assess365

softwerx
The Microsoft Security Specialists

Cybersecurity QuickScan Report

Sample Ltd

Table of Contents

1 Management Summary

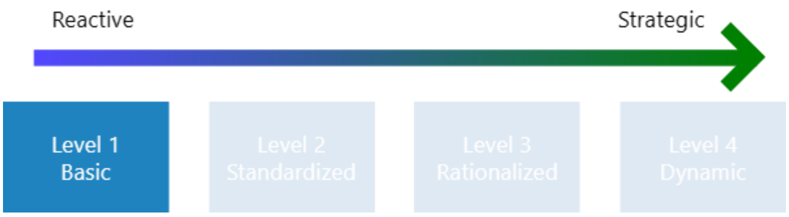
This document is part of the cybersecurity QuickScan assessment that was carried out in March 2024 for Example Ltd by Softwerx Ltd. It provides an overall review regarding your cybersecurity program and practices, as assessed through a questionnaire and through an automated scan of security related data and deployed settings.

The report is not meant to serve as a detailed control review nor a security audit, although it can serve to prepare you for it. In addition, the outcomes of the assessment can be used as input for an action plan to mitigate the discovered risks, enhancing your organization's security posture and cybersecurity resilience. More information about the CSAT methodology can be found in Appendix B.

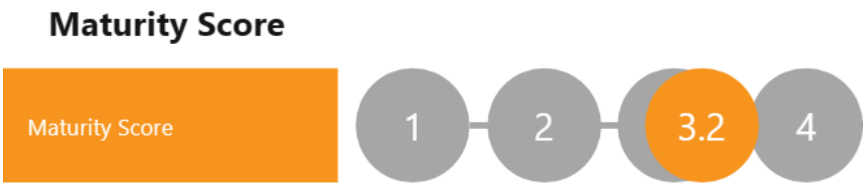
1.1 Organization's Maturity Level

Security is like water, finding the path of least resistance. Hackers will break into a system as quietly and with as little effort as possible. Therefore, it is important to look at the lowest scoring controls as well as the overall average score.

After reviewing the Security Control Domains, described in detail later, the current overall maturity level of Example Ltd 's cybersecurity program and practices matches level 1 - basic. Your organization's maturity level is based on the lowest scored security control answer, gathered during the interview with your security team.



The maturity rating is calculated based on the average of all rated answers in the questionnaire. This score can be used as a benchmark for future assessments based on QuickScan assessment. Your current maturity score is shown below.



The organization's size, industry, regulatory requirements, and other risk factors influence the final recommendations associated with this global rating. Among others, your cybersecurity situation implicates the following:

- Patch management of core software (Microsoft) is well automated and enforced through automated controls and monitoring. Other software is taken on an ad-hoc basis. The organization should consider introducing a more robust patching methodology to ensure critical security patches are deployed within 2 weeks of release or within 48 hours if an exploit exists.

- The security risks to the organization are generally understood, some automation is in place, however improvements can be made in regular reviews and reassessment of risk methodology.
- The is little control on the installation of browser plugins, email client plugins, and add-on applications.
- A process to implement the latest stable version of any security-related updates on all network devices is in place but not scheduled or based on risk.

1.2 Strategic Recommendations

The core business benefit of implementing the improvements mentioned in this document is that your organization establishes better resilience against today's security threats, the connected compliancy risks, and therefore a higher maturity level.

Organizations should be proactive and programmatic to mitigate cybersecurity threats. Establishing policies and procedures, implementing, and governing them enables your business achieving their goals while protecting the organization's assets. A proactive approach as opposed to reactive mitigation of incidents is key to improve your position. This approach is generally in place for Example Ltd. Improvements could be made in the areas of Data Retention and Secure Data Disposal,

Risk management is another key element too. It is necessary to take the appropriate steps to identify the risks to protect, detect, and respond to them. Modern security risk management is a boardroom topic and requires executive leadership participation as key stakeholder in the process.

In the next chapter, the Plan of Approach highlights a bird's eyes view of the actions that should be taken. They are based on industry controls, architectures and recommendations as explained in chapter 3. Detailed assessment outcomes and recommendations are explained in the chapters following that.

2 Suggested Plan of Approach

The following is our suggestion to start mitigating security risks, considering recommended practices.

The approach is threefold. The first phase is focused to enable the so-called ‘low-hanging fruit’ features (features that are relatively easy to implement, yet with high impact on preventing security incidents). It also focuses on rejuvenating your security strategy. The second phase focuses on features that further harden your IT environment, and on implementing governance and reporting features. The third phase covers the creation/revision of processes, and implementation of solutions that take a longer preparation time.

For your environment we suggest the following Plan of Approach:

2.1 Phase 1 | 0-30 days

The following list are quick wins that can be considered for implementation by Example Ltd. Overview of the advised actions and products:

Topic	Action	Associated software products	ZTA zone
Quick Wins			
(Azure) Active Directory Accounts	• Disable old/unused accounts. • Review the reasons behind Multi Factor Authentication (MFA) not being enabled for all user accounts. Enable where feasible or ensure that further controls (such as location restriction) are in place where this is not possible. • Review external users and enforce Multi Factor Authentication for the external users	• Microsoft Entra ID Multi Factor Authentication • Microsoft Entra ID Conditional Access • Microsoft Entra ID	0 1
Administrators	• Implement a process to regularly review administrator accounts and clean up old/unused accounts. • Ensure admin roles are only placed on admin accounts and not on normal user accounts	• Microsoft Entra ID Privileged Identity Management (PIM)	0 1
Change default passwords	• Ensure all default passwords on all services and devices are changed. • Implement Local Account Password Solutions (LAPS) for local admin accounts	•	1 2 6 7
Applications	• Ensure that all applications are kept to up to date. • Integrate all detected application with Microsoft Entra ID and enable Single Sign On where possible	• Microsoft Intune • Microsoft Defender for Cloud Apps • Microsoft Entra ID	2 3 5
Email Protection	• Implement the DMARC record	•	4
Antivirus	• Update the out-of-date antivirus definitions	• Defender for Endpoint	2 3
Protect your Sensitive assets	• Ensure all privileged users are using dedicated machines for administrative tasks	• Secure Azure managed workstation	1 2

2.2 Phase 2 | 30-90 days

To provide you with a condensed overview of most urgent findings for 30-90 days, we assembled them here. For detailed information, refer to the respective topics in chapter 4. We recommend reviewing the items and, depending on your risk appetite and budget priorities, to add your choices to the beforementioned plan of approach or roadmap/project plan.

Topic	Action	Associated Software Products
Urgent (30-90)		
Data Management	- Define an information classification policy.	- Microsoft Information Protection (MIP) - Windows Information Protection (WIP)

2.3 Phase 3 | 90+ days

To provide you with a condensed overview of most urgent findings for 90+ days, we assembled them here. For detailed information, refer to the respective topics in chapter 4. We recommend reviewing the items and, depending on your risk appetite and budget priorities, to add your choices to the beforementioned plan of approach or roadmap/project plan.

Topic	Action	Associated Software Products
Urgent (90+)		
Data Management	- Enforce an information classification policy with the use of Microsoft Information Protection (MIP) and/or Windows Information Protection (WIP) in Windows 10.	- Microsoft Information Protection (MIP) - Windows Information Protection (WIP)

3 Cybersecurity Findings and Recommendations

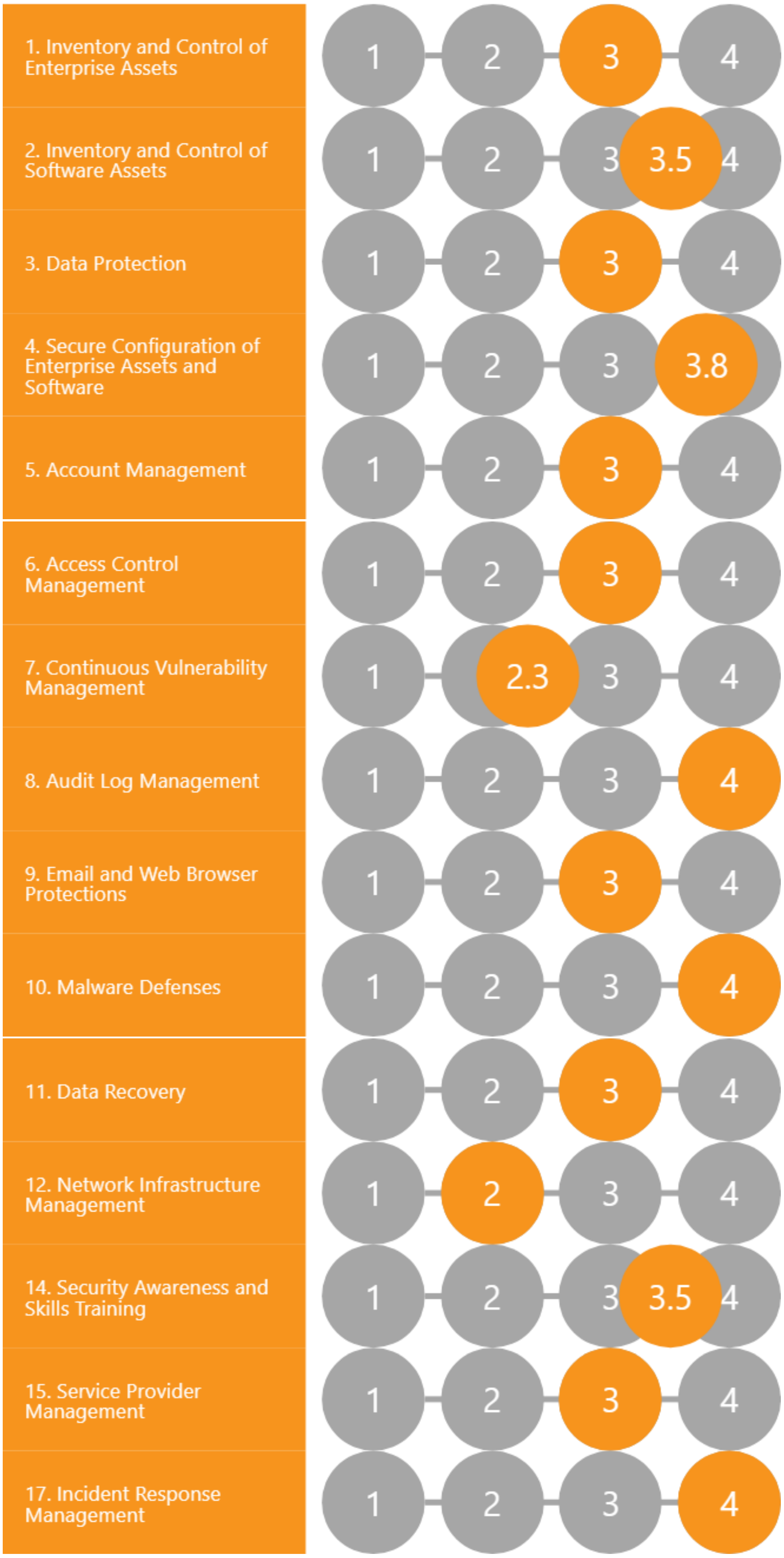
Besides the all-up maturity score, the ratings associated with the CIS Controls™ (v8.0) give a more detailed insight about how the current policies, procedures and management are organized.

This chapter reveals the respective ratings based on the interview we had with your security/IT staff. A rating represents the current situation; depending on your strategy, policies, risk appetite and/or regulatory requirements, the results can be interpreted as identifier which topics your team should address to improve your security rating in the next assessment.

3.1 CIS Controls - Rating

Based on the provided answers regarding the CIS controls, your current rating is stated in the below graphic.

CIS v8


1. Inventory and Control of Enterprise Assets
1 2 **3** 4
2. Inventory and Control of Software Assets
1 2 3 **3.5** 4
3. Data Protection
1 2 **3** 4
4. Secure Configuration of Enterprise Assets and Software
1 2 3 **3.8**
5. Account Management
1 2 **3** 4
6. Access Control Management
1 2 **3** 4
7. Continuous Vulnerability Management
1 **2.3** 3 4
8. Audit Log Management
1 2 3 **4**
9. Email and Web Browser Protections
1 2 **3** 4
10. Malware Defenses
1 2 3 **4**
11. Data Recovery
1 2 **3** 4
12. Network Infrastructure Management
1 **2** 3 4
14. Security Awareness and Skills Training
1 2 3 **3.5** 4
15. Service Provider Management
1 2 **3** 4
17. Incident Response Management
1 2 3 **4**

3.1.1 CIS Controls - Findings and Recommendations

The following action items apply to enhance your position with regards to the CIS controls. The number mentioned in the topic column correlates to the respective control.

High					
Topic	**Question**	**Answer**	**Advice**	**Advised Products**	**ZTA Zone**
3. Data Protection	How is your data management process organized regarding data retention and secure data disposal?	Standardized (2) A data retention and disposal process has been established. The process is invoked manually.	Ensure in the data retention process includes both the minimum and maximum timelines. Review the process at least once a year. Implement the policy on your storage assets to prevent unwanted data loss, and configure data automated data disposal when available.	Purview Data Map; Purview Data Catalog; Azure Files; Azure Backup; Azure Disaster Recovery; Purview Data Lifecycle Management	0, 3, 4
7. Continuous Vulnerability Management	Has your organization implemented risk management processes to address: identification and classification of potential risks; mitigation controls (measures taken to reduce risk); acceptance/transfer of remaining (residual) risks after mitigation steps have been applied?	Standardized (2) Risk assessments are executed on ad-hoc basis. Risks are recorded in a register.	Improve the risks assessment process to be executed on a monthly, or more frequent basis	Purview Compliance Manager [enables workflow based risk assessments and offers template for CIS assessments]; Purview Insider Risk Management (E5 Compliance); Defender Cloud Security	0, 3

				Posture Management	
7. Continuous Vulnerability Management	Do you have an automated patch management solution implemented to continuously update all the organization's systems and applications?	Standardized (2) A manual patch management strategy for user endpoints and software is in place and executed monthly. Critical security hotfixes are applied within one month of release.	Implement a patch management process, adopting the recommended practices of the respective vendor. Implement tools to control and automatically update all systems, in a secure and effective manner. Use the tools that are included in your cloud environment to monitor the current health status of your environment.	Microsoft Intune; Windows Server Update Services [WSUS]; Defender for Cloud; Defender Cloud Security Posture Management	2, 3, 5, 6
9. Email and Web Browser Protections	How are users prevented from installing unauthorized browsers, browser plugins, email client plugins, and add-on applications?	Standardized (2) Users are made aware to not install unauthorized browsers, browser plugins, email client plugins, and add-on applications. Tooling is used to ensure only full supported browsers and email clients are used.	Enforce a policy that only allows approved browser and email client plugins, and add-on applications to be installed.	Microsoft Intune; Defender for Endpoint	2, 3, 5

12. Network Infrastructure Management	What is the process to implement the latest stable version of any security-related updates on all network devices?	Standardized (2) A process is in place but is not scheduled or based on risks.	Schedule the execution of the update process for network devices, at least on a monthly basis.	Network Device Management Solution	0, 7

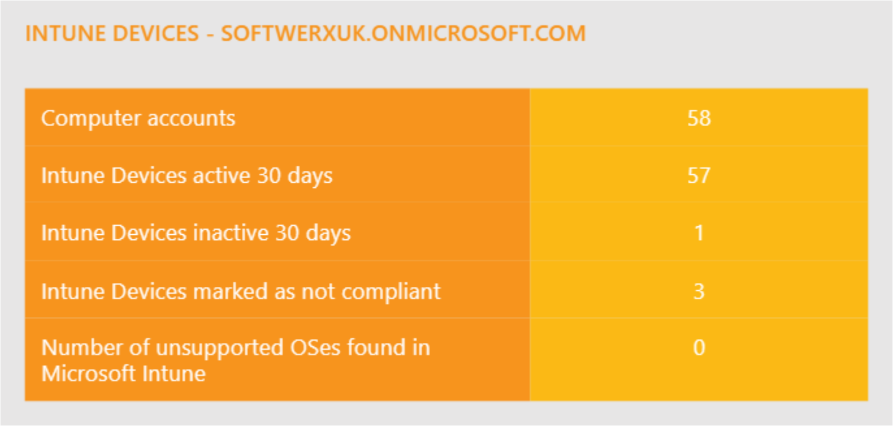
4 Technical Data and Analysis

Besides the interview with regards to the security controls, we conducted an automated scan throughout (a selection of) your IT environment. We have collected information regarding, among others, the current state of configuration of your IT landscape, discovery of personal identifiable information, identity management, software versioning, and many more.

This chapter summarizes the facts we have found along with the respective security risk/threat and recommendations to remediate those vulnerabilities.

4.1.1 CIS Control 2: Inventory and Control of Software Assets

CSAT Output – Operating system version status



INTUNE DEVICES - SOFTWERXUK.ONMICROSOFT.COM

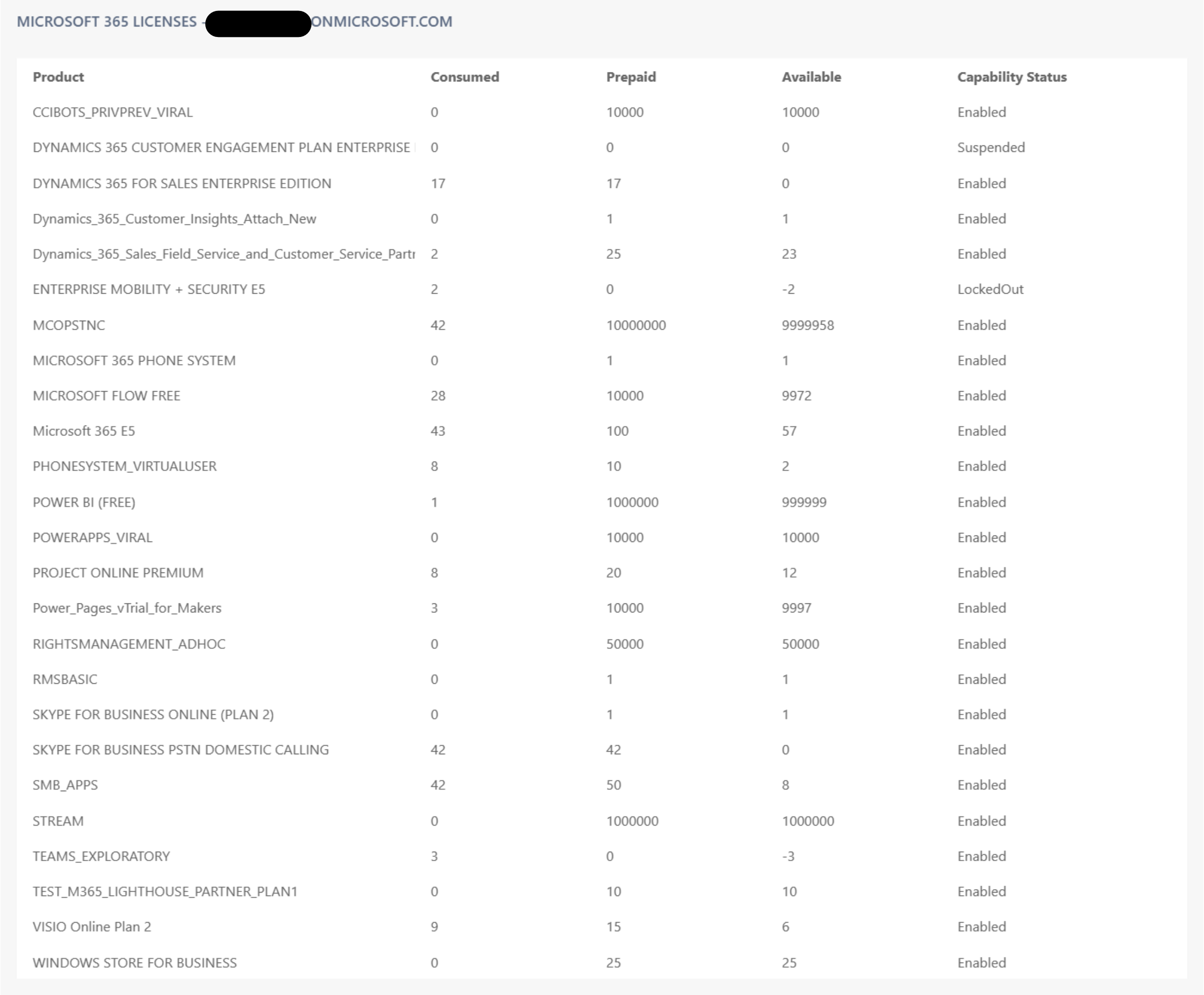
Computer accounts	58
Intune Devices active 30 days	57
Intune Devices inactive 30 days	1
Intune Devices marked as not compliant	3
Number of unsupported OSes found in Microsoft Intune	0

Conclusions and Recommendations

<u>Windows Operating Systems (OS)</u>

- Review Inactive devices. Locate and wipe where appropriate
- Configure reporting and remediation of non-compliant device. Apply conditional access rules to block non-compliant devices from accessing company data and services.

CSAT Output – Licensing Status

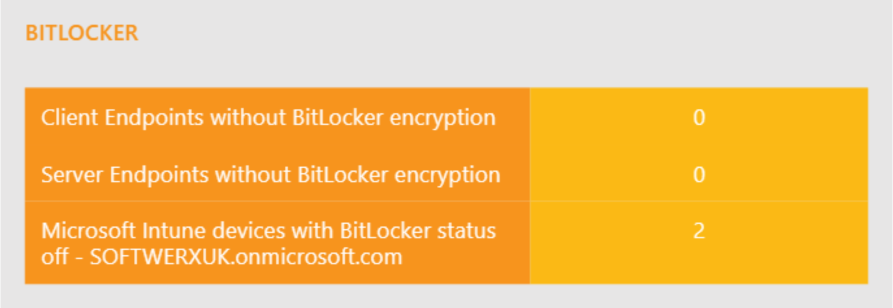


MICROSOFT 365 LICENSES - [redacted] ONMICROSOFT.COM

Product	Consumed	Prepaid	Available	Capability Status
CCIBOTS_PRIVPREV_VIRAL	0	10000	10000	Enabled
DYNAMICS 365 CUSTOMER ENGAGEMENT PLAN ENTERPRISE	0	0	0	Suspended
DYNAMICS 365 FOR SALES ENTERPRISE EDITION	17	17	0	Enabled
Dynamics_365_Customer_Insights_Attach_New	0	1	1	Enabled
Dynamics_365_Sales_Field_Service_and_Customer_Service_Partr	2	25	23	Enabled
ENTERPRISE MOBILITY + SECURITY E5	2	0	-2	LockedOut
MCOPSTNC	42	10000000	9999958	Enabled
MICROSOFT 365 PHONE SYSTEM	0	1	1	Enabled
MICROSOFT FLOW FREE	28	10000	9972	Enabled
Microsoft 365 E5	43	100	57	Enabled
PHONESYSTEM_VIRTUALUSER	8	10	2	Enabled
POWER BI (FREE)	1	1000000	999999	Enabled
POWERAPPS_VIRAL	0	10000	10000	Enabled
PROJECT ONLINE PREMIUM	8	20	12	Enabled
Power_Pages_vTrial_for_Makers	3	10000	9997	Enabled
RIGHTSMANAGEMENT_ADHOC	0	50000	50000	Enabled
RMSBASIC	0	1	1	Enabled
SKYPE FOR BUSINESS ONLINE (PLAN 2)	0	1	1	Enabled
SKYPE FOR BUSINESS PSTN DOMESTIC CALLING	42	42	0	Enabled
SMB_APPS	42	50	8	Enabled
STREAM	0	1000000	1000000	Enabled
TEAMS_EXPLORATORY	3	0	-3	Enabled
TEST_M365_LIGHTHOUSE_PARTNER_PLAN1	0	10	10	Enabled
VISIO Online Plan 2	9	15	6	Enabled
WINDOWS STORE FOR BUSINESS	0	25	25	Enabled

4.1.2 CIS Control 3: Data Protection

CSAT Output – BitLocker Encryption Status



BITLOCKER

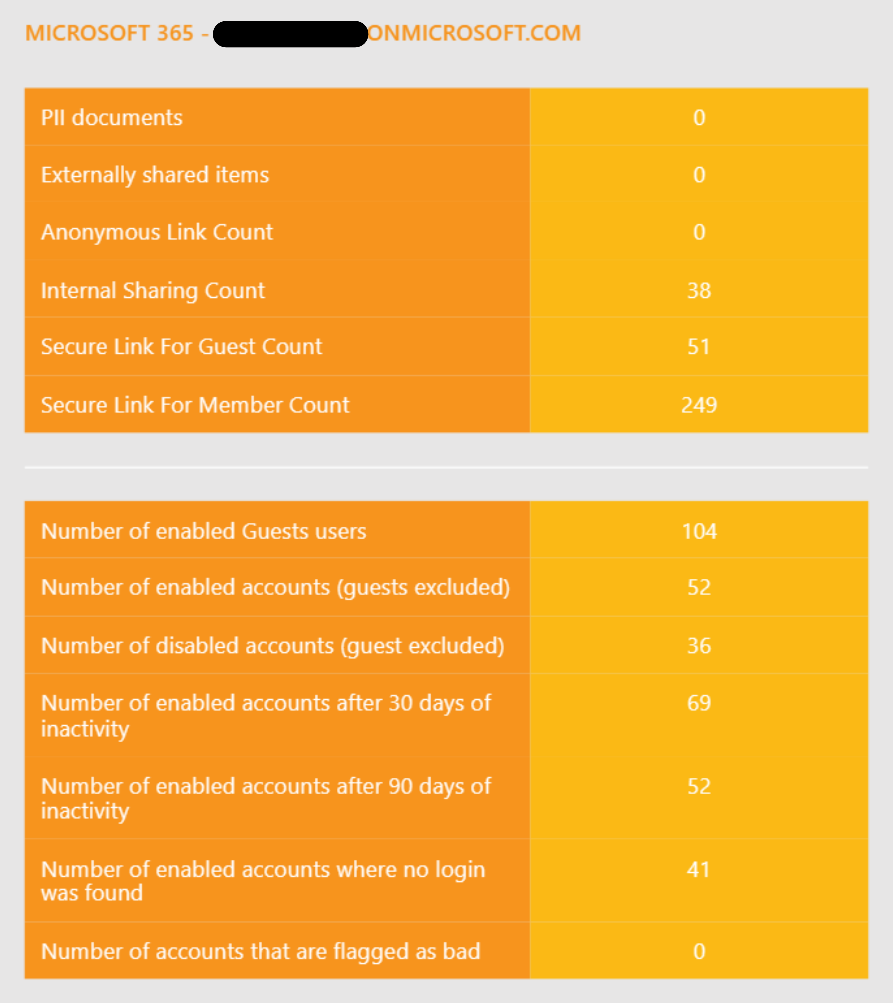
Client Endpoints without BitLocker encryption	0
Server Endpoints without BitLocker encryption	0
Microsoft Intune devices with BitLocker status off - SOFTWERXUK.onmicrosoft.com	2

Conclusions and Recommendations.

BitLocker Encryption

- **0** Client endpoints do not have BitLocker encryption enabled.
- **0** Server endpoints do not have BitLocker encryption enabled.

CSAT Output – Microsoft 365 overview



MICROSOFT 365 - [redacted]ONMICROSOFT.COM

PII documents	0
Externally shared items	0
Anonymous Link Count	0
Internal Sharing Count	38
Secure Link For Guest Count	51
Secure Link For Member Count	249

Number of enabled Guests users	104
Number of enabled accounts (guests excluded)	52
Number of disabled accounts (guest excluded)	36
Number of enabled accounts after 30 days of inactivity	69
Number of enabled accounts after 90 days of inactivity	52
Number of enabled accounts where no login was found	41
Number of accounts that are flagged as bad	0

4.1.3 CIS Control 4: Secure Configuration of Enterprise Assets and Software

CSAT Output – Endpoints Secure Configuration

Conclusions and Recommendations

<u>Operating system hardening baseline</u>

Hardening of systems is applied on Windows system. Network equipment doesn't follow recognized hardening benchmarks during deployment. CIS has various free benchmarks available on https://www.cisecurity.org/cis-benchmarks/.

Keep in mind to check for updates – especially every 6 months after the half-yearly release of Microsoft Intune Baselines. When using other Operating Systems, seek for similar baselines and create a process around it.

Microsoft Security Copilot, which is currently in Preview, can help to setup the correct policies for your organization. Microsoft Security Copilot can be used to detect hidden patterns, harden defenses, and respond to incidents faster with generative AI. To learn more about Microsoft Security Copilot visit https://learn.microsoft.com/en-us/security-copilot/?view=o365-worldwide.

4.1.4 CIS Control 5: Account Management

CSAT Output – Microsoft Entra ID Account status

Tenant Name	External User	Enabled User	Disabled User	Enabled User without MFA	O365 Audit log search
[redacted]onmicrosoft.com	104	60	40	7	Yes

Conclusions and Recommendations

Azure Active Directory Users

A strong, complex password is the first line of defense in protecting your accounts. MFA is a feature that requires the username and password, and one more verification method, to login to an account. This could for example be a randomly generated SMS-code, a phone call, a smart card (virtual or physical) or a biometric device. In case there are accounts (with MFA enabled) where usernames and passwords have been compromised, for example through phishing emails or brute force attacks, the attackers will not be able to gain access to the accounts, because they are not able to complete the second form of authentication. It is advised to implement MFA together with Conditional Access to protect your users, as this is highly effective at stopping attacks. Enforce it with **Azure MFA** and **Azure Active Directory Conditional Access**. By setting up a Conditional Access policy you can block access to resources for devices that exceed the threat level you set in your compliance policy.

During our analysis of your Microsoft 365 data, we identified that there are several disabled accounts. When an account is disabled, it still exists in the system, allowing for potential unauthorized access. Disabled accounts can be targeted by malicious actors who may attempt to exploit the account to gain access to sensitive data or resources. We recommend cleaning up these disabled accounts in your Microsoft 365 environment.

CSAT Output – Microsoft Entra ID – External Users

Conclusions and Recommendations

Microsoft Entra ID External Users

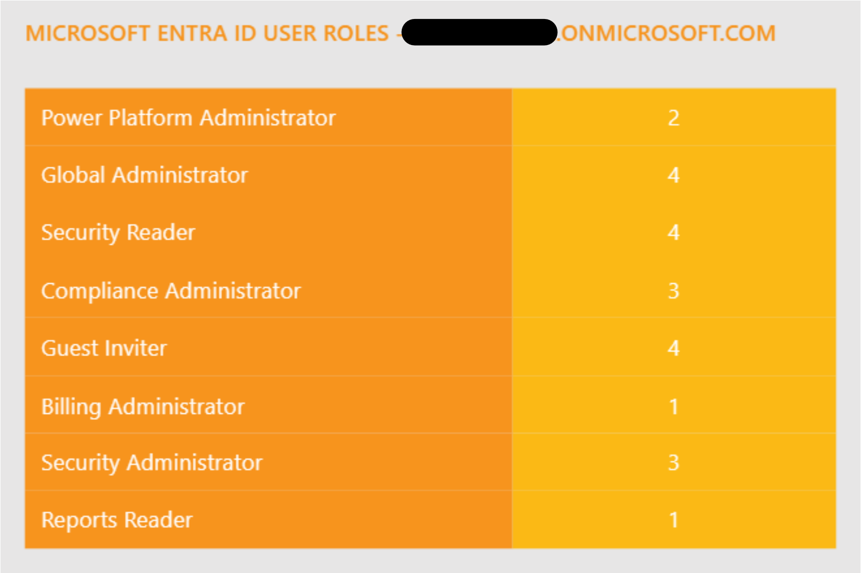
- There were external users found in Microsoft Entra ID that have been invited on their personal email account. Review these accounts and disable them where needed.

It is recommended to review the external users, and their access authorizations regularly. Especially users who have been invited on their personal email account, such as Outlook, Gmail, Hotmail, Yahoo mail etc. When these external users leave their organization, and your organization will not be notified, the users will still have access through their personal email account.

4.1.5 CIS Control 6: Access Control Management

CSAT Output – Microsoft Entra ID roles

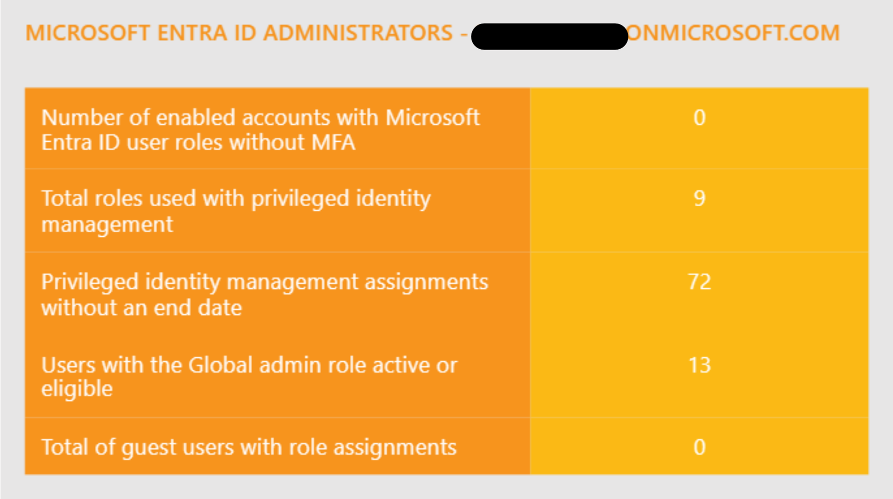
Roles are only shown if the role contains one or more members.



MICROSOFT ENTRA ID USER ROLES - [redacted].ONMICROSOFT.COM

Power Platform Administrator	2
Global Administrator	4
Security Reader	4
Compliance Administrator	3
Guest Inviter	4
Billing Administrator	1
Security Administrator	3
Reports Reader	1

CSAT Output – Microsoft Entra ID Administrators status



MICROSOFT ENTRA ID ADMINISTRATORS - [redacted]ONMICROSOFT.COM

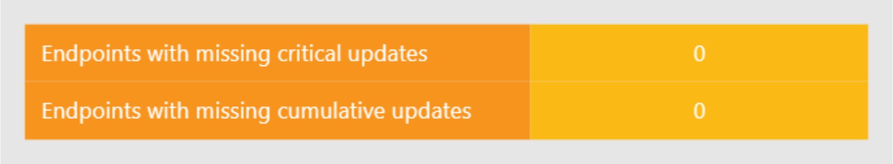
Number of enabled accounts with Microsoft Entra ID user roles without MFA	0
Total roles used with privileged identity management	9
Privileged identity management assignments without an end date	72
Users with the Global admin role active or eligible	13
Total of guest users with role assignments	0

Conclusions and Recommendations

Administrator accounts bring high risk to an organization's network, since they have access to your network, or systems and sensitive data. Therefore, it is recommended to limit the number of administrators as much as possible, and to enable **Multi Factor Authentication (MFA)** for all privileged accounts. Our advice is to implement a process to regularly review authorizations for privileged accounts. Avoid using on-premises synced accounts for cloud role assignments. If you are using a synced on-premises account, and that account is compromised, it can also compromise your cloud resources as well.

4.1.6 CIS Control 7: Continuous Vulnerability Management

CSAT Output – Update Status



Endpoints with missing critical updates	0
Endpoints with missing cumulative updates	0

Conclusions and Recommendations

- **0** Endpoints found with missing critical security patches.
- **0** Endpoints found with missing cumulative updates.

Operating Systems vulnerabilities are a potential security threat of the IT infrastructure. Especially if the security vulnerabilities are publicly known, attacking your organization through rapidly spreading mechanisms. It is recommended to establish a patch management process, adopting the publishing cycle for Microsoft security updates (patch Tuesday), and to enforce updating all your systems safely and effectively. It is also recommended to regularly gain insights on the patch status of all endpoints.

Microsoft Security Copilot, which is currently in Preview, has the capability to respond to your specific questions and suggest action to mitigate those concerns. For example, questions can be asked which devices are not compliant and a list of devices will be shown. Or if the Security Copilot can suggest policies to harden the organizations devices. To learn more about Microsoft Security Copilot visit https://learn.microsoft.com/en-us/security-copilot/?view=o365-worldwide.

4.1.7 CIS Control 8: Audit Log Management

No issues discovered

4.1.8 CIS Control 9: Email and Web Browser Protections

CSAT Output – Email authentication and DNS protection

Inventory	Value	Notes
Example.com		
DNSSec enabled	No	
SPF record	v=spf1 include:[redacted] include:marketing.dynamics.com include:eu._netblocks.mimecast.com include:spf.exclaimer.net include:servers.mcsv.net ip4:[redacted]-all	
DKIM record	selector1: v=DKIM1; k=rsa; n=[redacted]	
DMARC record	v=DMARC1; p=none; rua=mailto:[redacted]@rep.dmarcanalyzer.com; ruf=mailto:[redacted]@for.dmarcanalyzer.com; fo=1;	DMARC_POLICY_NOT_REJECT

Conclusions and Recommendations

Email Spoofing Protection

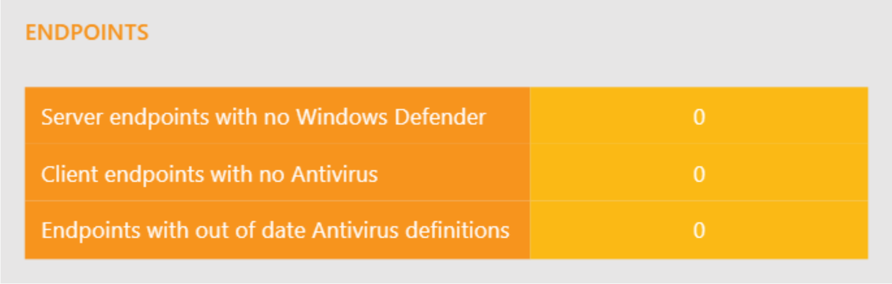
- **The DMARC record is setup without a policy**. The DMARC policy determines what will happen with the messages if the SPF and/or DKIM check fail. It is recommended to set the policy to ‘Reject’. With the reject policy the unauthorized mail will be dropped. This is key in the fight against spoofed messages. When the policy is set to p=none then DMARC is being checked, yet the receiving server will pass the message on to the mailbox, rendering the SPF and DKIM features useless.

We highly recommend implementing the appropriate **SPF, DKIM and DMARC** records to prevent unauthorized use of your email domain(s), enhancing protection from spam, fraud, and phishing senders masking their messages with your domain name(s). It will not only protect your own coworkers but also the recipients outside your organization.

> **Note**: Be aware that spoofers using the same domain name to send spoofed messages (like the commonly used cloud service providers) result in a 'pass' when your SPF record is checked, as it is mentioned in your SPF record. Hence, combine the SPF record with DKIM signatures and DMARC policy to enhance your protection against spoofers.

4.1.9 CIS Control 10: Malware Defenses

CSAT Output – Antivirus overview



ENDPOINTS

Server endpoints with no Windows Defender	0
Client endpoints with no Antivirus	0
Endpoints with out of date Antivirus definitions	0

Conclusions and Recommendations

- **0** Endpoints found with outdated antivirus definitions.
- **0** Endpoints found with disabled or no antivirus

CSAT is not utilized to collect antivirus status information of server endpoints that are not using Windows Defender. It is recommended to regularly check the antivirus status (using a centralized management tool) to ensure that all machines have an enabled and up-to-date antivirus running.

4.1.10 CIS Control 14: Security Awareness and Skills Training

The Cyber Security Assessment Tool does not provide technical data for this control, though the control is covered in the questionnaire interview.

Conclusions and Recommendations

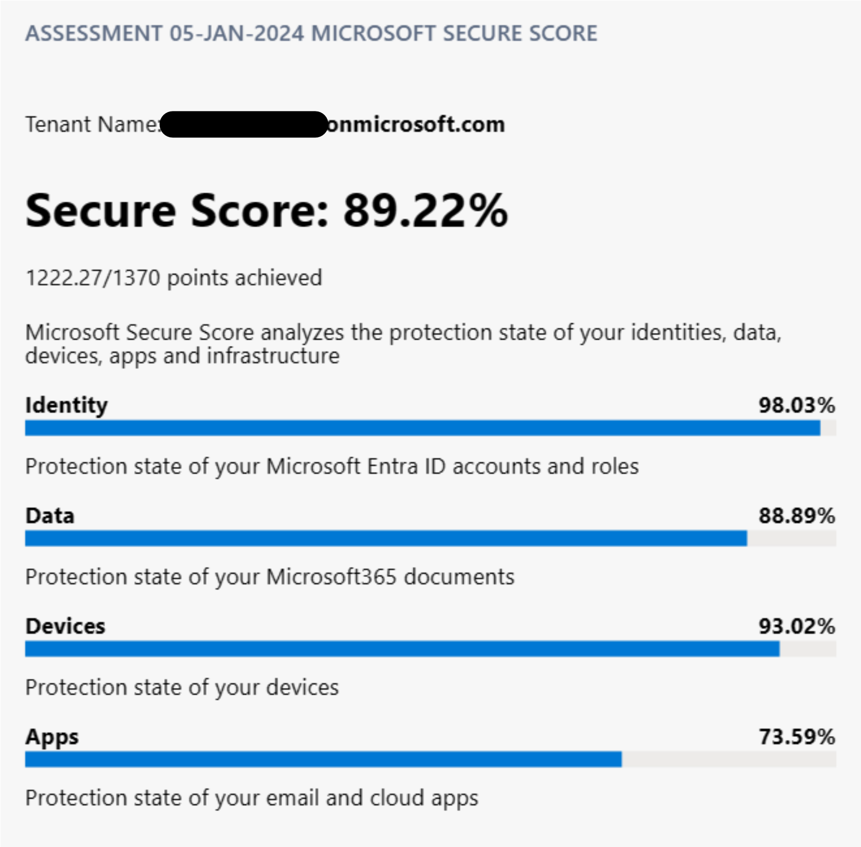
KnowBe4 training is used for Security Awareness and training.

A continuous training regime should be put in place

4.2 Microsoft and Defender for Cloud Secure Score

The Microsoft Secure Score looks at multiple items within the Microsoft 365 and Azure environments, these scores are retrieved from **EXAMPLE.onmicrosoft.com**. The score is based on the type of services being used on Microsoft 365 and Azure. The scores are compared to a baseline established by Microsoft. The score shows at what level you are aligned with the best security practices.

The Example Ltd's Microsoft Secure Score:



ASSESSMENT 05-JAN-2024 MICROSOFT SECURE SCORE

Tenant Name[redacted]onmicrosoft.com

Secure Score: 89.22%

1222.27/1370 points achieved

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps and infrastructure

Identity **98.03%**

Protection state of your Microsoft Entra ID accounts and roles

Data **88.89%**

Protection state of your Microsoft365 documents

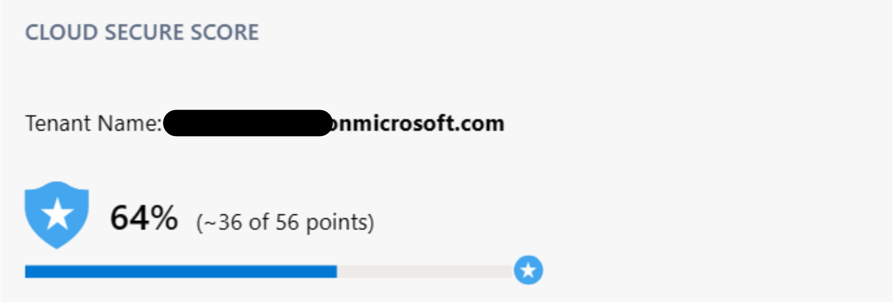
Devices **93.02%**

Protection state of your devices

Apps **73.59%**

Protection state of your email and cloud apps

The Example Ltd’s Cloud Secure Score:



CLOUD SECURE SCORE

Tenant Name:[redacted]onmicrosoft.com

64% (~36 of 56 points)

For more information about the Microsoft Secure Score you can visit the following link. Or check the score directly at: https://security.microsoft.com/securescore

4.3 Microsoft Product Support

Microsoft product support comes in two phases. Starting from the release date support is called Mainstream Support. At some point Microsoft announces that a product goes into Extended Support. During Mainstream Support product support benefits are available to all customers and consist of security fixes and product updates. In the Extended Support phase, security updates are provided to all customers for free, yet to get product break fixes an additional support contract is required. Because of that, we recommend planning life-cycle management to replace products around the end of Mainstream Support. Note that not all Microsoft products are eligible to extended support.

In addition, Microsoft normally requires that all available updates are installed before requesting support for the issue at hand.

The following information about the Microsoft Operating systems are found:

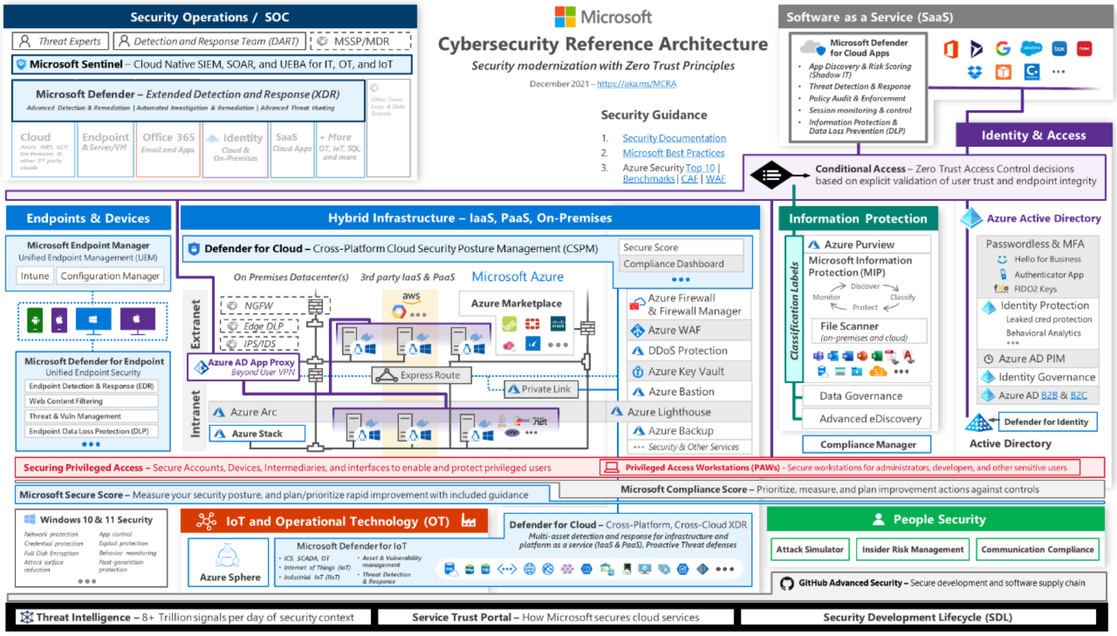
End of life products - None

The following products with an expected end of support very soon were found:

Soon to become End of life products - None

Appendix A - Overview of advised security software products

The references made to Microsoft products help mitigating the security vulnerabilities that were discovered. The recommended products integrate in Microsoft's Cybersecurity Reference Architecture, a holistic architecture approach that also adheres to the Open Group's Zero Trust Architecture. The picture below represents the MCRA and can be viewed better by going to https://aka.ms/mcra.


Security Operations / SOC
Threat Experts
Detection and Response Team (DART)
MSSP/MDR
Microsoft Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT
Microsoft Defender – Extended Detection and Response (XDR)
Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting
Other Tools, Logs, & Data Sources
Cloud
Azure, AWS, GCP, On Premises & other 3rd party clouds
Endpoint
& Server/VM
Office 365
Email and Apps
Identity
Cloud & On-Premises
SaaS
Cloud Apps
+ More
OT, IoT, SQL and more
Microsoft
Cybersecurity Reference Architecture
Security modernization with Zero Trust Principles
December 2021 – https://aka.ms/MCRA
Security Guidance
1. Security Documentation
2. Microsoft Best Practices
3. Azure Security Top 10 | Benchmarks | CAF | WAF
Software as a Service (SaaS)
Microsoft Defender for Cloud Apps
App Discovery & Risk Scoring (Shadow IT)
Threat Detection & Response
Policy Audit & Enforcement
Session monitoring & control
Information Protection & Data Loss Prevention (DLP)
Identity & Access
Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity
Endpoints & Devices
Microsoft Endpoint Manager
Unified Endpoint Management (UEM)
Intune
Configuration Manager
Microsoft Defender for Endpoint
Unified Endpoint Security
Endpoint Detection & Response (EDR)
Web Content Filtering
Threat & Vuln Management
Endpoint Data Loss Protection (DLP)
Hybrid Infrastructure – IaaS, PaaS, On-Premises
Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)
Secure Score
Compliance Dashboard
On Premises Datacenter(s)
3rd party IaaS & PaaS
Microsoft Azure
aws
Azure Marketplace
Extranet
NGFW
Edge DLP
IPS/IDS
Azure AD App Proxy
Beyond User VPN
Express Route
Private Link
Intranet
Azure Arc
Azure Stack
.net
Azure Firewall & Firewall Manager
Azure WAF
DDoS Protection
Azure Key Vault
Azure Bastion
Azure Lighthouse
Azure Backup
Security & Other Services
Information Protection
Classification Labels
Azure Purview
Microsoft Information Protection (MIP)
Discover
Classify
Protect
Monitor
File Scanner
(on-premises and cloud)
Data Governance
Advanced eDiscovery
Compliance Manager
Azure Active Directory
Passwordless & MFA
Hello for Business
Authenticator App
FIDO2 Keys
Identity Protection
Leaked cred protection
Behavioral Analytics
Azure AD PIM
Identity Governance
Azure AD B2B & B2C
Defender for Identity
Active Directory
Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users
Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users
Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance
Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls
Windows 10 & 11 Security
Network protection
Credential protection
Full Disk Encryption
Attack surface reduction
App control
Exploit protection
Behavior monitoring
Next-generation protection
IoT and Operational Technology (OT)
Azure Sphere
Microsoft Defender for IoT
ICS, SCADA, OT
Internet of Things (IoT)
Industrial IoT (IIoT)
Asset & Vulnerability management
Threat Detection & Response
Defender for Cloud – Cross-Platform, Cross-Cloud XDR
Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses
People Security
Attack Simulator
Insider Risk Management
Communication Compliance
GitHub Advanced Security – Secure development and software supply chain
Threat Intelligence – 8+ Trillion signals per day of security context
Service Trust Portal – How Microsoft secures cloud services
Security Development Lifecycle (SDL)

Source: https://aka.ms/mcra

Microsoft 365 Business Premium

The following security products are available in Microsoft 365 Business Premium. Note that Microsoft 365 Business has a maximum of 300 seats. If there is a need for more seats, Microsoft 365 E3 is required.

- Data Loss Prevention
- Microsoft Defender for Office 365 plan 1
  - Anti-Phishing
  - Real-Time Reports
  - Safe Attachments
  - Safe Links
- Office 365 Message Encryption
- Enterprise Mobility + Security
  - Azure Active Directory P1
  - Azure Active Directory Password Protection
  - Azure Multi-Factor Authentication (MFA)
  - Cloud App Discovery
  - Conditional Access
  - Information Protection
  - Microsoft Intune
- Windows - BitLocker
- Windows - Hello for Business

- Windows - Windows Defender Application Control Guard

Recommended Azure Security Solutions

Azure has many security-related services and technologies to offer in order to help customers enhance the security of their Azure services. A list of recommended Azure Security solutions is shown below:

- Azure DDoS Protection
- Azure Firewall
- Azure Confidential Computing
- Azure Virtual Desktop

Appendix B – The CSAT Methodology

This report aims to bring you a better understanding of your organization's current cybersecurity posture, and actionable items to mitigate the discovered risks. The Cyber Security Assessment Tool (CSAT) consists of a technical scan of your environment and an interview based on renowned CIS controls. The report that you are reading now is packed with recommendations to enhance your IT environment, based on industry recommended practices. In this appendix the CSAT methodology will be explained.

Control Framework background (CIS)

The Center for Internet Security® (CIS) is a nonprofit organization responsible for the globally recognized CIS Controls® and CIS Benchmarks™, offering best practices for securing IT systems and data. The CIS community continually updates these standards to address emerging threats.

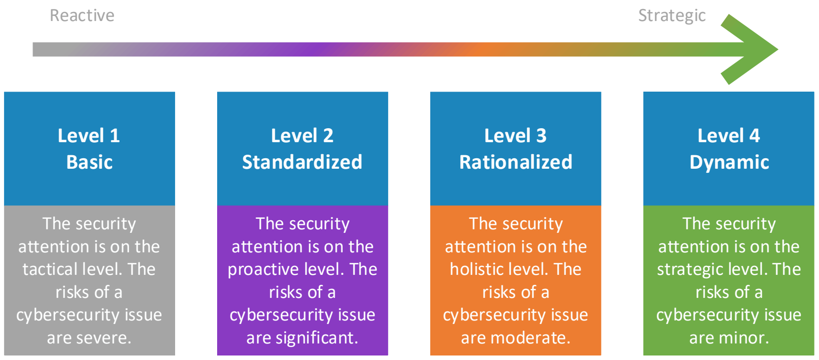
The CSAT questionnaire is based on the CIS Controls and includes questions related to ISO27001:2022 controls. It aims to gather relevant information about your IT processes. To learn more about the Center for Internet Security, visit https://cisecurity.org.

CIS Controls™ (v8) take a community-based approach, derived from consensus risk assessments involving experts from government, industry, and academia. These controls focus on common threats and vulnerabilities in large enterprises, serving as a strong foundation for high-impact actions. They complement, rather than replace, comprehensive IT and security risk management frameworks.

For the Cybersecurity Assessment, the technical CIS Controls™ (v8) are expanded with high-level controls from ISO/IEC 27001:2022 in the Organizational control domain. These questions are related to IT- and data governance, and cover the areas of policies, compliancy, risk management and privacy.

SOM Model

To achieve this goal, the Cybersecurity Assessment utilizes a Maturity Model to communicate the findings and recommendations. The maturity model construct for the Cybersecurity Assessment is based on a similar model developed by Microsoft (Security Maturity Model v1) and is consistent with the Software Optimization Model (SOM). The below reflects the levels:



Level 1 Basic: The security attention is on the tactical level. The risks of a cybersecurity issue are severe.

Level 2 Standardized: The security attention is on the proactive level. The risks of a cybersecurity issue are significant.

Level 3 Rationalized: The security attention is on the holistic level. The risks of a cybersecurity issue are moderate.

Level 4 Dynamic: The security attention is on the strategic level. The risks of a cybersecurity issue are minor.

The complete score of the organization is determined by the lowest score in the organization, for example if most processes are at Level 3, but one process is at Level 1, the whole organization is rated at Level 1.