

Position Description

Senior Manager Operational Resilience

Our Vision

Northern Inland Credit Union (NICU) is committed to helping its Members find smarter ways to manage their money by offering smart financial solutions and building strong, enduring relationships. This shapes products and service delivery and drives the core strategic objective to achieve Main Financial Institution status with Members. By encouraging new Member growth, increasing the value of existing Members and exceeding Member expectations through personalised service and innovative technology, NICU is committed to being the premier local alternative to the big banks in northwestern NSW. NICU seeks team members who are committed to operating in a Member-centric environment.

Job Purpose

The Senior Manager Operational Resilience (SMOR) is responsible for overseeing and managing Northern Inland's operational resilience, information technology and infrastructure, information security, operations, projects and payments systems. The SMOR collaborates with their direct reporting teams to identify and address technology needs, payment innovations, appropriate projects, and operational resilience measures. The SMOR is directly responsible for compliance of policies and procedures and ensures the security, suitability and integrity of Northern Inland's data systems and processes.

Required Smart Values

The SMOR delivers a superior level of service to colleagues, Members and stakeholders via: * **Smart Solutions** * **Motivation** * **Achievement** * **Relationships** * **Team**. Refer to the Employee Handbook on the intranet.

Responsibilities

The primary focus of the SMOR is the implementation of policies, procedures and processes to drive operational resilience and efficiency within Northern Inland. The SMOR works with all departments of the organisation, ensuring that under periods of business as usual, and periods of disruption, Northern Inland continues to provide critical business functions to Members, suppliers, staff and stakeholders. The SMOR is responsible for:

Strategic development and Project Planning

- Developing, reviewing and implementing strategy aligned with Northern Inland's goals and objectives.
- Participating in the development of organisational strategy and implementation within the department, as required.
- Identifying emerging technologies and trends to enhance operational efficiency and effectiveness.
- Assisting with Operational project planning, budgeting and implementation.
- Overseeing and determining timeframes for major IT projects including system updates, upgrades, migrations and outages.
- Collaborating with senior management and executive to establish and implement IT, Operations, Cybersecurity and Payments budgets and priorities.
- Liaising with senior and executive management on the effectiveness of processes, controls, measurements and KPI's.

Team Leadership and Management

- Managing and supervising the IT, Information Security, Operations, Projects and Payments departments.
- Fostering a collaborative and productive work environment, promoting professional development and knowledge sharing between IT, Information Security, Operations, Projects and Payments.
- Delegating tasks and responsibilities effectively, ensuring timely and high-quality delivery of IT, Information Security, Operations, Projects and Payment services.
- Overseeing and measuring the efficiency and effectiveness of the IT Helpdesk function.
- Ensuring the effectiveness of change management processes.
- Actively participate in the Change Advisory Board.
- Overseeing the quality and quantity of workflow delegated to staff within areas of responsibility.
- Managing and assisting in reporting on Northern Inland's operating circumstances, resilience and operational risk rating to the Chief Risk Officer, Risk Management Committee, Executive and Board.
- Preparing clear and concise monthly reports for the Board, attending Board meetings as and when necessary.
- Actively participating in Cybersecurity and Risk Management committee meetings, both at Board and management levels.
- Ensuring processes and procedures are followed in accordance with direction from management.

Position Description

Senior Manager Operational Resilience

IT Infrastructure and Operations

- Overseeing the design, implementation, and maintenance of Northern Inland's IT infrastructure, including core banking services, networks, servers, hardware and software systems.
- Overseeing the implementation of new software, system modules and upgrades.
- Overseeing administration of systems and communications hardware.
- Ensuring the availability, performance and security of all IT systems and applications.
- Developing and implementing IT policies and best practice guides.
- Monitoring and managing IT service levels, addressing infrastructure incidents, problems, and service requests in a timely manner.
- Overseeing automation activities across all departments.

Information Security and Data Protection

- Developing and enforcing IT security policies, procedures, and best practices to safeguard Northern Inland's data and systems.
- Implementing measures to strengthen data security, cyber risk and general IT security.
- Reviewing regular system reports and highlighting irregularities and areas for improvement.
- Taking responsibility for the implementation, education, remediation and development of Northern Inland's overall information security framework in conjunction with the Information Security Officer.

Third-party Supplier Management

- Acting as the contact person for larger suppliers and providers.
- Evaluating, selecting and managing relationships with larger third-party suppliers and service providers (including corporate network, cloud hosting, managed print services and telephone solutions).
- Negotiating contracts and service level agreements, ensuring cost-effectiveness and adherence to quality standards.
- Sourcing alternative third-party suppliers, when required, following third party supplier reviews.
- Monitoring supplier and contractor compliance with Service Level Standards and resolving any issues or disputes that arise.

Regulatory Requirements

- Meeting regulator and auditor requisitions in a timely manner.
- Overseeing CPS230 Operational Risk compliance for Operations, IT, Cybersecurity, Projects and Payments systems.
- Overseeing compliance with CPS234 Information Security mandatory requirements and guidelines, including organising regular security audits and risk assessments.

Refer to the matrix of operational policies and procedures for specific functions, activities and tasks.

Risk Management

Ensures controls are applied in accordance with Board and operational policies and procedures, particularly with regard to material risks, as identified in the Risk Register within the Board-authorized Risk Management Strategy, for which IT & Operations has a detection, monitoring, escalating or risk ownership aspect.

As an owner of material risks, effectively discharge monitoring, management and reporting obligations, including raising awareness amongst NICU stakeholders and proactively identifying and treating future or impending risks.

Position Parameters

- Performs tasks and service requirements with due diligence within the guidelines as set by management
- Actively supports the managerial control and operations of Northern Inland
- Operates in accordance with policies, procedures and deadlines
- Undertakes required training
- Participates in projects and continual improvement and risk management processes
- Provides supportive and meaningful guidance to staff as required
- Other responsibilities and duties within their skills, qualifications and experience.

Position Description

Senior Manager Operational Resilience

Performance Review

Regular reviews against Northern Inland's objectives and values and position's objectives and competencies set by management.

Employment Conditions

Appointed by	CEO
Reports to	CEO
Hours of work	Fulltime: M/W/Th/Fri 8.30am - 5.00pm, Tues 8.15am - 5.00pm, with reasonable additional hours as required and with reasonable notice.
Location	NICU Head Office Tamworth or Newcastle office with reasonable travel to other sites for work related purposes.
Remuneration	Commensurate on qualifications and experience. Superannuation: contributions paid by Northern Inland in accordance with the Superannuation Guarantee scheme.
Leave	In accordance with the Award. Fulltime: 4 NICU Personal Leave Days per calendar year, accruing one per quarter; not cumulative. 1 Personal Leave Day in lieu of Bank Holiday per calendar year; not cumulative.

Inherent and desirable criteria

Essential	Fit & proper: Clear APRA, ASIC and criminal history checks. Eligibility to act as an ASIC Responsible Manager. Eligibility to act as an APRA Responsible Person and to meet requirements for the Financial Accountability Regime. Valid authority to work in Australia.
	General: Presence on site during business hours. Ability to carry up to 5kg over short distances using manual handling aids. Current driver's license.
	Qualifications & Experience: Prior financial services experience. Tertiary qualification in Computer Science, Information Technology, Operational resilience or a related field. Demonstrated experience in a senior management role, with a solid understanding of project management and Information Technology in a banking environment.
	Skills: <ul style="list-style-type: none"> • Proven experience in a managerial or leadership role within an IT or Operational department. • Strong knowledge of IT infrastructure, systems and operational policies and procedures. • Familiarity with information security principles and best practices related to the finance industry in general. • Exceptional problem-solving and decision-making abilities. • Excellent written and verbal communication skills. • Strong organisational and project management skills, with the ability to handle multiple priorities and deadlines.
	Attributes: Professional appearance. Attention to detail. Positive work ethic and demonstrated experience in managing team members to achieve strategic objectives. Solution-driven with a high level of initiative. Ability to multi-task.
Desirable	Cybersecurity qualifications (or currently undertaking).

Effective: 13 January 2025

I have read this Position Description. I agree to comply with its provisions. I am of good fame and character. I am a fit and proper person to carry out my obligations in an honest and fair manner. I am not an undischarged bankrupt. I undertake to advise NICU of any matters which may lead to a conflict of interest arising from my continued appointment. I acknowledge my continued appointment is subject to fit and proper checks, verification of my qualifications, and independent reference checks.

Name: Signature: Date: