Enterprise Security Audit & Compliance Case Study

Author: Mba Nonna

Focus Areas: Governance, Risk & Compliance (GRC), Enterprise Security Auditing

Frameworks & Standards: NIST CSF, NIST SP 800-30, ISO/IEC 27001, SOC 2

---

1. Executive Summary

This documents a comprehensive Enterprise Security Audit & Compliance Assessment conducted as part of formal GRC training. The engagement evaluated the security posture of two critical enterprise systems, Microsoft Exchange Server and Cisco AnyConnect VPN which support organizational communication and remote access.

The audit applied a risk-based methodology aligned with NIST SP 800-30, and mapped findings to NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and SOC 2 Trust Services Criteria. The outcome was a set of prioritized security risks, identified control gaps, and actionable remediation recommendations designed to reduce organizational exposure while supporting compliance and business continuity objectives.

This case study is structured to reflect real-world enterprise and consulting audit practices, not academic exercises.

2. Engagement Scope & Objectives

2.1 In-Scope Systems

- **Microsoft Exchange Server**
  Enterprise email infrastructure used for internal and external communication
- **Cisco AnyConnect VPN**
  Secure remote access solution for employees and administrators

2.2 Out-of-Scope

- End-user devices
- Physical Security Controls
- Third-party SaaS platforms not directly integrated with the systems assessed

2.3 Audit Objectives

- Identify threats, vulnerabilities, and risks affecting critical enterprise systems
- Evaluate effectiveness of existing technical and administrative controls
- Assess alignment with recognized security and compliance frameworks
- Prioritize risks based on likelihood and business impact
- Provide clear, actionable remediation and risk treatment recommendations

3. Business Context & Assumptions

3.1 Organizational Context

The assessed environment represents a mid-sized organization operating a hybrid work model. Secure email communication and VPN access were classified as high-impact assets due to their role in:

- Business communications
- Data exchange
- Remote workforce enablement
- Access to internal and cloud-based resources

A compromise of these systems would have a direct impact on confidentiality, availability, and operational continuity.

3.2 Key Assumptions

- Email systems process sensitive organizational and user data
- VPN access provides entry into internal corporate networks
- Credential-based attacks represent a primary threat factor
- Security incidents impacting these systems would have material business impact

4. Audit Lifecycle

The engagement followed a structured enterprise IT audit lifecycle, consistent with industry GRC and consulting practices.

Phase 1: Planning & Scoping

- Defined audit objectives and success criteria
- Identified critical systems and assets
- Established assumptions, constraints, and boundaries
- Selected applicable frameworks (NIST CSF, ISO 27001, SOC 2)

Output: Approved audit scope and methodology

Phase 2: Asset Identification & Classification

- Identified high-impact assets supporting core business functions
- Classified assets based on confidentiality, integrity, and availability (CIA)
- Prioritized assets based on business criticality

Output: Asset inventory and impact classification

Phase 3: Threat & Vulnerability Identification

- Identified relevant threat actors and attack vectors
- Mapped vulnerabilities to exposed assets
- Considered both technical and procedural weaknesses

Output: Threat–vulnerability mapping

Phase 4: Risk Analysis & Evaluation

- Identified relevant threat actors and attack vectors
- Mapped vulnerabilities to exposed assets
- Considered both technical and procedural weaknesses

Output: Threat–vulnerability mapping

Phase 5: Control Assessment & Gap Analysis

- Evaluated control effectiveness against framework requirements
- Identified control gaps and partial implementations
- Assessed alignment with compliance standards

Output: Control gap analysis

Phase 6: Compliance Mapping

- Mapped findings to NIST CSF categories
- Aligned risks with ISO/IEC 27001 Annex A controls
- Evaluated impact on SOC 2 Trust Services Criteria

Output: Compliance alignment summary

Phase 7: Reporting & Recommendations

- Developed executive-level summaries
- Produced detailed technical findings
- Provided prioritized remediation recommendations

Output: Final audit deliverables and remediation roadmap

---

5. Asset Identification & Classification

Asset	Description	CIA Impact
Exchange Server	Enterprise email platform	High
VPN Infrastructure	Remote access gateway	High
User Credentials	Authentication assets	High
Email Data	Sensitive communications	High

6. Threat Modeling Approach

Threat identification considered:

- Credential theft (phishing, brute-force, credential stuffing)
- Unauthorized remote access
- Exploitation of unpatched vulnerabilities
- Insider misuse
- Service disruption and availability attacks

Threats were mapped to affected assets and evaluated in relation to existing controls.

7. Risk Assessment Methodology

Risks were evaluated using a qualitative risk assessment model aligned with NIST SP 800-30:

- **Likelihood:** Low / Medium / High
- **Impact:** Low / Medium / High
- **Risk Rating:** Likelihood × Impact

8. Detailed Findings – Microsoft Exchange Server

EX-01: Weak Authentication Controls

- **Threat:** Credential compromise
- **Vulnerability:** Inconsistent MFA enforcement
- **Impact:** Unauthorized access to email and sensitive data
- **Likelihood:** Medium
- **Risk Rating:** High

EX-02: Patch Management Gaps

- **Threat:** Exploitation of known vulnerabilities
- **Vulnerability:** Delayed security patching
- **Impact:** System compromise and service disruption
- **Likelihood:** Medium
- **Risk Rating:** Medium–High

9. Detailed Findings – Cisco AnyConnect VPN

VPN-01: Unauthorized Remote Access

- **Threat:** Credential abuse or stolen credentials
- **Vulnerability:** Inadequate access review processes
- **Impact:** Internal network compromise
- **Likelihood:** Medium
- **Risk Rating:** Medium

VPN-02: Insufficient Authentication Monitoring

- **Threat:** Undetected brute-force attacks
- **Vulnerability:** Limited logging and alerting
- **Impact:** Delayed detection and response
- **Likelihood:** Medium
- **Risk Rating:** Medium

10. Consolidated Risk Register

ID	Risk	System	Likelihood	Impact	Rating
EX-01	MFA gaps	Exchange	Medium	High	High
EX-02	Patch delays	Exchange	Medium	High	Med-High
VPN-01	Unauthorized access	VPN	Medium	Medium	Medium
VPN-02	Limited monitoring	VPN	Medium	Medium	Medium

11. Control Gap Analysis

Identified control gaps included:

- MFA policies not enforced organization-wide
- Access reviews not formally documented or scheduled
- Logging enabled but not actively monitored or correlated
- Incident response procedures lacked authentication-specific workflows

12. Compliance Mapping

NIST Cybersecurity Framework

- **ID.RA** – Risk Assessment
- **PR.AC** – Identity & Access Management
- **PR.IP** – Information Protection Processes
- **DE.CM** – Continuous Monitoring

ISO/IEC 27001

- **A.5** – Information Security Policies
- **A.8** – Asset Management

- **A.9** – Access Control
- **A.12** – Operations Security

SOC 2 Trust Services Criteria

- Security
- Availability

13. Risk Treatment Strategy

Recommended risk treatment actions:

- Enforce MFA for all users and privileged accounts
- Implement formal vulnerability and patch management cycles
- Apply least-privilege access controls
- Enhance logging, monitoring, and alerting
- Formalize access review and incident response procedures

14. Residual Risk Consideration

Residual risk remains where:

- Business constraints limit immediate remediation
- Legacy systems restrict full control implementation

Such risks require formal acceptance or compensating controls.

15. Deliverables

- Executive risk summary
- Detailed risk assessment reports
- Risk register and prioritization matrix
- Compliance alignment documentation
- Remediation roadmap

16. Lessons Learned

- Credential-based threats remain a dominant enterprise risk
- MFA enforcement significantly reduces attack surface
- Compliance mapping improves stakeholder communication

- Continuous monitoring is critical for early threat detection

17. Supporting Artifacts

- Risk Assessment on Microsoft Exchange & Cisco AnyConnect VPN
- IT Audit on Microsoft Exchange & Cisco AnyConnect VPN

18. References

- NIST SP 800-30 – Guide for Conducting Risk Assessments
  https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- NIST Cybersecurity Framework
  https://www.nist.gov/cyberframework
- ISO/IEC 27001:2022
  https://www.iso.org/standard/27001
- SOC 2 Trust Services Criteria (AICPA)
  https://www.aicpa.org/resources/article/soc-2-report
- CISA – Cross-Sector Cybersecurity Performance Goals
  https://www.cisa.gov/cpgs
- Microsoft Exchange Security Documentation
  https://learn.microsoft.com/security
- Cisco AnyConnect Secure Mobility Client Documentation
  https://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client