Technical Review

Prepared for:

Prepared by:
Copper Mountain Consulting
02/01/2025

Technical Risk Analysis

Scan Date: 02/01/2025

Table of Contents

Technical Risk Analysis Overview

The Technical Risk Analysis aggregates risk analysis from multiple assessments performed on the network, providing you with a high-level overview of the health and security of the network.

The report details the scan tasks undertaken to discover security issues. In addition to the overall Risk Score, the report also presents separate risk scores for all IT assessments (Network, Security) performed on the network environment. This includes a summary of individual issues, as well as their severity and weighting within the risk analysis.

At the end of the report, you can find a summary of the assets discovered on the network, in addition to other useful information organized by assessment type.

Risk analysis and risk management are not one-time activities. Risk analysis and risk management are dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management process to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Technical Risk Analysis Discovery Tasks

The following discovery tasks were performed.

	TASK	DESCRIPTION
Network		
✓	Detect Azure Environment	Scan for Azure AD and infrastructure components.
✓	Detect Domain Controllers	Identifies domain controllers and online status.
✓	FSMO Role Analysis	Enumerates FSMO roles at the site.
✓	Enumerate Organization Units and Security Groups	Lists the organizational units and security groups (with members).
✓	User Analysis	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
✓	Detect Local Accounts	Detects local accounts on computer endpoints.
✓	Detect Added or Removed Computers	Lists computers added or removed from the Network since the last assessment.
✓	Detect Local Mail Servers	Detects mail server(s) on the network.
✓	Detect Time Servers	Detects server(s) on the network.
✓	Discover Network Shares	Discovers the network shares by server.
✓	Detect Major Applications	Detects all major apps / versions and counts the number of installations.
✓	Detailed Domain Controller Event Log Analysis	Lists the event log entries from the past 24 hours for the directory service, DNS server and file replication service event logs.
✓	Web Server Discovery and Identification	Lists the web servers and type.
✓	Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
✓	Internet Access and Speed Test	Tests Internet access and performance.
✓	SQL Server Analysis	Lists the SQL Servers and associated database(s).
✘	Internet Domain Analysis	Queries company domain(s) via a WHOIS lookup.

	TASK	DESCRIPTION
✓	Missing Security Updates	Identifies computers missing security updates.
✓	System by System Event Log Analysis	Discovers the file system and app event log errors for servers.
✓	External Security Vulnerabilities	Lists the security holes and warnings from External Vulnerability Scan.
Security		
✓	Detect System Protocol Leakage	Detects outbound protocols that should not be allowed.
✓	Detect Unrestricted Protocols	Detects system controls for protocols that should be allowed but restricted.
✓	Detect User Controls	Determines if controls are in place for user web browsing.
✓	Detect Wireless Access	Detects and determines if wireless networks are available and secured.
✓	External Security Vulnerabilities	Performs a detailed External Vulnerability Scan. Lists and categorizes external security threats.
✓	Network Share Permissions	Documents access to file system shares.
✓	Domain Security Policy	Documents domain computer and domain controller security policies.
✓	Local Security Policy	Documents and assesses consistency of local security policies.
Microsoft Cloud		
✓	Microsoft Cloud Scan	Performed Microsoft Cloud Scan.

Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.

Several critical issues were identified. Identified issues should be investigated and addressed according to the Technical Risk Analysis.

ISSUE TYPE	RISK SCORE
Network	
Security	
Data Security	
Azure AD	

Issue Graph

This section contains a summary of issues detected during the Technical Review process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.

Issue Graph

Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)

Network Issue Graph

Security Issue Graph

Data Security Issue Graph

Azure AD Issue Graph

Issue Summary

Network Issue Summary

2805 **Inactive computers (15 pts each)**

Current Score: 15 pts x 187 = 2805: 36.24%

Issue: Computers have not checked in during the past 30 days.

Recommendation: Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, logged into by authorized users, or powered on.

2250 **User password set to never expire (30 pts each)**

Current Score: 30 pts x 75 = 2250: 29.07%

Issue: User accounts with passwords set to never expire present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.

Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

776 **Unsupported operating systems (97 pts each)**

Current Score: 97 pts x 8 = 776: 10.03%

Issue: Computers found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.

Recommendation: Upgrade or replace computers with operating systems that are no longer supported.

611 **User has not logged on to domain in 30 days (13 pts each)**

Current Score: 13 pts x 47 = 611: 7.9%

Issue: Users have not logged on to domain in 30 days. A user that has not logged in for an extended period of time could be a former employee or vendor.

Recommendation: Disable or remove user accounts for users that have not logged on to active directory in 30 days.

375 Few Security patches missing on computers. (75 pts each)

Current Score: 75 pts x 5 = 375: 4.85%

Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Few is defined as missing 3 or less patches.

Recommendation: Address patching on computers missing 1-3 security patches.

270 Anti-spyware not up to date (90 pts each)

Current Score: 90 pts x 3 = 270: 3.49%

Issue: Up to date anti-spyware definitions are required to properly prevent the spread of malicious software. Some anti-spyware definitions were found to not be up to date.

Recommendation: Ensure anti-spyware definitions are up to date on specified computers.

200 Operating system in Extended Support (20 pts each)

Current Score: 20 pts x 10 = 200: 2.58%

Issue: Computers are using an operating system that is in Extended Support. Extended Support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.

Recommendation: Upgrade computers that have operating systems in Extended Support before end of life.

194 Unsupported Microsoft Office Version (97 pts each)

Current Score: 97 pts x 2 = 194: 2.51%

Issue: Computers found using a version of Microsoft Office that is no longer supported. Unsupported software no longer receives vital security patches and present an inherent risk.

Recommendation: Upgrade Microsoft Office versions that are no longer supported.

90 Insecure listening ports (10 pts each)

Current Score: 10 pts x 9 = 90: 1.16%

Issue: Computers are using potentially insecure protocols.

Recommendation: There may be a legitimate business need, but these risks should be assessed individually. Certain protocols are inherently insecure since they often lack encryption. Inside the network, their use should be minimized as much as possible to prevent the spread of malicious software. Of course, there can be reasons these services are needed and other means to protect systems which listen on those ports. We recommend reviewing the programs listening on the network to ensure their necessity and security. See Listening Ports sheets in Excel Export for details.

90 Excessive security patches missing on computers (90 pts each)

Current Score: 90 pts x 1 = 90: 1.16%

Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Excessive is defined as missing four or more patches.

Recommendation: Address patching on computers missing 4+ security patches.

68 Potential disk space issue (68 pts each)

Current Score: 68 pts x 1 = 68: 0.88%

Issue: 1 computer were found with significantly low free disk space.

Recommendation: Free or add additional disk space for the specified drives.

10 Un-populated organization units (10 pts each)

Current Score: 10 pts x 1 = 10: 0.13%

Issue: Empty organizational units (OU) were found in Active Directory. They may not be needed and can lead to misconfiguration.

Recommendation: Remove or populate empty organizational units.

Security Issue Summary

71155 Critical Internal Vulnerabilities Detected (95 pts each)

Current Score: 95 pts x 749 = 71155: 89.38%

Issue: Critical internal vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. Internal vulnerabilities are considered potential security holes that can allow hackers access to your network and information.

Recommendation: We recommend assessing the risk of each vulnerability and remediating all internal vulnerabilities as prescribed.

1680 Medium External Vulnerabilities Detected (70 pts each)

Current Score: 70 pts x 24 = 1680: 2.11%

Issue: Medium severity external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.

Recommendation: Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed.

1615 Critical External Vulnerabilities Detected (95 pts each)

Current Score: 95 pts x 17 = 1615: 2.03%

Issue: Critical external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.

Recommendation: Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed.

1425 Passwords less than 8 characters allowed (75 pts each)

Current Score: 75 pts x 19 = 1425: 1.79%

Issue: Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.

Recommendation: Enable enforcement of password length to 8 or more characters.

1224 Password history not remembered for at least six passwords (72 pts each)

Current Score: 72 pts x 17 = 1224: 1.54%

Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.

Recommendation: Increase password history to remember at least six passwords.

1152 Automatic screen lock not turned on (72 pts each)

Current Score: 72 pts x 16 = 1152: 1.45%

Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.

Recommendation: Enable automatic screen lock on the specified computers.

750 Password complexity not enabled (75 pts each)

Current Score: 75 pts x 10 = 750: 0.94%

Issue: Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.

Recommendation: Enable password complexity to assure that network user account passwords are secure.

340 Inconsistent password policy / Exceptions to password policy (68 pts each)

Current Score: 68 pts x 5 = 340: 0.43%

Issue: Password policies are not consistently applied from one computer to the next. A consistently applied password policy ensures adherence to password best practices.

Recommendation: Eliminate inconsistencies and exceptions to the password policy. See the Security Policy Assessment report for policy details.

200 Open or insecure WiFi protocols available (50 pts each)

Current Score: 50 pts x 4 = 200: 0.25%

Issue: Open or insecure WiFi protocols may allow an attacker access to the company's network and resources.

Recommendation: Ensure company's WiFi is secure and discourage the use of any open WiFi connections.

70 Maximum password age greater than 90 days (70 pts each)

Current Score: 70 pts x 1 = 70: 0.09%

Issue: Passwords that are not changed regularly are more vulnerable to attack and unauthorized use. Minimizing the allowed password age greatly reduces the window of time that a lost or stolen password poses a threat.

Recommendation: Modify the maximum password age to be 90 days or less.

Azure AD Issue Summary

90 Customer Lockbox Not Enabled (90 pts each)

Current Score: 90 pts x 1 = 90: 100%

Issue: A misalignment between Microsoft best practices based on Microsoft Secure Score was detected related to Customer Lockbox Not Enabled. The control may not be implemented or partially implemented. See Risk Report or Management Plan for recommendations.

Recommendation: Turning on the customer lockbox feature requires that approval is obtained for datacenter operations that grants a Microsoft employee direct access to your content. Access may be needed by Microsoft support engineers if an issue arises. There's an expiration time on the request and content access is removed after the support engineer has fixed the issue.