Cybersecurity Assessment

Contoso

QS Solutions
David Lane
Issued in November | 2022

Contents

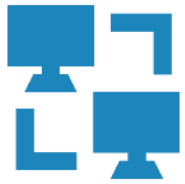
Introductions

Who is Who

Expectations for this meeting

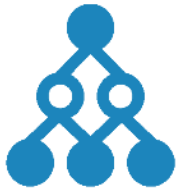
Assessment approach | CSAT information

The Cyber Security Assessment Tool is developed by a team of seasoned security experts. It collects relevant data from:



Endpoints

Microsoft 365, Google Workspace, SharePoint, Azure, and Intune



Active Directory Microsoft Entra ID

Questionnaire, Interview

Assessment approach | CIS Framework

QS solutions has conducted a review of Contoso's current IT security practice and implementation. The assessment is based on the CIS Controls™ (v8) security framework, published by the Centre for Internet Security® (CIS).

Contoso's cybersecurity maturity level is classified based on the questionnaire interview; the CSAT scan provides further information about your environment's current security state.

This presentation summarizes the CSAT report to inform the stakeholders of our findings and recommendations to enhance your security resilience. The full report is intended for technical stakeholders involved in security strategy and management.

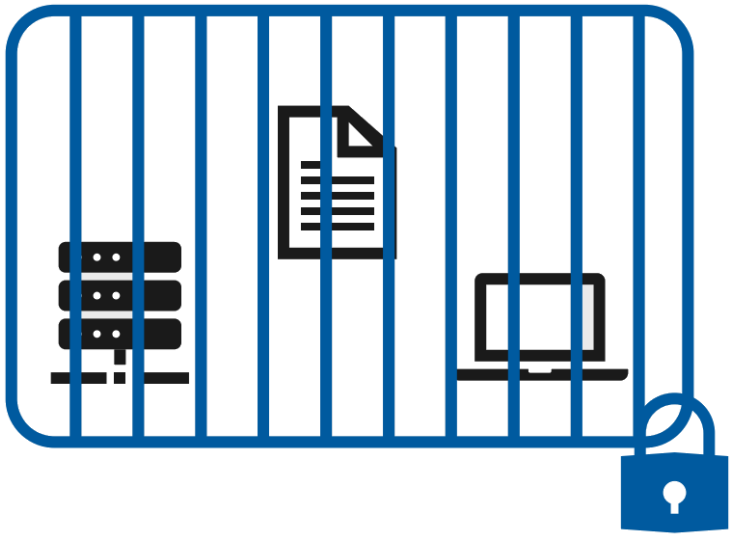
The CSAT report contains all findings and recommendations. Although it is not a governance control review nor a security audit, the report's recommendations can be used to prepare the organization for an audit.

Security Threat Landscape Evolution

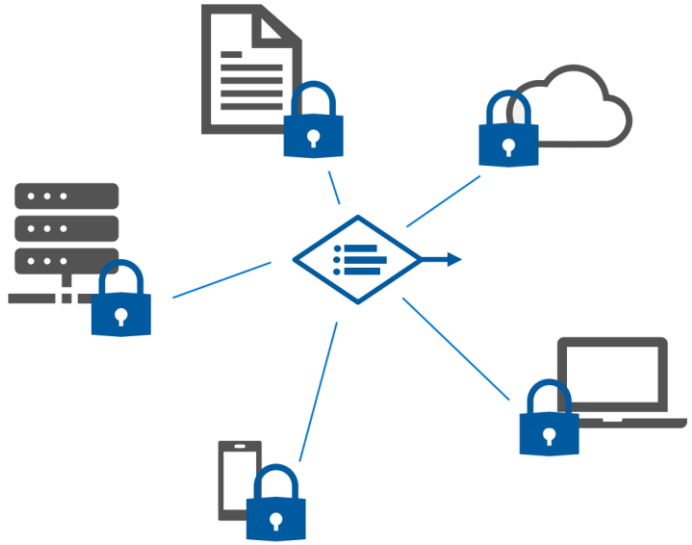
Zero Trust Security Architecture principles

Security Landscape | Zero Trust Security

Modern security architecture principles; Microsoft and many other vendors have embraced these principles in their reference architectures



Classic Approach – Secure all assets within your on-premises ‘castle’



Zero Trust – Protect all assets wherever they are located

Security Landscape | Zero Trust Security Architecture

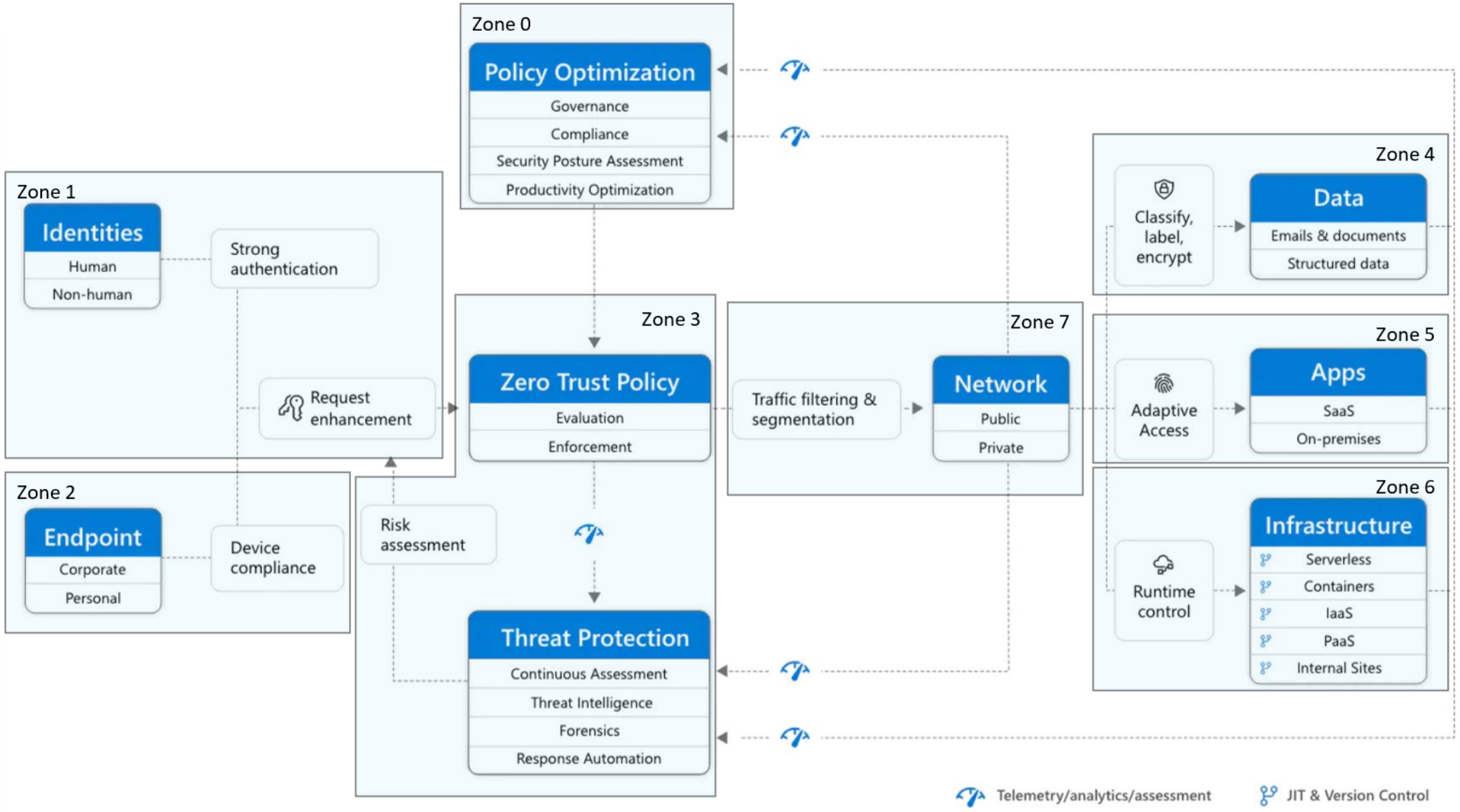
Modernized security architecture principles, defined by The Open Group

Embraced by Microsoft and many other vendors in their reference architectures

The Zero Trust Security Architecture principles are:

1. **Verify explicitly**
   Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
2. **Use least privileged access**
   Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.
3. **Assume breach**
   Minimize blast radius for breaches and prevent lateral movement by segmenting access by network, user, devices, and app awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility, drive threat detection, and improve defenses.

Security Landscape | Zero Trust Architecture Overview



Security Landscape | How CSAT relates to said topics

Many CSAT recommendations are linked to Zero Trust Security Architecture zones.

This helps prioritizing the CSAT recommendations in order to better protect your organization against ransomware.

It also shows that the recommendations fit into a long-term strategy to rejuvenate your IT environment into an enhanced secure infrastructure, based on the Zero Trust Security architecture principles.

Management Summary

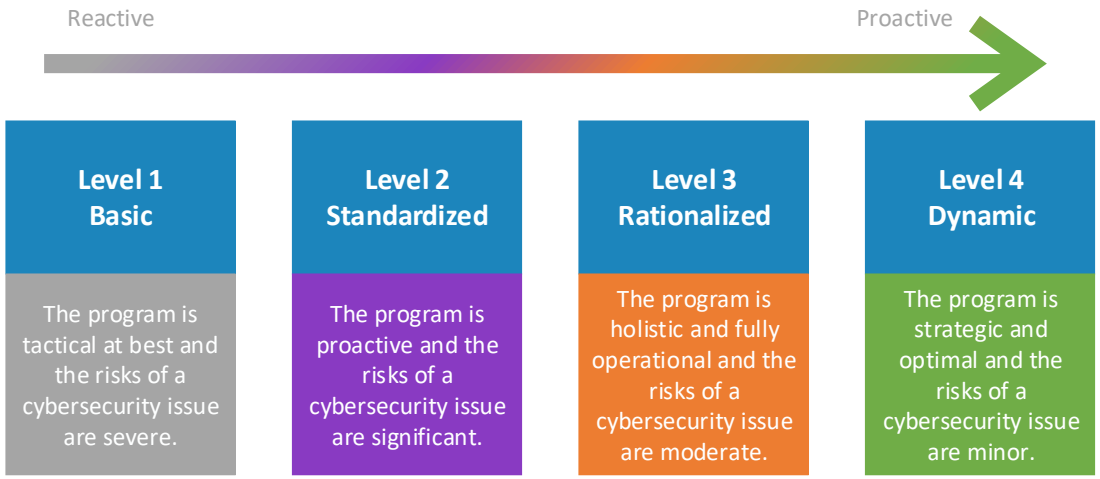
Management Summary | Current State and Major Risks

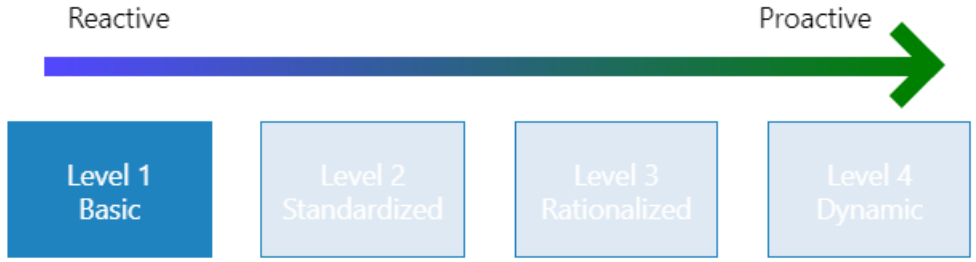
CIS Maturity Level

Your current average security maturity level score is between Basic and Standardized.

Lowest score

Special attention is needed for the lowest scoring items





Management Summary | Major risks

Major Risks

- **Reputation damage**
  - Unauthorized use of your email domain(s)
- **Financial damage after Ransomware attacks**
  - Identity theft
  - Unsupported legacy software
- **Leaked company information** (for example, PII, confidential information, IP)
  - Accidental sharing of documents

Management Summary | Strategic Recommendations

Strategic recommendations

The security risks facing the organization are generally understood although not in a managed way.

The governance of the cybersecurity program is structured but not fully integrated with other governance areas.

The organization’s employees are unaware of today’s (cyber)security threats and related training around security and privacy awareness is missing.

Management Summary | Top recommendations | Interview

Topic	Action	Associated Software Products	ZTA Zone
Urgent			
4. Secure Configuration of Enterprise Assets and Software	• Implement tooling to apply a default security baseline to all Windows assets in the organization. Start with deployment for a limited subset of targets and monitor whether users can still work as they are used to	• Microsoft Endpoint Manager • Azure Defender for Cloud • Windows 10 and 11 Pro/Enterprise	0, 2, 3
8. Audit Log Management	• Implement tooling to ensure a central time sync source is setup on the company assets.	• Microsoft Endpoint Manager	2
11. Data Recovery	• Secure the organization's back-ups through either physical or technical security measures.	• Azure Backup	3
13. Network Monitoring and Defense	• Implement a host-based intrusion detection solution for all supported devices and implement a process to finetune the policies annually.	•	2, 3
19. AQ 1. IT Governance	• Implement a review process, based on industry best practices.	• Microsoft Purview Compliance Manager	0, 3
20. AQ 2. Data Governance	• Implement a basic risk management process.	•	0, 3, 4

Management Summary | Top recommendations | Scan findings

Topic	Action	Associated software products	ZTA zone
Quick Wins			
(Azure) Active Directory Accounts	• Review accounts with risky UAC details (see chapter 4.1.16) and remove these AD settings • Implement Multi Factor Authentication (MFA) for all user accounts	• Microsoft Entra ID MFA • Microsoft Entra ID Conditional Access	1
Administrators	• Ensure admin roles are only placed on admin accounts and not on normal user accounts	• Microsoft Entra ID Privileged Identity Management (PIM)	1
Operating Systems	• Migrate the (almost) end-of-life operating systems • Isolate (or retire) endpoints that cannot be updated or patched	• Windows Server 2016 or 2019 • Windows 10	2 7
Applications	• Ensure that all applications are kept to up to date • Integrate all detected application with Microsoft Entra ID and enable SSO where possible	• Microsoft Endpoint Manager • Microsoft Defender for Cloud Apps	2 3 5

Plan of Approach

Suggested Roadmap

Plan of Approach | 0-30 days

Identities

- Review accounts with risky UAC details and remove these AD settings
- Disable old/unused accounts
- Implement Multi Factor Authentication (MFA) for all user accounts
- Ensure admin roles are only placed on admin accounts and not on normal user accounts

Devices

- Ensure that all applications are kept to up to date
- Isolate (or retire) endpoints that cannot be updated or patched

Data

- Review the documents that might contain sensitive data

Cybersecurity Strategy Workshop

A One-day workshop to elaborate on today's security landscape, current security principles, how cloud security features help fortifying your security program, providing input to revise your cybersecurity strategy. Deliverable: overview of discussed principles and conceptual design decisions.

Plan of Approach | 30 – 90 days

Cybersecurity Strategy

Define policies and procedures based on workshop outcomes

- Identity & Access Management
- Device Management
- Data Protection, Management
- Governance
- Reporting

Data

- Identify sensitive information on the organization's main data sources.

Infrastructure

- Create the appropriate SPF, DKIM and DMARC record for all email domains.

Automation

- Establish a (review) process to grant/deny administrative accounts granular privileged access.
- Implement a basic risk assessment process.

Plan of Approach | Beyond 90 days

Define lifecycle management procedures for

- Applications
- Operating Systems
- Security Architecture

Create plan of approach for other Urgent action Items.

Perform a Cybersecurity assessment periodically, to measure and prove your progress, identify new pitfalls proactively and to present the progress to your management board in clear language

Plan of Approach | Suggested Products & Licensing

Phase	Feature/Function	Product/Suite	# Licenses owned/required
0-30 days	Multi-Factor Authentication	Microsoft Entra ID P1	153
	Privileged Identity Management	Microsoft Entra ID P2	32
	Conditional Access basis	Microsoft Entra ID P1	251
	Device patching/security baseline	Enterprise Management & Security (EMS) E3	153
	Application/shadow IT monitoring	Microsoft Defender for Cloud apps/ Microsoft365 E3	16
30-90 days	Risk-based Conditional Access	Microsoft Entra ID P2/EMS E3	245
	Application/shadow IT policy enforcement	Microsoft Defender for Cloud Apps	15
	Dedicated Admin Workstations	Azure Windows Virtual Machines/Bastion	164
	Teams/SharePoint self-service creation	QS PortalTalk	75
90+ days	Document classification, automated	Microsoft Information Protection P2/M365 E5	245
	Alert/finding reporting to SIEM	Azure Security Center/Sentinel	
	Teams/SharePoint governance/reporting	QS PortalTalk	75

Interview Results Summary

Interview results| CIS controls

Lowest ranked question answers

1. Inventory and Control of Enterprise Assets

Implement a manual process to collect and store asset information in a central Content Management Database (CMDB).

4. Secure Configuration of Enterprise Assets and Software

Implement tooling to apply a default security baseline to all Windows assets in the organization. Start with deployment for a limited subset of targets and monitor whether users can still work as they are used to.

8. Audit Log Management

Implement tooling to ensure a central time sync source is setup on the company assets.

Interview results| CIS controls

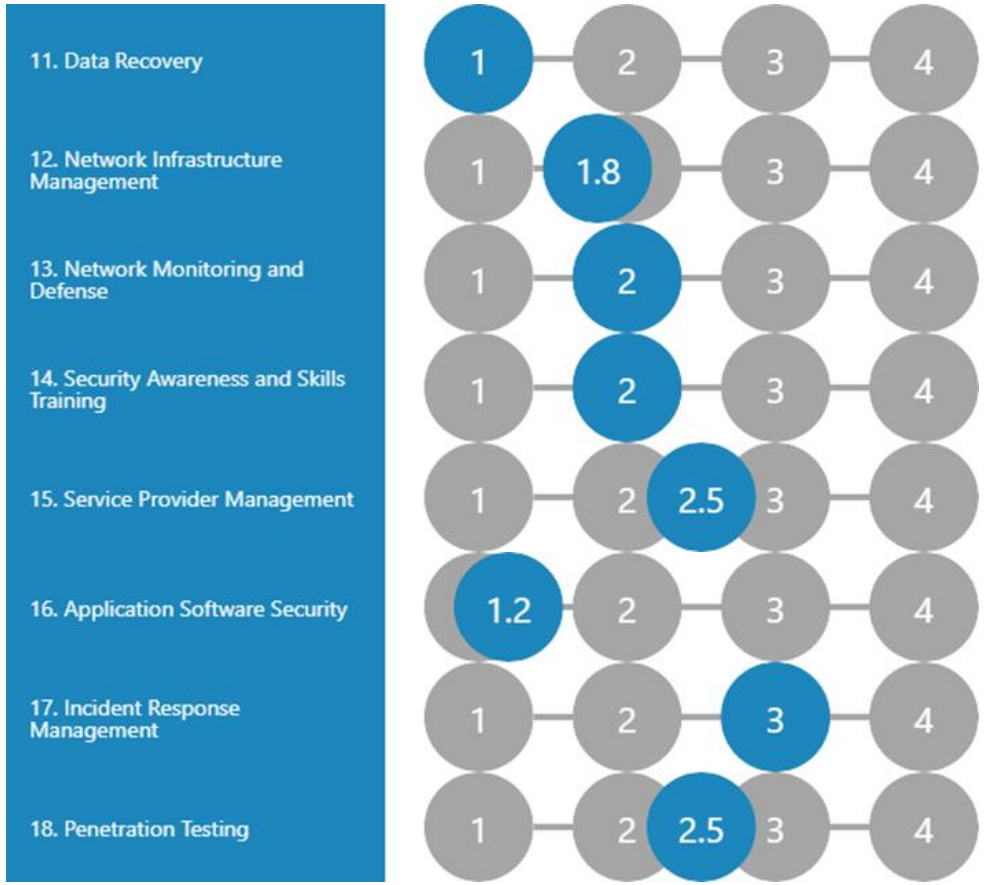
Lowest ranked question answers

11. Data Recovery

Secure the organization's back-ups through either physical or technical security measures.

16. Application Software Security

Implement a training program to give guidance on how to use secure application development. Support the training with a secure application development process. Ensure the commits are checked each quarter if the security application development process is used.



Interview results | Additional Questions

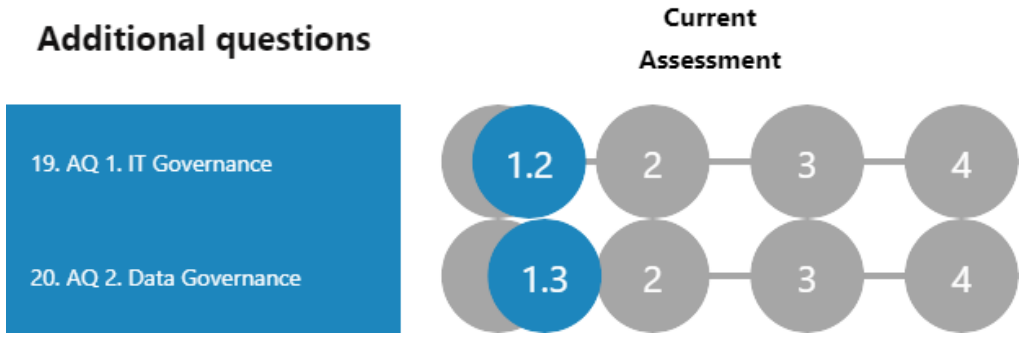
Lowest ranked question answers

19. AQ 1. IT Governance

Implement a review process, based on industry best practices.

20. AQ 2. Data Governance

Implement a basic risk management process.



Scan Findings Summary

Scan Findings | Windows versions

CIS control 2; Zero Trust zone 3

Findings

- End of Life and almost end of life operating systems were found
- Versions are not updated

Associated Risks

- Compliance issues: Regulated industries like healthcare and e-commerce deal with lots of sensitive customer data
- Security vulnerabilities: Security patches no longer issued by Microsoft; e.g., Windows XP has well known exploitable security hazards

Recommendations

- Create a plan to phase out unsupported OS
- Update all endpoints to the latest version

Scan Findings | Endpoint Secure Configuration

CIS control 4

Findings

- Endpoints were found with SMB v1 enabled
- Several endpoints were found that are not using the secure remote connection protocol
- No security baseline is applied to endpoints

Associated Risks

- Security vulnerabilities: (older) protocols have well known security hazards that are often misused
- Too many services enabled: by default, there are service that are not used however they are enabled, creating a possible entry way for unwanted people

Recommendations

- Find a security baseline that fits your company and apply that to the endpoints
- Ensure SMB v1 is disabled on all the endpoints

SECURE CONFIGURATION

Powershell x32 unrestricted	1
Powershell x64 unrestricted	1
Incoming RDP enabled with no NLA	1
Endpoints with RDP security level lower than 2	1
Endpoints with LM Compatibility lower than 5	4
SMB V1 Enabled	1
SMB V2 Enabled	3
SMB V3 Enabled	2

Scan Findings | Active Directory administrator accounts

CIS control 6

Findings

- Many domain, enterprise and schema admins were found

Associated Risks

- Leaked administrator-IDs provide unrestricted access to your environment

Recommendations

- Review all users in the admin groups for legitimacy; limit these numbers as much as possible.
- Implement a process to regularly review the admin groups

AD ADMINISTRATORS

Built in Administrators domain group	27
Domain Admin	74
Enterprise Admin	17
Schema Admin	11
Users with admin count	122

Scan Findings | Azure Active Directory administrator accounts

CIS control 6

Findings

- Many accounts in administrative roles were found
- Multi-Factor Authentication is not used on multiple admin accounts

Associated Risks

- Leaked user accounts will be misused to gain administrator access

Recommendations

- Review all users in the admin groups for legitimacy; limit these numbers as much as possible.
- Enforce Multi-Factor Authentication for all admin/privileged users

CONTOSO.ONMICROSOFT.COM

Directory Synchronization Accounts	1
Company Administrator	35
Device Administrators	25
Helpdesk Administrator	75
Security Administrator	22

Scan Findings | Risk management

CIS control 7

Findings

- No regular risk management process is being used
- No vendor risk management process is being used

Associated Risks

- Risk management processes are often required by many industry-specific standards and legislation resulting in incompliance
- Without risk and/or vendor management, there is no insight and no awareness about the impact of disruption

Recommendations

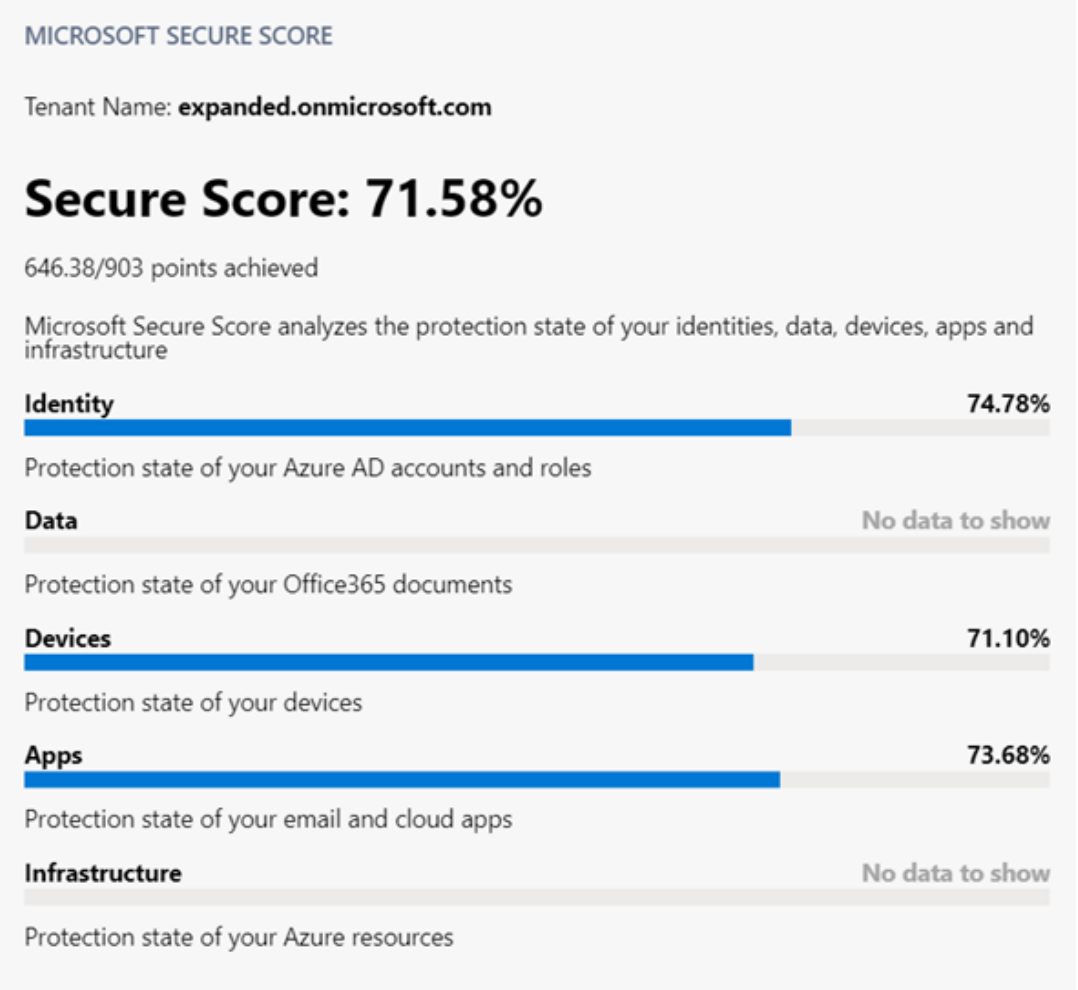
- Investigate to which regulatory requirements your company must adhere to
- Adopt and implement a risk management process, procedures to start your compliance journey

Scan Findings | Microsoft 365 Secure Score

The Microsoft Secure Score scans multiple areas within Office 365 and Microsoft Entra ID . The score is based on the type of services being used in and compares them to a baseline established by Microsoft. The score shows to what extend you are aligned with the recommended security practices.

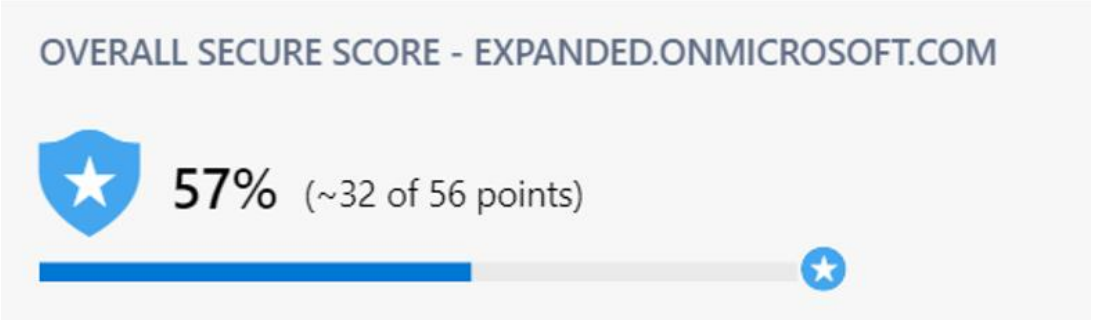
We recommend starting with the following topics

- Require MFA for administrative roles
- Designate fewer than 5 global admins
- Enable policy to block legacy authentication



Scan Findings | Cloud Secure Score

The Cloud Secure Score scans all Azure resources within our tenant. The Secure Score is based on the type of services being used and compares them to Microsoft security baselines and recommended practices.



We recommend to start with the following items

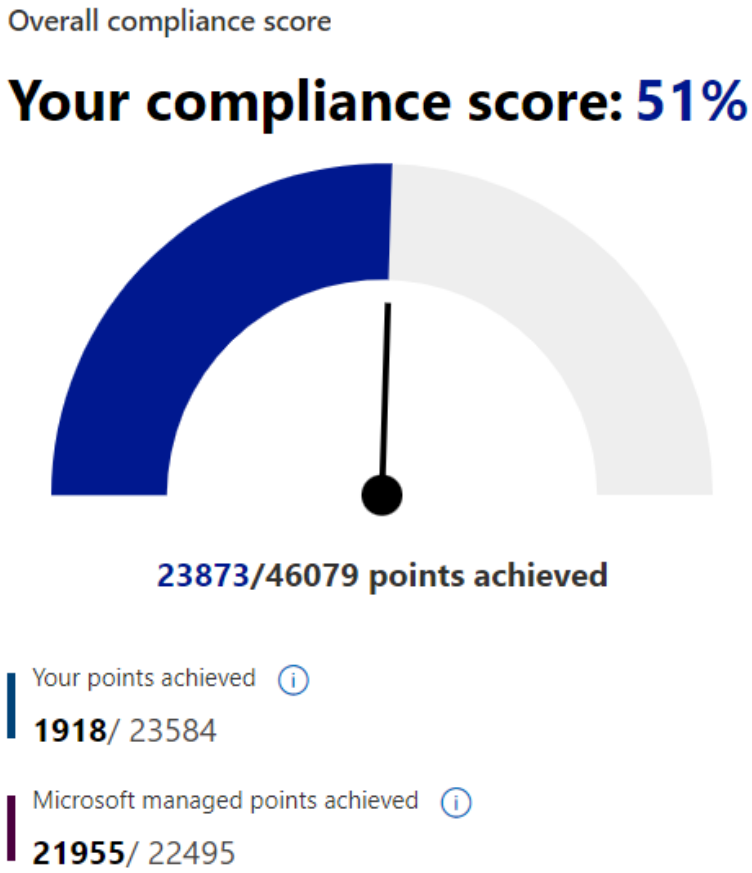
- MFA should be enabled on accounts with write permissions on your subscription
- Internet-facing virtual machines should be protected with network security groups
- Web Application should only be accessible over HTTPS

Scan Findings | Microsoft Purview Compliance Manager Score

The Microsoft Purview Compliance Manager looks at the compliance status in the Microsoft 365 environment. The score is based on the type of services being used in Microsoft 365 and compares them to a baseline established by Microsoft.

We recommend starting with the following topics

- Retain training records
- Enforce rules of behavior and access agreements



Next steps

Next steps | How can we assist?

Prioritize recommendations

Implement 0-30 days actions

Re-assessing security periodically

Define project plans based on plan of approach

Next steps | Microsoft Security Workshops

Sales – Secure Multi-Cloud Environments
Help customers identify current, ongoing risks to their cloud environment and define next steps to accelerate their security journey.

Go to workshop

Sales – Defend Against Threats with SIEM Plus XDR
Enable customers with visibility into immediate threats across email, identity and data and demonstrate how Microsoft Sentinel and Microsoft 365 Defender help organizations use intelligent security analytics and threat intelligence to detect and quickly stop active threats.

Go to workshop

Usage – Secure Identities and Access
Help customers find and mitigate identity risks and safeguard their organization with a seamless identity solution.

Go to workshop