

|  |
| --- |
| Information Security Operations Analyst |
| Corporate IT |
|  |
| **Grade:** TBC |

# Departmental/Directorate overview

|  |
| --- |
|  |
| The **Central Change and Corporate IT** department reports to the Director of Central Change and Technology. It is one of several teams overseen by the Chief Technology and Operations Officer (CTOO). We are a team of about 25 colleagues and our aim is to ensure the smooth running and implementation of Nest technology and change.  The **IT Team** of 11 colleagues in 2 functional teams exists to:   * Set IT strategy and architecture in order to ensure that we all have the IT tools to do our jobs. * Make sure that we have an infrastructure that is fit for the future.   The **IT Service Operations Team** in which this role sits is responsible for:   * Overseeing the relationship with our outsourced IT service provider and other suppliers. * Introducing new services. * Ensuring value for members’ money * First line security.   The **Business Applications and Solutions** section of the IT Team supports the organisation to:   * Better organise and manage its files and other data. * Manage and automate its processes with the deployment and configuration of effective applications and solutions, including development of low and no-code solutions and with AI. * Help select, onboard and administer various 3rd party applications such as CRM and Finance systems. |

# The role

|  |
| --- |
|  |
|  |
| This is a new role for nest and will report to the Senior IT Service Operations Manager.  Nest operates a three lines of defence approach to information security with the second and third lines delivered by an internal information security team and external auditors respectively. This role covers the first line of defence, of which a large part is outsourced.  Currently management of the 3rd party contract provisions related to security, together with various internal control responsibilities are covered by other members of the team for whom this is not a specialism. This role will take on those responsibilities, bringing more specialist experience and knowledge. You will help to develop and improve our information security controls as we seek to improve our infosec maturity using the NIST framework as an externally assessed benchmark.  This first line role combines a contract management aspect with the requirement for hands-on process operation for internally managed controls such as access reviews, and some investigations such as subject access requests or insider threats.  This role will support the ‘cyber security’ theme within the Corporate Technology IT Strategy 2030 |

# Scope and deliverables

## Accountability

|  |
| --- |
|  |
|  |
| Responsible for :  Ensuring that the security related contractual obligations of the 3rd party are met to nest’s satisfaction and management are kept appraised of any non-conformance and progress of plans to rectify.  Ensuring that all the security controls operated by the IT team and its partners are fit for purpose and operating as designed, kept up to date and evidencable.  Ensuring new and existing processes are developed and maintained as fit for purpose.  Ensuring that Subject Access Request searches and audit evidence requests and Freedom of Information requests related to IT are executed correctly and on time.  Ensuring that new SaaS or installed applications and new infrastructure implementations have had adequate security assessments and any risks identified, mitigated and accepted. |

## Deliverables

|  |
| --- |
|  |
|  |
| * Provide advice based on your operational security expertise to IT Management and Compliance colleagues. * Oversee contractual requirements related to information security, ensuring they are met and continue to be fit for our organisational standards and requirements. * Represent the organisation in risk and security working groups, * Own the information security risk documentation associated with IT and the mitigating controls. * Advise on the adequacy and effectiveness of IT controls operated by our 3rd parties * Develop new controls, processes and policies as required to improve security maturity at nest. * Monitor and track amendments and updates to security controls, facilitating compliance with information security and data protection standards. * Manage the process for information requests, including subject access requests, ensuring they meet organisational and legal standards. * Facilitate evidence gathering for controls for all internal and external audit requirements including ISO27001 and AAF 05/20. * Oversee the cyber incident response planning and execution, ensuring readiness for major cyber incidents. * Liaise with third-party suppliers to ensure their services meet the organisation's security standards, including those not directly managed by the first line of defence. * Facilitate investigations as required by information security, legal, compliance, financial crime and HR teams. * Deliver cyber incident reporting to senior stakeholders, working with the scheme teams and second line to ensure these reports are consistent. |

## Relationships and autonomy

|  |
| --- |
|  |
|  |
| This role will regularly interact with the IT Service Operations and Business Apps teams, the Information Security and Enterprise risk teams, will be a key attendee of the security working group and liaise with the outsourced IT Service providers Cyber Security Operations Centre (CSOC). Regular contact with external auditors can also be expected. |

# Role requirements

## Experience and technical skills

|  |
| --- |
|  |
|  |
| * Experience in IT security. * Experience of security controls around data warehouses\analytics functions would be an advantage. * Understanding of contract management and service level agreements in the context of information security. * Experience in risk management, with the ability to identify, document and manage risks, and their control and mitigation. * Knowledge of compliance, information security, and data protection standards. * Ability to operate and oversee processes and controls related to information security in an externally audited environment such as ISO27001, FCA or TPR regulation, * Experience in cyber incident investigation, response planning and execution. * A working knowledge of Information security related tooling, preferably in a Microsoft cloud environment – for example Purview and Defender, DLP, Insider Risk, Audit log searches, eDiscovery tools and SIEM solutions, vulnerability management, * Strong communication skills, with the ability to represent the organization in various working groups and liaise with third-party suppliers, information security specialists and auditors. * Strong collaboration skills, with the ability to work closely with both internal and external stakeholders on shared goals. |

## Personal attributes

|  |
| --- |
|  |
|  |
| The role will require someone with the following personal attributes:   * The ability to effectively engage with a wide range of stakeholders * An ability to distil complex requirements and issues quickly into a form which can be understood and acted upon by others * A strong attention to detail * A strong desire for continuous improvement and keeping ahead of the curve * Ability to make risk based decisions on prioritisation * Qualifications in an operational information security discipline would be an advantage |

## Differentiators

|  |
| --- |
|  |
|  |
| This role is brand new and so suits someone who is looking for a role where they can use their skills and experience to shape the role and its responsibilities over time. It offers a mix of supervisory\governance responsibilities and hands on tasks.  Nest operates a modern public cloud and SaaS based infrastructure and manages the personal data of 13+ million people with £50bn assets under management making this an ideal opportunity to work in an environment with high security concerns and modern up to date systems. Nest is certified to ISO27001 and regulated by the Pensions Regulator and Financial Conduct Authority. As a public corporation it offers a mix of public sector and financial services opportunities and challenges giving a wide experience. |

## Working pattern

|  |
| --- |
|  |
|  |
| Nest operates flexible working and most aspects of this role can be done working from home. Attendance at our Canary Wharf Office for meetings should be expected regularly but not usually more than 2 days a week. |

## Grade Descriptor

|  |
| --- |
|  |
|  |
| 2Technical |

|  |  |
| --- | --- |
| Nest Corporation  10 South Colonnade  Canary Wharf  London, E14 4PZ  [nestpensions.org.uk](https://www.nestpensions.org.uk/schemeweb/nest.html) |  |