

About us...



Lincolnshire Co-op is a long-standing, community-focused organisation proud to serve the people of Lincolnshire and surrounding counties. Our Support Centre, based in Lincoln, is the operational heart of our business. It's home to a range of specialist teams who work behind the scenes to support our front-line colleagues and ensure we deliver exceptional service across all our trading areas.

Essential Information – what you need to know

<p>Job purpose:</p>	<ul style="list-style-type: none"> - Leading the Governance, Risk and Compliance (GRC) of all cyber and technology operations across Lincolnshire Co-op. - Developing and maintaining GRC frameworks that protect colleagues, members, customers and data. - Providing independent assurance on IT and cyber controls, strengthening resilience and confident decision-making.
<p>You'll report to:</p>	<ul style="list-style-type: none"> - Senior Cyber Security Manager
<p>Your hours:</p>	<ul style="list-style-type: none"> - 37.5 hours per week (FTE)
<p>Your relationships:</p>	<ul style="list-style-type: none"> - Senior Cyber Security Manager: aligning cyber risk priorities, reporting on assurance outcomes and improvement plans. - Cyber Operations & IT Infrastructure Teams: reviewing incidents, vulnerabilities and system controls to strengthen resilience. - Technology Leadership Team & ELT/Audit Committee: providing clear updates on cyber risk posture, compliance and mitigation actions. - Trading Area Leads: supporting secure system use, compliance and operational resilience. - External Auditors and Technology Partners: coordinating IT audits, penetration testing and third-party risk assurance.
<p>What you'll bring to us:</p>	<ul style="list-style-type: none"> - Relevant experience in a cyber GRC, IT audit or risk management role is essential. - Knowledge of frameworks and standards such as ISO 27001, NIST CSF or COBIT. - Excellent analytical and problem-solving skills, with attention to detail and accuracy. - Strong interpersonal and communication skills, with the ability to network effectively with stakeholders and translate technical issues into clear business language. - Collaborative mindset, with experience working across IT, Risk and Compliance functions. - Proactive approach to learning and staying current with emerging threats, tools, and best practices. - Strong organisational and time management skills, capable of managing multiple priorities simultaneously. - Certifications such as CISA, CISM, CRISC, CISSP or ISO 27001 Lead Auditor would be advantageous. - A full UK driving licence and access to a vehicle for business use.

Together we are



Providing and supporting
valued services



Helping to grow the
local economy



Caring for our
health and wellbeing



Looking after
our local environment

Your Purpose – I will contribute to my team and the Society’s ongoing success in this role by...

Your duties and responsibilities:

- Developing and maintaining Cyber Security GRC frameworks aligned to business strategy, regulation and industry standards.
- Leading cyber risk identification, assessment and mitigation aligned to the Society ERM framework.
- Maintaining the cyber risk register and producing clear reporting for senior leaders and governance panels.
- Supporting compliance with legislation including data protection, PCI-DSS and sector-specific obligations across Food, Pharmacy, Travel, Funeral and Support Centre operations.
- Strengthening policies, standards and controls across cyber security, IT governance, business continuity and disaster recovery.
- Planning and delivering risk-based IT audits across on-premise and cloud systems.
- Conducting application control reviews for core IT systems supporting all areas of the business.
- Tracking audit findings, monitoring remediation and confirming closure of risks.
- Supporting external audits and providing cyber/IT subject matter expertise.
- Partnering with the Senior Cyber Security Manager and Cyber Operations Manager to align audit and cyber priorities.
- Reviewing security controls including monitoring, incident response and vulnerability management.
- Supporting development of cyber security policies and standards across the Society.
- Providing assurance reporting on cyber risks and remediation progress.
- Acting as a trusted advisor to Technology, Retail, Pharmacy, Funeral and Support Centre colleagues.
- Translating technical risk into clear business-level insight for ELT and governance panels.
- Building strong cross-Society relationships that balance independence with collaboration.

Together we



- Trustworthy – we do what we say we'll do and trust others to deliver to the best of their ability
- Helpful - we support and challenge each other collaboratively, no matter the role or level.
- Respectful - we listen to other views and opinions with consideration and celebrate differences.
- Inspiring - we role model what good looks like and lead by example to be better.
- Valued - we recognise achievements and appreciate everyone's contributions.
- Empowered - we listen and encourage each other to take opportunities.

Your Approach – how you will contribute to your team and the Society's ongoing success in this role.

I will be trustworthy by:

- Delivering clear, accurate cyber risk assurance aligned to Society commitments.
- Acting with integrity when handling sensitive data and security information.
- Following through on audit actions, controls and compliance commitments.
- Using strong analytical judgement to provide honest, evidence-based advice.

I will be helpful by:

- Supporting managers across Food, Pharmacy, Travel and Support Centre to understand cyber risk.
- Working collaboratively across Technology and operational teams, regardless of role or level.
- Challenging constructively to improve controls, resilience and assurance practices.
- Balancing independent audit work with practical, solution-focused guidance.

I will be respectful by:

- Listening to different operational perspectives when assessing risk and controls.
- Treating colleagues and stakeholders fairly during audits and investigations.
- Recognising diverse ways of working across multi-site Lincolnshire Co-op teams.
- Communicating complex cyber issues clearly and considerately.

I will inspire others by:

- Role-modelling strong governance, organisation and high-quality assurance standards.
- Driving continuous improvement in cyber security policies, frameworks and reporting.
- Encouraging a proactive approach to managing technology risk.
- Demonstrating passion for protecting a purpose-driven, community-focused Society.

I will value people by:

- Recognising contributions from colleagues who strengthen cyber resilience.
- Celebrating improvements in compliance, audit outcomes and risk management.
- Supporting colleagues' development through coaching and knowledge-sharing.
- Appreciating cross-team collaboration that protects our members and communities.

I will empower others by:

- Encouraging colleagues to raise risks, concerns and improvement ideas early.
- Working confidently both independently and collaboratively across projects.
- Taking ownership of multiple priorities with proactive organisation and planning.
- Supporting leaders to make confident, informed technology decisions.