Network Infrastructure Security Audit Requirements Document

Prepared By:

Information Network Security Administration (INSA)

2025/2026

Submitted by:

[Client's Name / Organization]

Submitted to:

Information Network Security Administration (INSA)

Cyber Security Audit Division Wollo Sefer, Addis Ababa, Ethiopia

Contact Person:

Tilahun Ejigu (Ph.D.)

Cyber Security Audit Division Head

✉: tilahune@insa.gov.et

📱: +251 937 456 374

Submission Date: [Insert Date]

Due Date for Response: Within Five (5) Working Days from the Date of Receipt

1. Background of INSA

The Information Network Security Administration (INSA) is Ethiopia's leading government body entrusted with safeguarding the country's digital infrastructure and cyber ecosystem. Established with a vision to ensure national cyber sovereignty and resilience, INSA performs critical functions such as conducting cyber security audits, providing policy direction, issuing compliance guidelines, and offering technical support across various governmental and private institutions.

INSA's Cyber Security Audit Division assesses the security posture of digital platforms including web applications, APIs, mobile applications, internal portals, and Network infrastructures. Our assessments identify vulnerabilities and recommend mitigation strategies aligned with global best practices.

2. Introduction

This document outlines the key requirements and submission expectations for organizations undergoing Network Infrastructure Security Audit with INSA. The goal is to evaluate the security, resilience, and compliance of routers, switches, firewalls, IDS/IPS, VPNs, load balancers, and core data center infrastructure, ensuring availability, confidentiality, and integrity of network operations.

Audits are conducted in alignment with frameworks and standards such as:

- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27001
- ISO/IEC 27033 (Network Security)
- COBIT

3. Objectives of the Audit Request

These assessments are vital for:

- Identify and mitigate vulnerabilities in the network infrastructure.
- Validate compliance with Ethiopian cybersecurity laws and international standards.
- Assess configuration hardening of critical infrastructure devices.
- Ensure resilience against internal and external cyberattacks.
- Strengthen logging, monitoring, and incident detection capabilities.
- Safeguarding sensitive data and operations from cyber threats.
- Enhance stakeholder and customer trust by demonstrating robust cybersecurity governance and risk management practices.

4. Required Submissions from the Client

You must submit the following via INSA's Audit Request Portal. Where submissions include sensitive configurations (e.g., router or switch configurations, firewall rule sets, or VPN credentials), those specific files must be delivered on encrypted media (CD/DVD/USB) directly to INSA's office or sent through a secure courier service to the address provided.

4.1 Legal and Administrative Documents (Mandatory)

- Updated Trade License
- TIN Number or National ID
- System Ownership/Authorization Letter for the infrastructure.

4.2 Technical Documentation (Mandatory - For Network Infrastructure Security Auditing)

To initiate the network infrastructure audit process, organizations are required to submit all necessary documentation and information as specified below. Submission of these mandatory requirements is a prerequisite for the commencement of the audit.

4.2.1 Network Architecture and Design

a) Network Topology Diagram

Provide detailed visual representations of the network architecture. Include both **logical and physical diagrams**.

Purpose:

- Identify all network segments (LAN, WAN, DMZ, cloud/hybrid environments).
- Highlight the placement of critical devices and interconnections.
- Identify trusted, untrusted, and restricted zones to assess attack surfaces.

Required Submission:

- **Logical Diagram:** showing routers, switches, firewalls, VPNs, IDS/IPS, DMZ, load balancers, servers, and interconnections.
- **Physical Diagram:** showing actual device locations and cabling/connection paths.
- Security zones (trusted/untrusted/restricted) clearly marked.

b) Asset Inventory List

Document all network devices and critical infrastructure components.

Purpose:

- Maintain visibility of all assets and their configurations.
- Support risk assessment and vulnerability prioritization.

Required Submission:

- Device type, vendor, model, OS/firmware version.
- IP addresses, VLANs, and subnets.
- Critical appliances such as firewalls, IDS/IPS, WAF, VPN gateways, load balancers, and servers.

c) Configuration Documentation

Provide configuration details for all critical network devices.

Purpose:

- Validate security configurations and hardening practices.
- Identify misconfigurations that may lead to vulnerabilities.

Required Submission:

- Router and firewall Access Control Lists (ACLs**)**.
- Switch port security policies (e.g., 802.1X, MAC filtering).
- VPN configurations including protocols and encryption standards.
- IDS/IPS, proxy, and load balancer rule sets.
- Security device settings aligned with best practices and organizational policies.

d) Access Control & Authentication Policies

Document all authentication and authorization mechanisms for network access.

Purpose:

- Ensure only authorized personnel have access to devices and critical segments.

- Evaluate privileged account management and password policies.

Required Submission:

- AAA configuration (RADIUS/TACACS+).
- Privileged/admin account management policies.
- Password and key management policies.
- Multi-factor authentication (MFA) usage where applicable.

e) Logging & Monitoring Details

Provide documentation of how network activity is logged and monitored.

Purpose:

- Ensure early detection of anomalies and potential incidents.
- Support incident response and forensic investigations.

Required Submission:

- Syslog/log server setups and configurations.
- SIEM integration and monitoring rules.
- Incident response triggers and escalation procedures.
- Log retention policies and formats.

f) Security Controls Documentation

Provide details of network security controls and their deployment.

Purpose:

- Verify that defence-in-depth measures are implemented effectively.
- Assess the protection of sensitive data and critical systems.

Required Submission:

- Firewalls, WAFs, IDS/IPS, VPNs, DLP solutions.
- Network segmentation (e.g., user VLANs, management VLAN, DMZ).
- Encryption protocols in use (TLS, IPsec, etc.).
- Network access restrictions and perimeter security measures.

4.2.3 Define Specific Auditing Scope (Mandatory)

Purpose: Clearly define the assets, locations, and systems to be audited.

Required Submission (Sample):

Asset Type	**Location**	**IP Address / VLAN**	Notes
Core Router	Data Center 1	10.0.0.1	Core WAN Router
Firewall	HQ DMZ	192.168.1.1	Internet Edge FW
Switches	Branch Office	10.1.0.0/24	Access Switch
VPN Gateway	HQ	203.0.113.5	

4.2.4 Security Functionality Documentation

Purpose: Provide details of implemented security features and operational safeguards within the network infrastructure.

Required Submission:

- User roles and access levels (e.g., network admins, operators, auditors).
- Device access control mechanisms (RBAC/AAA/TACACS+/RADIUS).

- Firewall policies and filtering rules.
- VPN and remote access configurations (protocols, authentication, encryption).
- Session management for network devices (timeouts, lockout policies).
- Secure communication protocols (TLS, IPsec, SSH, SNMPv3).
- Error handling and logging standards on critical appliances.
- Technical description of each function and control in place.

4.2.5 Security Configuration & Hardening Standards *(Network Equivalent)*

Purpose: Demonstrate compliance with industry best practices for securing network infrastructure.

Required Submission:

- Device hardening guidelines (firewalls, routers, switches, servers).
- Patch and firmware upgrade policy.
- Default credential removal and password policy enforcement.
- Secure management protocols (SSH, HTTPS, SNMPv3 vs. Telnet/HTTP/SNMPv1/2).
- Configuration baselines/checklists used during deployment.
- Evidence of regular vulnerability scans and compliance checks.

4.2.6 Previous Security Testing & Audit Reports (if available)

Purpose: Demonstrate history of security testing and remediation efforts.

Required Submission:

- Previous infrastructure audit reports (e.g., penetration testing, VA scans).
- Re-audit/remediation testing documents.
- Evidence of fixes implemented based on earlier findings.

- Documentation of lessons learned and applied security improvements.

5.4.8 Authorization and Access Control *(Network Focused)*

Purpose: Validate enforcement of least privilege across the infrastructure.

Required Submission:

- Role-based access to network devices (admins, operators, auditors).
- Privileged account management process (e.g., PAM solutions, password vaults).
- MFA usage for remote and administrative access.
- Access review policies and audit trails.

6. Contact Information and Communication

(keep as is, just update with your organization's details)

Name	Role	Email Address	Phone Number
John Doe	IT Security Officer	john@yourorg.com	+2519XXXXXXXX
Jane Smith	Network Operations Lead	jane@yourorg.com	+2519XXXXXXXX

7. Submission Instructions *(Corrected for Network)*

Submit all materials via INSA's Audit Request Portal. For sensitive files (e.g., router/firewall configs, VPN credentials, ACLs), deliver those on **encrypted CD/DVD/USB** to INSA's office or send securely via courier to:

Information Network Security Administration (INSA)

Cyber Security Audit Division

Wollo Sefer, Addis Ababa, Ethiopia

Contact: Tilahun Ejigu (Ph.D.), Cyber Security Audit Division Head

Email: tilahune@insa.gov.et

Mobile: +251 937 456 374

8. Conclusion

INSA is committed to working collaboratively to strengthen the resilience of your organization's network infrastructure. By submitting the required documentation within the specified timeline, you enable a comprehensive and accurate audit that enhances compliance, strengthens stakeholder trust, and reduces exposure to cyber threats.