IT and Change Risk and Controls Manager

Department:	IT & Change
Report to:	Head of IT Services and Cyber Security
Job Family:	Group Services
Career Family / Job Capsule:	Managerial – Experienced Manager
Key dimensions:	(£Budget, Team headcount FTE, any other relevant P&L metrics as they become available)

Purpose of the role:

The IT and Change Risk and Controls Manager is a first line of defence role reporting into the Head of IT services and Cyber Security.

The purpose of the role is to:

- Ensure OneFamily's operational risk management framework is embedded within the IT and Change function and oversee adherence to the framework and the RCSA process.
- Provide the IT & Change Senior Management Team (SMT) with support and assurance over its risk and control environment.
- Collaborate with IT teams to develop, implement, document and test controls in order to reduce IT risks to an acceptable level.
- Assist in the development and documentation of IT and Change policies, processes, procedures and controls.
- Monitor and evaluate the effectiveness of IT controls and risk mitigation strategies.
- Monitor and evaluate the effectiveness of IT and Change issues management.
- Produce the Risk Management MI required for the IT and Change Risk Committee, Executive Operational Resilience Group and OneFamily's Group Risk Committee.
- Ensure the effective analysis of emerging risks and issues is reported, tracked and managed.
- Act as the departments' point of contact with Internal and External Audit, Compliance and Risk, supervising and supporting the publication of audit reports and the closure of audit actions.

The role holder will own the IT and Change risk and controls registers and issue logs, ensuring agreed mitigating actions are in place across the function and that robust controls are defined, and regular controls testing is taking place.

Key accountabilities: • Chair the monthly IT and Change Risk Committee and prepare reports for executive management committees. • Drive effective implementation & communication of the Group Risk Management Framework, in particular the RCSA across IT & Change. • Work across IT and Change to analyse and understand the departmental risk profile. • Provide technology risk and change risk management consulting to the business and IT operational teams. • Develop and deliver a programme of controls testing within IT & Change and report results to SMT. • Conduct risk assessments of projects, IT systems and technology suppliers and provide guidance on remedial activities. • Proactively manage risks to reduce major incidents, breaches, or examples of non-compliance. • Develop risk management policies standards & processes. • Manage the relationship between IT & Change and Internal and External Audit. • Track internal and external audit actions for IT & Change and drive or escalate as necessary, if mitigating actions are not progressing. • Maintain an adequate level of current knowledge and proficiency in Technology and Change risk management through annual Continuing Professional Education (CPE) credits.	**Skills / Experience / Knowledge:** • Ideal candidate will have a minimum of degree level qualification and relevant further professional qualifications (e.g., CISA, CRISC). • Ideal candidate will have worked in the financial services sector in a technology risk management role. • Displays leadership and independence in performing their role. • Experience of analysing, reporting and managing risk in line with structured business frameworks. • Demonstrable experience in Technology Risk Management. • Strong understanding of IT risk management principles, frameworks, and methodologies, such as ISO 27001, NIST Cybersecurity Framework, or COBIT. • Strong organisational skills and attention to detail with a demonstrated ability to work independently focusing on priorities, and managing a high-volume of tasks, deadlines, requirements, and decisions. • Track record of building effective relationships and matrix influence senior stakeholders and peers. • Excellent interpersonal skills with the ability to successfully engage and influence a broad range of individuals across various internal and external businesses and support functions. • Ability to work under pressure in a dynamic environment. • Ability to conduct own analysis of relevant information in situations that are not always governed by set procedures and frameworks, using judgement and technical knowledge to make decisions on this analysis. • Prince2 or other project management qualification desirable but not essential.
Values	**PRINCIPLED**: We pledge to be and look to you to be: Inclusive, fair, caring, supportive and respectful. **COURAGEOUS**: We pledge to be and look to you to be: Brave, bold, dynamic, determined, and decisive. **EFFECTIVE**: We pledge to be and look to you to be: Smart, commercial, innovative, rigorous and delivery focused.
Adaptability	This job description is intended to provide a broad outline of the main responsibilities only. The post holder is required to be flexible in developing their role in agreement with their Line Manager. In addition, they may be required to carry out any other duties deemed appropriate within the role and expertise.

Performance Management	All employees have a responsibility to participate in regular one to ones with their manager and to identify performance standards of the post. As part of the performance management process every employee is responsible for participating in identifying their own training and development needs to meet the requirements of their role.
Health and Safety	Employees must be aware of the responsibilities placed on them under Health and Safety at Work Act 1974, and take reasonable care for the health and safety of themselves and of other people who may be affected by their acts or omissions at work.
Equality and Diversity	The Society is committed to building an environment where the diversity of its employees is valued, respected and seen as an asset to enabling delivery of the best possible service to our customers and colleagues. It is unlawful to discriminate directly or indirectly in recruitment or employment because of any of the nine 'protected characteristics' contained in the Equality Act 2010. These are age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation. Failure to comply with organisational policies on equality and diversity may result in disciplinary action.
Confidentiality	The unauthorised use or disclosure of customer or other personal information is regarded as gross misconduct and will be subject to disciplinary procedures and could result in a prosecution for an offence or action for civil damages under the General Data Protection Regulations. (GDPR)

Regulatory
(all roles in the organisation must comply with points 1 – 3 and the individual conduct rules – any SIMR/SMCR or role with apportioned responsibilities are required to comply with all four points and both individual and Senior Conduct Rules – Delete when drafting JD) • To comply, at all times, with all regulatory, statutory and legislative requirements so far as they relate to the role • To abide by the Rules of the Society at all times • To understand and comply with all Group Governance Polices, as appropriate to the role • To delivery all apportioned and assigned accountabilities and responsibilities

Individual Conduct Rules	
Rule 1	You must act with integrity
Rule 2	You must act with due skill, care and diligence.
Rule 3	You must be open and cooperative with the FCA, the PRA and other regulators.
Rule 4	You must pay due regard to the interests of customers and treat them fairly.
Rule 5	You must observe proper standards of market conduct.

Senior Conduct Rules	
SC1	You must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively.
SC2	You must take reasonable steps to ensure that the business of the firm for which you are responsible complies with the relevant requirements and standards of the regulatory system.
SC3	You must take reasonable steps to ensure that any delegation of your responsibilities is to an appropriate person and that you oversee the discharge of the delegated responsibility effectively.
SC4	You must disclose appropriately any information of which the FCA or PRA would reasonably expect notice.
SC5	When exercising your responsibilities, you must pay due regard to the interests of current and potential future policyholders in ensuring the provision by the firm of an appropriate degree of protection for their insured benefits.

Declaration	
I hereby confirm that I have read and understood the content of this Job Description and Person Profile and I accept the content as an accurate description of the role which I am required to perform.	
Job holders full name:	
Job holders signature:	
Date:	

Version Control:

Amendment Summary	Date	Reviewer