TRUST

NETWORK AUDIT FRAMEWORK

Strategic Guide

www.trustsystems.co.uk
networks@trustsystems.co.uk

WHY NETWORK AUDITING MATTERS

In today's landscape of constant technological change, the enterprise network is no longer just an operational asset, it's the critical enabler of digital transformation. Whether enabling remote work, supporting IoT, or underpinning hybrid cloud architectures, the network is the digital nervous system of every modern business.

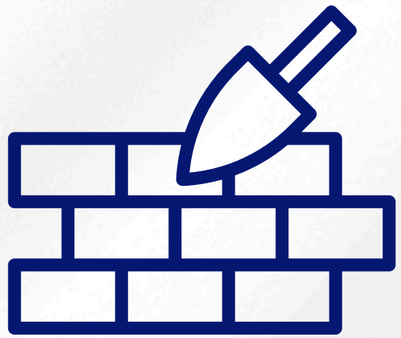
Yet, despite its importance, many organisations operate with blind spots, limited visibility into infrastructure performance, resilience, or risk. A network audit is not merely a technical checklist. It is a strategic initiative designed to evaluate the health of your network, identify vulnerabilities, align IT infrastructure with broader business objectives, and lay the groundwork for secure and scalable innovation.

PHASE ONE

PLANNING & SCOPING SETTING THE STRATEGIC FOUNDATION

Every successful audit begins with a clear purpose. Without defined objectives and scoping, even the most detailed audit can miss the mark. This phase focuses on aligning audit activities with high-level business goals and creating the conditions for a smooth and insightful process.

We begin by working with stakeholders to understand the business's direction. Are you preparing for a cloud migration? Implementing zero-trust architecture? Seeking operational efficiencies? The answers shape how we plan the audit and define its success.



Key activities include:

- **Objective Definition:** Translate business goals into audit criteria.
- **Documentation Review:** Existing network diagrams, asset inventories, and policies are analysed. Missing or outdated documentation often reveals weak spots in governance and visibility.
- **Access and Authorisation:** Defining change windows (especially for out-of-hours access), verifying access credentials, and ensuring compliance frameworks are respected.

A well-scoped audit minimises disruption and maximises strategic relevance.

PHASE TWO

PHYSICAL AUDIT
THE TANGIBLE LAYER OF INFRASTRUCTURE

Although digital transformation is often discussed in virtual terms, the physical reality of network infrastructure has a profound impact on performance, resilience, and scalability. Poor cable management or neglected hardware maintenance can cause real bottlenecks, downtime, and compliance issues.

This phase involves a meticulous on-site review of physical components, with attention to:

- Geographical footprint across sites or branches
- Comms room layout and organisation
- Rack cleanliness and cable management
- Labelling consistency
- Power resilience and cooling
- Fire suppression and environmental controls

Deliverables from this stage typically include:

- A refreshed and validated asset inventory, complete with photographic documentation
- Updated rack and cabling diagrams
- A review of power and connectivity resilience
- Optional integration of third-party testing (e.g., OTDR or Ethernet testing)

The physical audit ensures your infrastructure is not just fit for purpose today, but ready for tomorrow.

PHASE THREE

NETWORK AUDIT
THE DIGITAL NERVOUS SYSTEM

This is the technical core of the audit, where we assess how data flows through your organisation. It's where architecture meets performance, and where resilience can be measured in real-time.

We analyse:

- Network architecture and logical topology
- Routing and switching configurations
- Firmware versions and update practices
- Redundancy and failover mechanisms
- High availability designs
- Monitoring systems, logs, and alerting platforms

The strategic output? A comprehensive understanding of your network's current-state capability. Where are the performance painpoints? How well does the infrastructure respond to faults or spikes in demand? How aligned is it to business continuity needs?

You'll receive:

- A full IP matrix and network device inventory
- QoS configuration and resilience review
- Capacity utilisation analysis
- Tactical and strategic recommendations for redesign or upgrades

This phase helps organisations shift from reactive troubleshooting to proactive performance tuning.

trustsystems.co.uk **networks@trustsystems.co.uk**

PHASE FOUR

WLAN SURVEY
WIRELESS WITHOUT WEAKNESS

Wireless networks are essential for mobility, flexibility, and user experience, but they're often the weakest link in both performance and security chains. This phase addresses that by conducting a thorough WLAN assessment.

Key areas of focus include:

- **Design and Coverage:** Does your current WLAN design reflect the real-world usage and physical environment?
- **Security**: We assess access controls, encryption standards, and SSID configurations.
- **Performance**: We test for dead zones, interference, channel overlap, and hardware limitations.
- **Compliance**: Regulatory considerations are factored into recommendations.

We provide:

- A visualised WLAN layout review
- A device-level performance report
- Insights into firmware needs and hardware modernisation options

A robust WLAN is foundational for everything from guest experiences to operational workflows.

trustsystems.co.uk **networks@trustsystems.co.uk**

PHASE FIVE

SECURITY AUDIT
BUILDING DIGITAL TRUST

Security is no longer an optional add-on, it must be embedded into every layer of your IT estate. Our security audit provides a snapshot of your organisation's digital trust posture and uncovers risks before they become incidents.

We evaluate:

- Vulnerability and penetration testing results
- Firmware and configuration risks
- Identity and access management policies
- Regulatory compliance and audit readiness
- Monitoring, logging, and incident response capabilities

This isn't just about ticking compliance boxes. It's about understanding how well your network can defend, detect, and recover from threats.

Outcomes include:

- **A full security posture report**
- **Compliance and policy gap analysis**
- **Prioritised mitigation recommendations**
- **Suggestions for resilience enhancements**

PHASE SIX

OT DEVICES & THE PURDUE MODEL - BRIDGING IT AND OT

Industrial networks bring a unique challenge. Operational Technology (OT) environments often run on legacy systems with limited visibility and high uptime demands. The convergence of IT and OT means that these environments must be secured and optimised with the same rigour as traditional IT networks.

We apply the Purdue Model as a framework for assessing:

- Device segmentation and trust zones
- Remote access and vendor management protocols
- Security gaps between IT and OT layers
- Update and patch management in control environments
- Traffic flow between levels (e.g., Level 0 sensors to Level 3 SCADA systems)

For industries like manufacturing, logistics, and energy, this phase is crucial to aligning operational resilience with cybersecurity best practices.

PHASE SEVEN

REPORTING & ROADMAP DEVELOPMENT – FROM INSIGHT TO ACTION

A network audit has little value without clear, actionable outcomes. That's why our final phase is focused on transforming technical findings into a roadmap that supports strategic decision-making and prioritised investment.

Our reporting principles:

- **Clarity:** Technical enough for engineers, yet understandable to executives
- **Relevance:** Findings are aligned with your organisation's strategic priorities
- **Actionability:** Clear recommendations with impact and effort scores

Roadmap development is where we chart the course forward—layering audit insights with budget realities, risk tolerance, and innovation ambitions.

We also promote a culture of continuous improvement with:

- Follow-up milestones and check-ins
- Scheduled re-audits or phased rollouts
- Training and handover where necessary

NETWORK AUDIT

BUILDING TRUST THROUGH TRANSPARENCY

A network audit is more than a service, it's a partnership grounded in transparency, precision, and strategic vision. By surfacing unseen risks and untapped opportunities, we empower IT leaders to take control of their infrastructure, communicate confidently with stakeholders, and drive meaningful transformation.

If you already suspect there are compromises in your environment or you're ready to take a proactive step, **explore our Network Services.** You'll find further insights and the opportunity to book an in-depth network audit tailored to your organisation.

What you'll get:

- A full diagnostic of your current network
- Clear identification of risks and inefficiencies
- Tailored recommendations to strengthen your infrastructure

When your network is trusted, your business can move faster, operate smarter, and scale without compromise.

BOOK TODAY

A network audit pays for itself in clarity, control, and long-term value.

trustsystems.co.uk **networks@trustsystems.co.uk**

SPEAK TO THE TEAM

NEXT STEPS

The Network Audit Framework – Strategic Guide outlines a comprehensive, strategic approach to understanding, securing, and optimising your network infrastructure. Here's a quick recap of what we've covered:

- **Planning & Scoping:** Aligning audit objectives with your business goals
- **Physical Audit**: Evaluating the tangible infrastructure layer
- **Network Audit:** Assessing architecture, performance, and resilience
- **WLAN Survey**: Ensuring wireless networks are secure, robust, and scalable
- **Security Audit:** Uncovering and mitigating cyber risk
- **Reporting & Roadmap:** Turning insights into a clear path forward
- **OT & The Purdue Model:** Bridging the IT/OT divide for industrial networks

CONTACT US

Start the conversation today with a member of the team.

Whether you're addressing current network concerns, planning for future innovation, or simply need to validate your infrastructure against today's demands, our team is here to help.

Let's Talk: *If you have questions, want further detail, or are ready to explore how a network audit could benefit your organisation, speak to one of our network specialists. We'll help you uncover the right next step, whether it's strategic advice, technical input, or a full audit engagement.*

trustsystems.co.uk **networks@trustsystems.co.uk**