CTG Environment Assessment

Sanitized Sample Report

Prepared by:

Brandon Fogliano

Wednesday, March 16, 2022

March 16, 2022

Prepared for:
ABC Corp
333 Newbie Blvd.
Cleveland, OH 44221

This report contains the results of the January 2020 Environment Assessment performed for ABC Corp, (ABC Corp). The scope of the engagement was to identify pertinent information across 3 main modules that make up the company environment.

Corporate Technologies Group (CTG) has outlined our methodologies and the approach taken to discover the environment and provide the information to better develop long term strategies and goals. The recommendations included in this report will help strengthen ABC Corp's ability to manage, maintain, and secure the corporate network.

Additionally, the report includes both Operational and Strategic Recommendations. Operational Recommendations reflect point-in-time issues identified during the engagement, whereas Strategic Recommendations are longer-term issues that may require more time to address.

CTG appreciates the opportunity to provide services for ABC Corp. If you have any questions or concerns, please feel free to contact us at any time.

Report Disclaimer Statement

This disclaimer governs the use of this report. Client shall own all right, title, and interest in and to any written summaries, reports, analyses, and findings or other information or documentation prepared for client in connection with CTG consulting services to Client. CTG specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary, or punitive) arising from or related to reliance by anyone any guidance in this report or any contents thereof.

Corporate Technologies Group Confidential

This document has been classified as Corporate Technologies Group Confidential. This is an internal CTG designation, which has the highest classification ranking for Client data. Stringent protection of this document is required by CTG's information classification policy and security controls. This document should never be communicated from CTG to the Client in an unencrypted format. Additionally, the information contained in this report is strictly prohibited from any type of release except to the Client.

Table of Contents

Executive Summary and Component Description

Corporate Technologies Group (CTG) was commissioned by ABC Corp to assess the current information technology environment based on 3 different modules, Network, Security, and Cloud. The objective of the assessment is to provide information pertinent to each area covered, including but not limited to the following:

Network

- Detailed Inventory of Devices in the Environment
- Colored and Scored Client Risk Report
- Risk Report and Management Plan
- Layer 2-3 Detailed Network Report
- Windows Patch Assurance Report
- Service Account Report

Security

- Device Security Report Card
- Missing Critical Patch and Software Inventory Report
- External Vulnerability Scan
- Failed Login Report
- Login History per Machine
- Outbound Security Report
- Security Assessment PowerPoint
- Security Health Report
- Security Management Plan
- Security Risk Report
- Share Permission Report
- User Behavior Analysis
- Data Breach Liability Report

Cloud

- Microsoft Azure Assessment
- Microsoft Management Plan
- Microsoft Cloud Assessment
- Microsoft Teams Assessment
- OneDrive Usage Report
- Risk Report
- SharePoint Assessment

Assessment Priority Rating Per Component

CTG scores on a simple Low, Medium, High scale per component to show user what modules need to be addressed first. The following are the Priority levels for each component in the assessment.

Component	Priority Rating
Network	**High**
Security	**High**
Cloud	**High**

Assessment Overview

CTG performed an assessment of the environment encompassing the 3 modules discussed in the executive summary, network, security, and cloud. The intent of the assessment was to ensure that ABC Corp, to the best of their ability, is in accordance and adherence to leading best practices in designing, securing, and maintaining the corporate IT environment to minimize the exposure of information systems.

Solutions and recommendations in this assessment that would help to lower the risk exposure to ABC Corp may require additional technology purchases or cost increases due to advanced licensing needs. Examples of this would be advanced Microsoft 365 licensing, such as MS 365 E5, Enterprise Mobility + Security, O365 Advanced Threat Protection (ATP) Plan 1 or 2, and Azure Active Directory P2. CTG has detailed each of the assessment areas, the information reviewed, Strategic Recommendations, and Technical Findings in the following pages of the report.

Summary of Strategic Recommendations

In the following sections, Strategic and Operational Recommendations, CTG will outline long term goals and short-term items that will help to improve and build upon the ABC Corp technology environment. Strategic Recommendations are improvement goals over the long term and may take more time to implement and could incur costs and advance technology purchases. Operational Recommendations are items that may help to improve the environment in the immediate time frame.

Building a strong information technology strategy based on the Strategic Recommendations will help to address gaps, will help to identify similar vulnerabilities in the future, and will create a strong environment, based on best practice and industry standards. The Strategic Recommendations per component identified during the assessment are as follows:

Total Findings Per Assessment Module	High	Medium	Low
Network	4	1	6
Security	5	2	1
Cloud	12	0	0

Strategic Recommendations	Priority Rating
Network	
Implement MFA – Internally and Externally	High
Cloud	
Utilize Microsoft Secure Score Services	High
Assign Adequate Licensing Level	High
Security	
Monitoring and Managing Darkweb for credentials	High

Summary of Operational Recommendations

Operational Recommendations	Priority Rating
Network	
Update Outdated Operating Systems	High
Ensure Antivirus and Antimalware/EDR deployed to all endpoints	High
Ensure all Antivirus/EDR definitions are up to date	High
Address Missing Patches	High
Free Up or Add Space for Drives	Medium
Investigate All Accounts with Passwords Set to Never Expire	Low
Upgrade Computer Operating Systems in Extended Support	Low
Investigate the List of Inactive Computers	Low
Disable or Remove User Accounts Not Logged on to Active Directory in 30 Days	Low
Investigate Insecure Listening Ports on Machines	Low
Remove or Populate Empty Organizational Units	Low
Cloud	
Customer Lockbox Not Enabled	High
Self-Service Password Reset	High
Block Legacy Authentication	High
Integrated Apps	High
Calendar Sharing with External Users	High
Disallow Addition of Accepted Domains or Common Domains to Allowed Domains	High
Microsoft Defender for Office 365	High
Turn On Safe Attachments in Block Mode	High
Safe Documents Protection	High
Safe Links Protection	High
Turn On User Risk Policy	High
Turn On Sign-In Risk Policy	High
Security	
Ensure All Compromised Passwords Are No Longer in Use	High
Enable Account Lockout for All Users	High
Enable Enforcement of Password Length to More Than 10 Characters	High
Enable Password Complexity for All Users	High
Increase Password History to Remember at Least 6 Passwords	High
Enable Automatic Screen Lock	Medium
Eliminate Inconsistencies and Exceptions Password Policy	Medium
Ensure Company WIFI is Secure, Don’t use Open WIFI Connections	Low

Strategic Recommendations

Strategic Recommendations are systemic exposures identified during the assessment that may indicate deficiencies within the solutions for ABC Corp. Without resolving the Strategic Recommendations, the Operational Recommendations could reappear gradually over time. A comprehensive strategy for tackling exposures can exist by addressing both the Strategic and Operational Recommendations, without the likelihood of reoccurrence.

Network Recommendations

The following section lists the systemic issues identified during the assessment, describes the associated exposure, provides a remediation plan, and includes additional information where applicable.

High-Priority Recommendations

Implement MFA

Priority Rating	**High**
Description:	
During the assessment, CTG identified that multi-factor authentication (MFA) was not enabled for all users. As such, access to ABC Corp's Microsoft 365 environment is dependent solely on the strength of end-users' passwords. This implementation should be a requirement, as passwords could be easily guessed, stolen via social engineering, or harvested from data breaches.	
Remediation:	
A common deployment of MFA utilizes a push notification to the user's mobile device, in which clicking a button to accept is required. Users will often simply accept any notifications, even if a login attempt was not recently performed. Requiring the user to take the response sent to a mobile device	

or a one-time PIN (OTP), such as Google Authenticator or Duo Mobile, and type it into the challenge box on a login page is considered a much safer implementation. As requirements for cybersecurity insurance and other compliances grow in complexity, MFA will become more required for internal environments as well. For instance, logging into servers or admin accounts on desktops. There are other platforms that can be implemented to meet this need.

Short-Term Objectives:

• Raise Awareness - Use an internal campaign to raise awareness about how compromised credentials can cause damage to the organization's mission. Even 'good' passwords can be compromised.
• Plan an Enrollment Campaign - Encourage employees to use the https://aka.ms/mfasetup link to enroll in MFA. Reports are available to measure and aid in enforcing enrollment progress. Employees will need to have a smartphone or phone number that can receive an SMS message. This enrollment period should have a deadline.

Mid-Term Objectives:

Begin the process to enroll users in MFA and provide Self-Service Password Reset as an option. Since this process can be lengthy, coordinate groups for a phased deployment. All Administrators should use MFA, which can be enforced with a Conditional Access Policy.

• Schedule MFA Enforcement by Group

1. Select a group, such as IT, Executives, and Finance, where the enforcement will begin and ensure that that group has the correct version of Outlook that supports modern authentication.
2. Set a date for completion and enforce the policy with Conditional Access.
3. Continue with each group, moving from high-privilege groups to low-privilege groups.
4. Password resets and MFA enforcement should be mandatory for high-privilege accounts, regardless of position in the MFA rollout schedule.

Note: Additional consideration may be required for applications that utilize legacy authentication.

Long-Term Objectives:

Enforce MFA for all connections and all employees. Microsoft Hello for Business should also be implemented to further improve identity protection.

References:

https://pages.nist.gov/800-63-3/sp800-63b.html
MFA Settings:
https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/set-up-multifactor-authentication
MFA Rollout Materials:
https://www.microsoft.com/en-us/download/details.aspx?id=57600
Microsoft Hello:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-forbusiness/hello-overview
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-forbusiness/passwordless-strategy

Cloud Recommendations

High-Priority Recommendations

Utilize Microsoft Security Score Services

Priority Rating	**High**
Description:	
Microsoft Secure Score and Azure Identity Secure Score services are security analytics tools that analyze and score security posture against Microsoft's recommended best practices and controls. These tools also identify and prioritize specific actionable recommendations aimed at reducing overall risk and potential compromise. Note: Microsoft advises against relying upon Secure Score as the 'sole source' of security measurement to calculate risk, prevent breach, or prevent compromise.	
Remediation:	
Use the Microsoft Secure Score and Azure Identity Secure Score services to continuously monitor and remediate to align with Microsoft's recommended security best practices and controls.	
Short-Term Objectives:	
Microsoft Secure Score and Azure Identity Secure Score should be evaluated on a regular basis. This score should be tracked as a Key Performance Indicator (KPI) for the IT team. The formal review should take place on a regular (quarterly) basis, as additional threats or best practices could be discovered and implemented.	
Long-Term Objectives:	
A framework, such as NIST 800-171 or NIST CSF, should be selected by the organization. Once selected, the Microsoft Compliance Manager, located at https://servicetrust.microsoft.com, should be leveraged to measure progress toward improving the organization's security posture.	
References:	
Login Portal: https://securescore.office.com/ https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-securescore?view=o365-worldwide https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/identity-securescore	

Assign Adequate Licensing Level

Priority Rating	**High**
Description:	
Licensing levels in Microsoft 365 and Office 365 determine the products and features available to individual users within the platform. Many of the features add protection that prove beneficial for high profile or easily targeted users. These additional protections are not available in the Microsoft 365 Business suite of products. Enterprise level licenses provide additional protections when properly assigned and configured. <u>Enterprise E3 Licensed Users Gain:</u> • Email Message Encryption - Protect data sent via email • Information Rights Management - Protect data from being shared without permission	

• Data Loss Prevention - Protect data from being accidentally exposed or shared At the E3 level, only Email and Files can be protected • Email Archiving - Retain email data for extended periods of time • eDiscovery - Search data for keywords related to internal or legal inquiries • Legal Hold - Freeze data at a point in time, track all future changes and access <u>Enterprise E5 Licensed Users Gain E3 Protections plus:</u> • Advanced Threat Protection - Microsoft's evolving detection techniques • Cloud App Security - Advanced alerting and SIEM integration tool • Customer Lockbox - Define Microsoft's access to sensitive data during support tickets • Data Loss Prevention - Protect Teams data from accidental exposure • Privileged Access Management - Fine tune administrative access and detailed audits • Advanced Message Encryption - Automatically encrypt messages containing protected data types.
Remediation:
• Create a policy that defines the necessary protections based on a user's profile and access. • Review license levels for high-profile employees and users with access to sensitive data. • Update user account creation processes to include a license assessment.
References:
https://www.microsoft.com/en-us/microsoft-365/business/compare-more-office-365-forbusiness-plans https://azure.microsoft.com/en-us/services/information-protection/ https://docs.microsoft.com/en-us/microsoft-365/compliance/privileged-accessmanagement-overview?view=o365-worldwide

Security Recommendations

High-Priority Recommendations

Monitoring and Managing Darkweb for Credentials

Priority Rating	**High**
Description:	
As more technology moves to cloud infrastructure or SaaS platforms such as Office 365, Salesforce etc., identity management and password protection are more important than ever. Any attacker can now attempt to breach web portals that are available to the world. Companies must monitor the Darkweb for user credentials that have been compromised and make sure they are corrected immediately.	
Remediation:	
There are many websites that can monitor for credentials on the Darkweb but in many cases they are manual and cannot alert to new compromises. Obtain a platform that can monitor the whole company domain and possibly private email addresses and can also alert periodically and on new compromise detections.	
Short-Term Objectives:	
Companies should actively be looking for Darkweb monitoring services that provide the capabilities mentioned above. These platforms are easy to use and quick to setup and all companies should take advantage of them as soon as possible.	
References:	
https://ctgusa.net/services/dark-web-scan/ https://www.idagent.com/blog/10-dark-web-facts-you-need-to-see-right-now/	

Operational Recommendations

Operational Recommendations are more technical in nature and may have immediate remediations that can be applied. In many cases licensing is already in place and there is no need to purchase anything. Configurations could have been overlooked or not implemented for specific reason, but the capabilities to fix these items may be present. Some configurations may need advanced licensing.

Network Recommendations

The following section lists the operational issues identified during the assessment, describes the associated exposure, provides a remediation plan, and includes additional information where applicable.

High-Priority Recommendations

Update Outdated Operating System

Priority Rating	**High**
Description:	
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.	
Remediation:	
Replace or update computers with outdated operating systems as soon as possible.	
Short-Term Objectives:	
On occasion there are software packages that need to live on older operating systems. If any machine in the report is in this category create a secured VLAN and move those machines to the VLAN to	

segregate the vulnerable machines for the rest of the network. The following machines have unsupported operating systems: ☐ Generic PC 1 / 10.10.10.1,172.22.6.54 / Windows 10 Pro for Workstations Version 1909 ☐ Generic PC 2 /172.22.6.51 / Windows 10 Pro for Workstations Version 1909

Ensure Antispyware and Antivirus is Installed on All Endpoints

Priority Rating	**High**
Description:	
Antivirus and Antispyware software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.	
Remediation:	
Assure that Antivirus and Antispyware is deployed to all possible endpoints in order to prevent both security and productivity issues. The following machines may not have Antivirus and Antispyware:	
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PCIP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	☐ Computer: GENERIC PC IP Address: 10.10.10.5
☐ Computer: GENERIC PC IP Address: 10.10.10.5	

Ensure All Antivirus and Antispyware Definitions are up to Date

Priority Rating	**High**
Description:	
Up to date Antispyware definitions are required to properly prevent the spread of malicious software. Some Antispyware definitions were found to not be up to date.	
Remediation:	
Ensure anti-spyware definitions are up to date on specified computers. Machines with Antispyware definitions possibly out of date are below:	
☐ Computer: GENERIC PC IP Address: 10.10.10.5 Security Center: Windows Defender ☐ Computer: GENERIC PC IP Address: 10.10.10.5 Security Center: Windows Defender ☐ Computer: GENERIC PC IP Address: 10.10.10.5 Security Center: Windows Defender	☐ Computer: GENERIC PC IP Address: 10.10.10.5 Security Center: Windows Defender ☐ Computer: GENERIC PC IP Address: 10.10.10.5 Security Center: Windows Defender ☐ Computer: GENERIC PC IP Address: 10.10.10.5 Security Center: Windows

Address Missing Patches

Priority Rating	**High**
Description:	
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 missing patches on the machines listed. Make sure important patches are instead unless there is a specific reason to not have them installed. The following machines are missing 1-3 security patches:	
☐ GENERIC PC / 10.10.10.5 / Windows 10 Pro Version 20H2 ☐ GENERIC PC / 10.10.10.5 / Windows 10 Pro Version 20H2 ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Standard	☐ GENERIC PC / 10.10.10.5 / Windows 10 Pro Version 20H2 ☐ GENERIC PC / 10.10.10.5 / Windows 10 Pro Version 20H2

Medium-Priority Recommendations

Free Up or Add Space for Drives

Priority Rating	**Medium**
Description:	
2 computers were found with significantly low free disk space. If these drives are system drives it cause issues installing software or logging onto the users' profile.	

Remediation:
Free space or add space for the specified drives
☐ GENERIC PC - E: : 0.05 GB free ☐ GENERIC PC - A: : 0.06 GB free

Low-Priority Recommendations

Investigate All Accounts with Passwords Set to Never Expire

Priority Rating	**Low**
Description:	
Although NIST (National Institutes for Standards and Technology) no longer advocates for password expirations, many compliances and company policies still enforce this policy. If passwords are not created to be strong, weak passwords can be compromised in many ways.	
Remediation:	
Investigate all accounts with passwords set to never expire and configure them to expire regularly if your company enforces these policies or make sure the passwords were created to be strong. If they are not, make the passwords strong following the minimum standard of 12 alphanumeric/symbol characters that are completely unique.	
☐ DOMAIN.LOCAL\service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name	☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name ☐ DOMAIN.LOCAL\ service account name

Upgrade Computer Operating Systems in Extended Support

Priority Rating	**Low**
Description:	
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.	
Remediation:	

Upgrade computers that have operating systems in Extended Support before end of life. The following machines are in Extended Support.	
☐ GENERIC PC / 10.10.10.5/ Windows Server 2012 R2 Standard ☐ GENERIC PC / ::10.10.10.5/ Windows Server 2012 R2 Standard ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / ::1,10.10.10.5/ Windows Server 2012 R2 Standard ☐ GENERIC PC / 10.10.10.5/ Windows Server 2012 R2 Standard ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC /10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter	☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC /10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Standard ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Standard ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / f10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5 / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / 10.10.10.5/ Windows Server 2012 R2 Standard ☐ GENERIC PC / ::1,10.10.10.5/ Windows Server 2012 R2 Standard ☐ GENERIC PC / 10.10.10.5/ Windows Server 2012 R2 Standard ☐ GENERIC PC / ::1,10.10.10.5 / Windows Server 2012 R2 Standard

Investigate the List of Inactive Computers

Priority Rating	**Low**
Description:	
Computers have not checked in during the past 30 days	
Remediation:	
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. Create a	

schedule to review these items and act accordingly. The following machines have not checked in, in 30 days or more:

☐ GENERIC PC/ / Windows 2000 Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PCM / / Windows Server 2008 R2 Standard	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC01 / / Windows Server 2012 R2 Standard	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows 2000 Professional	☐ GENERIC PC/ / Windows 10 Pro for Workstations
☐ GENERIC PC/ / Windows 2000 Professional	☐ GENERIC PC/ / Windows 7 Professional
☐ GENERIC PCTEST / / Windows Server 2012 R2 Standard	☐ GENERIC PC / / Windows 10 Pro
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC / / Windows 2000 Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC / /	☐ GENERIC PC/ 10.10.10.5/ Windows Server 2008 R2 Datacenter
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows 10 Pro
☐ SIMPLEX / / Windows Server 2003	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows 2000 Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PCP / / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC01 / / SLES	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows 2000 Server	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC / / Windows 7 Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ Windows 7 Ultimate	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / SLES	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC / / Windows Server 2003	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows 2000 Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC / / Windows XP Professional	☐ GENERIC PC/ / Windows 10 Pro
☐ GENERIC PCP01 / / Windows Server 2012 R2 Standard	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC / / Windows Server 2003	☐ GENERIC PC/ / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows Server 2008 R2 Standard	☐ GENERIC PC/ / Windows Storage Server 2012 Workgroup
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC/ / Windows 10 Pro for Workstations
☐ GENERIC PC/ / Windows 7 Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC/ / Windows XP Professional	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter
☐ GENERIC PC / / Windows XP Professional	
☐ GENERIC PC/ / Windows XP Professional	
☐ GENERIC PC/ / Windows XP Professional	
☐ GENERIC PC/ / Windows XP Professional	

☐ GENERIC PC/ / Windows XP Professional ☐ GENERIC PCL / / Windows 7 Enterprise ☐ GENERIC PC1 / / Windows 8 Enterprise ☐ GENERIC PC/ / Windows 7 Professional ☐ GENERIC PC/ / Windows 7 Professional ☐ GENERIC PCES-W7 / / Windows 7 Professional ☐ GENERIC PC / / Windows 7 Professional ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC/ / Windows 10 Pro for Workstations ☐ GENERIC PC/ / Windows 10 Pro for Workstations	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC/ / Windows 10 Pro for Workstations ☐ GENERIC PC/ / Windows 7 Professional ☐ GENERIC PC/ / Windows 10 Pro for Workstations ☐ GENERIC PC / / Windows 10 Pro ☐ GENERIC PC / / Windows 10 Pro ☐ GENERIC PC/ / Windows 10 Pro ☐ GENERIC PC / / Windows 10 Pro ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC/ / Windows 10 Pro ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2

	☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC / / Windows Server 2012 R2 Datacenter ☐ GENERIC PC/ / Windows Server 2012 R2 Datacenter

Disable or Remove Inactive User Accounts

Priority Rating	Low
Description:	
Users have not logged on to domain in 30 days. A user that has not logged in for an extended period could be a former employee or vendor. Accounts left active could create opportunity for malicious use if they are not monitored. Systematic reviews of Active Directory should be conducted to eliminate these accounts.	
Remediation:	
Disable or remove user accounts for users that have not logged on to active directory in 30 days. Create a schedule to have accounts reviewed periodically to reduce active accounts. The following user accounts have not logged on to Active Directory in 30 days:	
☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name	☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name ☐ username / User's name

Investigate Insecure Listening Ports on Machines

Priority Rating	Low

Description:
Devices are using potentially insecure protocols.
Remediation:
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 Excel Spreadsheet for details.
Short-Term Objectives:
Using the Listening Ports Sheet located in the Network Folder of the Assessment Package investigate the ports listed for each machine and determine their necessity.
References:
Listening Ports Excel Spreadsheet located in Network Folder of the Assessment Package

Remove or Populate Empty Organizational Units

Priority Rating	Low
Description:	
Empty organizational units (OU) were found in Active Directory. They may not be needed and can lead to misconfiguration.	
Remediation:	
Remove or populate empty organizational units. Keeping Active Directory maintained helps to avoid misconfigurations and incorrect policy application.	
☐ GENERIC OU / OU=GENERIC OU, OU=Computers, OU= GENERIC OU, DC=DOMAIN, DC=local ☐ GENERIC OU / OU= GENERIC OU, DC=DOMAIN, DC=local ☐ GENERIC OU / OU= GENERIC OU, OU= GENERIC OU, DC=DOMAIN, DC=local	☐ GENERIC OU / OU= GENERIC OU, OU= GENERIC OU, DC=DOMAIN, DC=local ☐ GENERIC OU / OU= GENERIC OU, OU=GENERIC PC, DC=DOMAIN, DC=local ☐ GENERIC OU / OU= GENERIC OU, DC=DOMAIN, DC=local

Cloud Recommendations

High-Priority Recommendations

Customer Lockbox Not Enabled

Priority Rating	High
Description:	
Unimplemented Microsoft Control: Customer Lockbox Not Enabled.	
Remediation:	

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.
Short-Term Objectives:
For companies that would like to activate the Customer Lockbox feature, one of the following license levels are needed. Licensed users of Office 365 E5, Microsoft 365 E5, Microsoft 365 E5 Compliance, and the Office 365 Advanced Compliance are entitled to receive the benefit of Customer Lockbox
References:
https://itblog.ldlnet.net/wp-content/uploads/2019/06/Guide-to-MS-O365-Licensing.pdf

Self-Service Password Reset

Priority Rating	**High**
Description:	
Unimplemented Microsoft Control: Self Service Password Reset. See Risk Report or Management Plan for recommendations. You have 44 of 68 users who don't have self-service password reset enabled.	
Remediation:	
With self-service password reset in Azure Active Directory, users no longer need to engage help desk to reset passwords. This feature works well with Azure AD dynamically banned passwords, which prevents easily guessable passwords from being used.	
Short-Term Objectives:	
Companies wishing to implement Self Service Password Reset need one of the following licenses: **For Cloud Only Password Change** – Azure AD Free, M365 Business Standard, M365 Business Premium, Azure AD P1 or P2 **For Cloud Only Password Reset** - M365 Business Standard, M365 Business Premium, Azure AD P1 or P2 **For Hybrid User Password Change or Reset with on-prem writeback** - M365 Business Premium, Azure AD P1 or P2	
References:	
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-licensing	

Block Legacy Authentication

Priority Rating	**High**
Description:	
Unimplemented Microsoft Control: Block Legacy Authentication. See Risk Report or Management Plan for recommendations. You have 68 of 68 users that don't have legacy authentication blocked.	
Remediation:	
Today, most compromising sign-in attempts come from legacy authentication. Older office clients such as Office 2010 don't support modern authentication and use legacy protocols such as IMAP,	

SMTP, and POP3. Legacy authentication does not support multi-factor authentication (MFA). Even if an MFA policy is configured in your environment, bad actors can bypass these enforcements through legacy protocols.
Short-Term Objectives:
If you are using **Azure Active Directory Free** versions with Office 365 or other SAAS/Web applications integrated with Azure Active Directory, then we suggest you enable “security defaults” “Security defaults” achieves multiple objectives: 1. Requiring all users to register for Azure AD Multi-Factor Authentication. 2. Requiring administrators to do multi-factor authentication. 3. Blocking legacy authentication protocols. 4. Requiring users to do multi-factor authentication when necessary. 5. Protecting privileged activities like access to the Azure portal.
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

Integrated Applications

Priority Rating	**High**
Description:	
Unimplemented Microsoft Control: Integrated Apps.	
Remediation:	
Tighten the security of your services by regulating the access of third-party integrated apps. Only allow access to necessary apps that support robust security controls. Third-party applications are not created by Microsoft, so there is a possibility they could be used for malicious purposes like exfiltrating data from your tenancy. Attackers can maintain persistent access to your services through these integrated apps, without relying on compromised accounts.	
Short-Term Objectives:	
To prevent users in your organization from allowing third-party apps to access their Office 365 information and require future consent operations to be performed by an administrator, go to the Azure Active Directory admin center > Enterprise applications > User settings > Enterprise applications. Set the toggle "Users can consent to apps accessing company data on their behalf" to **No**. Optionally, you can set up a process for your users to request access to third-party applications. In the Azure portal, configure an admin consent workflow by going to Enterprise applications > User settings. Under Admin consent requests, set "Users can request admin consent to apps they are unable to consent to" to **Yes**. Select your preferences for the rest of the admin consent requests options. Select **Save**. It can take up to an hour for the feature to become enabled.	
References:	

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent?tabs=azure-portal

Calendar Sharing with External Users

Priority Rating	**High**
Description:	
Unimplemented Microsoft Control: External Calendar Sharing	
Remediation:	
Users should not be allowed to share the full details of their calendars with external users.	
Short-Term Objectives:	
1. In the Microsoft 365 Exchange admin center, go to **Organization > Sharing.** 2. Under **Organization Sharing**, make sure **all policies** are unticked.	
References:	
https://docs.microsoft.com/en-us/exchange/sharing/organization-relationships/organization-relationships	

Disallow Addition of Domains to Allowed Domains

Priority Rating	**High**
Description:	
Unimplemented Microsoft Control: Ensure that there are no sender domains allowed for Anti-spam policies	
Remediation:	
Never add your own accepted domains or common domains to the allowed domains list for Anti-spam. If these domains are allowed to bypass spam filtering, attackers will be able to easily send emails into your organization.	
Short-Term Objectives:	
Remove all allowed domains from all your inbound Anti-spam policies.	
References:	
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide	

Microsoft Defender for Office 365

Priority Rating	**High**
Description:	
Turn on Microsoft Defender for Office 365 in SharePoint, OneDrive, and Microsoft Teams.	
Remediation:	

Microsoft Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams protects your organization from inadvertently sharing malicious files. There are other products that a company may be using for protection, such as Trend Micro Cloud App Security.
Short-Term Objectives
A license to a Microsoft 365 security product generally entitles you to use Microsoft 365 Defender without additional licensing cost. We do recommend getting a Microsoft 365 E5, E5 Security, A5, or A5 Security license or a valid combination of licenses that provides access to all supported services.
Mid-Term Objectives:
Ensure that the following global tenant setting for **'Safe Attachments'** is **enabled**: • Turn on the Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams
References:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/turn-on-mdo-for-spo-odb-and-teams?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/security/defender/m365d-enable?view=o365-worldwide

Turn ON Safe Attachments in Block Mode

Priority Rating	**High**
Description:	
Unimplemented Microsoft Control: Turn on safe attachments in block mode	
Remediation:	
Safe Attachments in block mode prevents messages with detected malware attachments from being delivered. These messages are quarantined and only admins (not regular users) can review, release, or delete them. This will also automatically block future malware attachments.	
Short-Term Objectives:	
Ensure that all users have an assigned 'Safe Attachments' policy in **Block mode** by either updating your existing policies or creating new ones.	
References:	
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-safe-attachments-policies?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/security/defender/m365d-enable?view=o365-worldwide	

Safe Documents Protection

Priority Rating	**High**
Description:	
Unimplemented Microsoft Control: Turn on safe documents for clients	
Remediation:	

Safe Documents uses Microsoft Defender for Endpoint to scan documents and files for malicious content. To keep you protected, Safe Documents sends files to the Defender for Endpoint cloud for analysis. Files sent by Safe Documents are not retained in Defender for Endpoint beyond the time needed for analysis (typically, less than 24 hours).
Short-Term Objectives:
Licenses Required for Safe Documents • Microsoft 365 A5 for Faculty • Microsoft 365 A5 for Students • Microsoft 365 E5 • Microsoft 365 E5 Security
Mid-Term Objectives:
Ensure that the global tenant settings for '**Safe Attachments'** are configured as follows: • 'Turn on Safe Documents for Office clients**'** should be **Turned On** • Allow people to click through Protected View even if Safe Documents identified the file as malicious' should be **Turned Off**
References:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-docs?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/security/defender/m365d-enable?view=o365-worldwide

Safe Links Protection

Priority Rating	**High**
Description:	
Unimplemented Microsoft Control: Create safe links policies for email messages	
Remediation:	
Safe Links protection for links in email messages is controlled by Safe Links policies. There is no default Safe Links policy, so to get the protection of Safe Links in email messages, you need to create one or more Safe Links policies.	
Short-Term Objectives:	
Licensed users of Enterprise Mobility + Security E5, Microsoft 365 E5, Microsoft 365 E5 Security, and Azure Advanced Threat Protection for Users are entitled to receive the benefit of Azure ATP.	
Mid-Term Objectives:	
Ensure that all users have an assigned **Safe Links** policy, by either updating your existing policies or creating new ones, with the following settings configured: • **Select the action for unknown potentially malicious URLs in messages:** On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link. • **Apply Safe Links to email messages sent within the organization**: Select this setting to apply the Safe Links policy to messages between internal senders and internal recipients.	

References:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-safe-links-policies?view=o365-worldwide#use-the-microsoft-365-defender-portal-to-create-safe-links-policies https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-safe-links-policies?view=o365-worldwide#use-exchange-online-powershell-or-standalone-eop-powershell-to-configure-safe-links-policies

Turn On User Risk Policy

Priority Rating	High
Description:	
Unimplemented Microsoft Control: User Risk Policy	
Remediation:	
With the user risk policy turned on, Azure Active Directory detects the probability that a user account has been compromised. As an administrator, you can configure a user risk conditional access policy to automatically respond to a specific user risk level. For example, you can block access to your resources or require a password change to get a user account back into a clean state.	
Short-Term Objectives:	
License Required: Azure AD Premium P2	
Mid-Term Objectives:	
In Azure AD Identity Protection you can configure the user risk remediation policy. For the users in this policy, you need to set the conditions (risk level) under which the policy triggers and whether access is blocked when the policy is triggered. Switch the state of the policy to **ON**.	
Long-Term Objectives:	
References:	
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection	

Sign In Risk Policy

Priority Rating	High
Description:	
Unimplemented Microsoft Control: Sign in Risk Policy	
Remediation:	
Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication (MFA).	
Short-Term Objectives:	
License Required: Azure AD Premium P2	
Mid-Term Objectives:	
In Azure AD Identity Protection, you can configure the sign-in risk remediation policy. For the users in this policy, you need to set the conditions (risk level) under which the policy triggers. Switch the state	

of the policy to **ON**. It is important to configure the MFA registration policy for all users who are a part of the sign-in risk policy to ensure that they have registered MFA.
References:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

Security Recommendations

High-Priority Recommendations

Ensure All Compromised Passwords are No Longer in Use

Priority Rating	**High**
Description:	
A scan of the Dark Web revealed one or more compromised passwords from your domain. The most recent compromise occurred in 2022.	
Remediation:	
Refer to Appendix A, the Darkweb Compromise Report. Ensure the compromised passwords are no longer in use. We recommend having all users reset their password as the extent of the compromise is difficult to assess.	
Short-Term Objectives:	
After all users have verified that all compromised passwords have been corrected with strong unique passwords, CTG recommends 12 characters minimum, alphanumeric/symbols and completely unique. No names, dates, addresses, words at all. The company should then look to sign up with a proactive Darkweb monitoring service.	
References:	
https://ctgusa.net/services/dark-web-scan/	

Enable Account Lockout for All Users

Priority Rating	**High**
Description:	
Account lockout (disabling an account after several failed attempts) significantly reduces the risk of an attacker acquiring a password through a brute force attack.	
Remediation:	
Enable account lockout for all users.	
Short-Term Objectives:	
The Account Lockout Policy settings can be configured in the following location in the Group Policy Management Console: **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy**.	
References:	

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy

Enable Enforcement of Password Length

Priority Rating	**High**
Description:	
Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.	
Remediation:	
Enable enforcement of password length to more than 8 characters. The 8-character length is a Microsoft standard and is no longer adequate per most security experts. CTG recommends 12 characters minimum, alphanumeric/symbols and completely unique. No names, dates, addresses, words at all.	
Short-Term Objectives:	
The Minimum Password Length settings can be configured in the following location in the Group Policy Management Console: **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**	
References:	
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/minimum-password-length	

Enable Password Complexity for All Users

Priority Rating	**High**
Description:	
Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.	
Remediation:	
Enable password complexity to assure that network user account passwords are secure.	
Short-Term Objectives:	
The Password must meet complexity requirements settings can be configured in the following location in the Group Policy Management Console: **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**	
References:	
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements	

Increase Password History to Remember at Least 6 Passwords

Priority Rating	High
Description:	
Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.	
Remediation:	
Increase password history to remember at least six passwords. Microsoft password standards are not in line with NIST standards. NIST password best practice no longer supports frequent password changes. NIST standards now support long, unique, multi-character set passwords that don't change. Some compliance regulations still require expiring passwords; therefore, this policy is included.	
Short-Term Objectives:	
The Enforce Password History settings can be configured in the following location in the Group Policy Management Console: **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**	
References:	
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/enforce-password-history	

Medium-Priority Recommendations

Enable Automatic Screen Lock

Priority Rating	Medium
Description:	
Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.	
Remediation:	
Enable automatic screen lock on the specified computers.	
Short-Term Objectives:	
Interactive logon: Machine inactivity limit settings can be configured in the following location in the Group Policy Management Console: **User Configuration\Administrative Templates\Control Panel\Personalization\Enable screen saver**. **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options** **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options (While creating and linking group policy on server)**	
References:	
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-inactivity-limit	

Eliminate Inconsistencies and Exceptions Password Policy

Priority Rating	Medium
Description:	
Password policies are not consistently applied from one computer to the next. A consistently applied password policy ensures adherence to password best practices.	
Remediation:	
Eliminate inconsistencies and exceptions to the password policy. See Appendix C: Security Policy Assessment report for policy details. If there are reasons why all machines are not under the same password policy, analyze the needs and correct as needed.	
Short-Term Objectives:	
Review the Security Policy Assessment document under Password Policy and determine if machines not matching the password policies need to be corrected.	

Low-Priority Recommendation

Ensure Company WIFI is Secure, Don't Use Open WIFI Connections

Priority Rating	Low
Description:	
Open or insecure WIFI protocols may allow an attacker access to the company's network and resources.	
Remediation:	
Ensure company's WIFI is secure and discourage the use of any open WIFI connections. Verify that all WIFI networks with access to corporate resources are using WPA2 with either a pre shared key or 802.1X. Verify any guest networks cannot access the corporate network via any protocol.	
Short-Term Objectives:	
Securing corporate WIFI networks with WPA2, strong pre shared keys, and VLANs are the first step in securing wireless.	
Mid-Term Objectives:	
Additional methods such as using 802.1X with a Radius server such as Microsoft NPS can add a layer of authentication to the WIFI security strategy. Tunneling guest networks directly to the firewall can also help segregate traffic in an easy manner.	
References:	
https://www.cisa.gov/uscert/ncas/tips/ST05-003	