



Information Security Management at LINX



Daniel Smith

Cybersecurity Governance and Risk Manager

20th November 2025

LINX125

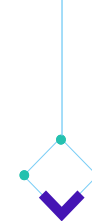







Context and Background

- LINX has traditionally been viewed by the UK Government as “critical national infrastructure”
- We’ve been regulated by Ofcom as an “essential service” under the NIS Regulations since 2018
- We achieved ISO/IEC 27001:2013 certification for the first time in 2021
- We were re-certified and transitioned to ISO/IEC 27001:2022 in 2024





Agenda

-  **ISO 27001 Approach to Information Security Management** 
-  **Implementing Information Security Management at LINX** 
-  **Using Information Security Management to Support Regulatory Compliance** 
-  **Value of Information Security Management** 





ISO 27001 Approach to Information Security Management



Overview of ISO 27001

- ISO 27001 is a governance framework
- It doesn't tell you how to secure things, it tells you how to put processes in place to determine for yourself how to secure things
- The audit asks not just whether controls are in place, but whether you're managing the system behind those controls





ISO 27001 Structure

- The standard is separated into two parts
- The first (main) part consists of 11 clauses (0 to 10)
- The second part, called Annex A, provides the guidelines for 93 control objectives and controls
- Clauses 4 to 10, which provide the ISO 27001 requirements, are mandatory if you want to be compliant with the standard





ISO 27001 Requirements

- 4 • Context of the organisation
- 5 • Leadership
- 6 • Planning
- 7 • Support
- 8 • Operation
- 9 • Performance evaluation
- 10 • Improvement





Information Security Management System (ISMS)

- An ISMS provides a systematic approach to managing an organisation's information security
- It defines the organisation's information assets
- And then it provides the following:
 - Assessment of the risks the information assets face
 - Steps taken to protect the information assets
 - Plan of action in case a security breach happens
 - Identification of individuals responsible for each step of the information security process

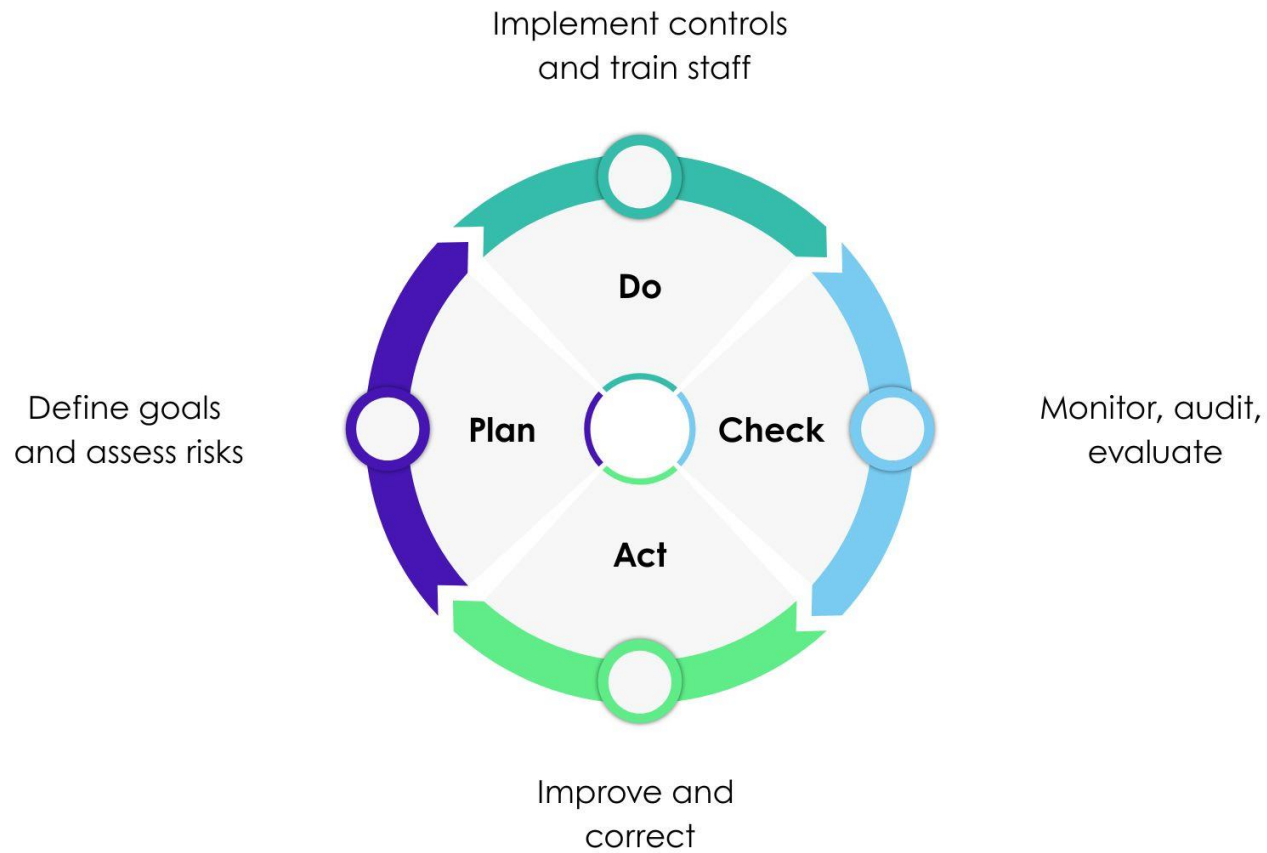




Implementing Information Security Management at LINUX



Plan-Do-Check-Act Cycle





PDCA Cycle: Plan

- Identify business objectives
- Obtain management support
- Select proper implementation scope
- Define Risk Assessment Methodology





PDCA Cycle: Do

- Manage risks through Risk Treatment Plan
- Design policies and procedures as appropriate to manage risks
- Allocate resources and train staff





PDCA Cycle: Check

- Monitor ISMS implementation
- Conduct periodic assessment audits





PDCA Cycle: Act

- Continual improvement
- Corrective action
- Preventative action





Using Information Security Management to Support Regulatory Compliance



NIS Regulations

- LINX is designated as an “essential service” under the NIS Regulations 2018
- This has two main requirements:
 - To take appropriate and proportionate technical and organisational measures to manage risks and ensure the security and service continuity of network and information systems
 - To notify Ofcom of any security incident that has a significant impact on the continuity of the services provided





NIS Assurance Programme

- Ofcom use a formal assurance programme to assess the security of operator's network and information systems on which their essential services rely, and the implementation of relevant security policies
- This is based on compliance with the NCSC's Cyber Assessment Framework (CAF)
- Ofcom gathers information to assess this through formal Legal Notices





Value of Information Security Management



Value of Information Security Management

- It's not about collecting certificates or perfecting paperwork- it's about building an operational core you can trust
- Effective implementation starts with risk: assets get mapped, owned, and tied to actions and reviews
- It helps shift from a "check-the-box" mentality to a culture of continuous monitoring and embedded risk management



Thank you