a security or computing related discipline)

Differentiators

* This role sits at the heart of Nest, helping the functions across the organisation implement information security processes from the outset within their projects and key initiatives. The role offers a unique opportunity to shape the future of an organisation facing unprecedented challenges and for the right candidate, huge rewards.
* This role is about integrating Information Security standards across Nest and its supply chain and will give ample opportunity to innovate and integrate with teams across this dynamic organisation

Grade Descriptor

**2T**: Works to achieve operational targets with significant impact on the results of the Function. Works independently with limited supervision