GRC Compliance Assessment Report

Overall Risk Rating: HIGH

Executive Summary

This report presents a comprehensive security assessment of your network infrastructure conducted on 2025-11-16. The assessment follows ISO 31000:2018 risk management standards and includes machine learning-based threat detection.

Key Findings

Metric	Count
Hosts Scanned	5
Vulnerabilities Found	12
Total Risks Identified	8
Critical Risks	2
High Risks	3
Threats Detected (ML)	4

■ **WARNING:** 2 critical risks require immediate attention!

Top Recommendations

1. Address all critical risks within 24 hours
2. Implement comprehensive patch management
3. Enhance access control mechanisms
4. Establish continuous monitoring
5. Conduct regular security assessments

Risk Assessment Details

Risk Distribution by Severity

Risk Level	Count
EXTREME	1
HIGH	2
MEDIUM	1

Top 10 Risks

1. Unauthorized access to web server
Risk Level: EXTREME | CVSS Score: 9.8
Cause: Outdated Apache version with known vulnerabilities

2. SSH brute force attack
Risk Level: HIGH | CVSS Score: 7.5
Cause: Weak SSH configuration

3. Data exfiltration via open port
Risk Level: HIGH | CVSS Score: 7.0
Cause: Unnecessary open ports

4. Denial of service attack
Risk Level: MEDIUM | CVSS Score: 5.5
Cause: Missing rate limiting

Vulnerability Details

CRITICAL Vulnerabilities (1)

CVE-2023-1234
Service: Apache | Port: 80
CVSS: 9.8

HIGH Vulnerabilities (1)

CVE-2023-5678
Service: OpenSSH | Port: 22
CVSS: 7.5

Mitigation and Remediation Plan

Immediate Actions (Within 24 hours)

Critical vulnerability in Apache
Timeframe: Within 24 hours
Estimated Effort: 2-4 hours

SSH hardening required
Timeframe: Within 48 hours
Estimated Effort: 1-2 hours

Remediation Project Plan

Total Duration: 2 weeks
Total Cost Estimate: $5,000-$10,000
Resources Required: 2 security engineers

Compliance Status

Requirement	Status
Context Established	✓
Risks Identified	✓
Risks Analyzed	✓
Risks Evaluated	✓
Mitigation Planned	✓

Overall ISO 31000:2018 Compliance: COMPLIANT