GLOBAL BRANDS GROUP

POWERING TRANSFORMATION

CISA M365 SECURITY ASSESSMENT (C-MSA)

POWERING
TRANSFORMATION

OVERVIEW

The CISA M365 Security Assessment (C-MSA) is an advanced, automated tool designed to evaluate and enhance the security posture of Microsoft 365 environments.

Developed to adhere to stringent CISA standards, this tool provides a thorough assessment of your M365 configuration, helping you identify vulnerabilities and implement security improvements efficiently.

POWERING
TRANSFORMATION

BENEFITS FOR YOUR BUSINESS

Compliance and Improvement:
Identifies gaps in compliance and highlights areas for security enhancement.

Actionable Insights:
Provides clear, actionable recommendations to improve your overall security posture.

Vulnerability Identification:
Evaluate the security posture of your M365 environment, pinpointing vulnerabilities that could be exploited by attackers.

Reduced Risk:
Properly configured M365 security features reduce the attack surface, minimizing the risk of data breaches.

Comprehensive Focus Areas:
Covers critical areas such as identity and access management, information protection, and threat protection to ensure all-round security.

POWERING
TRANSFORMATION

C-MSA FEATURES

1. **User-Friendly Interface:**
   Operates within a seamless GUI.

2. **Least Privilege Usage:**
   Ensures minimal impact on tenant security.

3. **Fast Reporting:**
   Detailed pass/fail reports are available within 15 minutes.

4. **Prioritized Recommendations:**
   Configuration changes are prioritized, with clear guidance for remediation.

5. **Comprehensive:**
   Includes necessary manual checks for thoroughness.

POWERING
TRANSFORMATION

THE SCOPE OF (C-MSA)

The CISA M365 Security Assessment (C-MSA) serves as an automated tool aimed at assessing and fortifying the security posture of Microsoft 365 (M365) ecosystems. The C-MSA's domain includes essential M365 services such as:

POWERING
TRANSFORMATION

MICROSOFT ENTRA ID (AZURE ACTIVE DIRECTORY)

Microsoft Entra ID, the identity and access management service for the M365 suite, plays a critical role in securing user identities and managing access.
The C-MSA tool assesses configurations related to:

- Identity protection and governance
- Multi-factor authentication (MFA) enforcement
- Conditional Access policies
- Privileged Identity Management (PIM)
- Audit logs and alerting mechanisms.

MICROSOFT 365 DEFENDER

Microsoft 365 Defender integrates threat protection across Microsoft 365 services.
C-MSA evaluates:

- Advanced Threat Protection (ATP) settings
- Endpoint detection and response (EDR) configurations
- Cloud App Security policies
- Automated investigation and remediation capabilities
- Security incident and event management (SIEM) integration.

POWERING
TRANSFORMATION

EXCHANGE ONLINE

Exchange Online, the cloud-hosted email service, is crucial for organizational communication.

The assessment for Exchange Online includes:

- Anti-spam and anti-malware configurations
- Mail flow rules and policies
- Data loss prevention (DLP) settings
- Email encryption protocols
- Secure Score Assessment for Exchange Online.

MICROSOFT POWER PLATFORM

Microsoft Power Platform enables automation, app development, and data insights.

C-MSA examines:

- Data integration and connectivity security
- Power Apps and Power Automate environment configurations
- Role-based access control (RBAC) settings
- Data policies and compliance measures
- Audit logging and monitoring for Power BI.

POWERING
TRANSFORMATION

SHAREPOINT ONLINE

SharePoint Online facilitates document management and collaboration.
The assessment focuses on:

- Site and document library security configurations
- External sharing and access controls
- Information Rights Management (IRM)
- Sensitivity labels and data classification

MICROSOFT TEAMS

Microsoft Teams is the collaboration hub within M365.
The C-MSA evaluates:

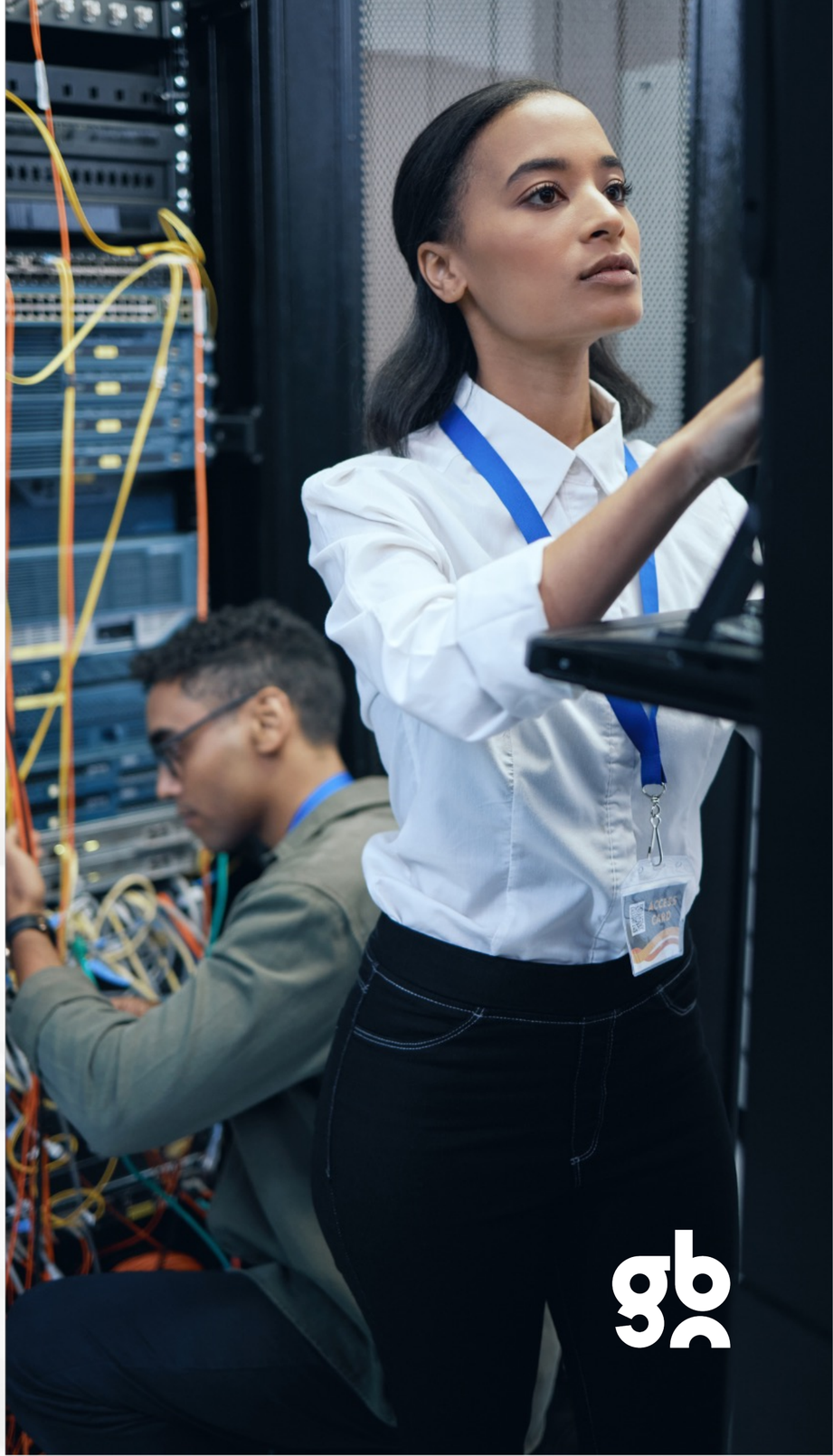
- Team and channel settings for security and compliance
- Meeting and calling security configurations
- Guest access policies
- Data retention and information protection settings
- Integration with other M365 security tools.

POWERING
TRANSFORMATION

C-MSA REPORTS

The automated assessment generates comprehensive reports that detail the pass/fail status of your current configurations.

These reports prioritize configuration changes and provide clear, actionable recommendations to bolster your M365 security posture. Including required manual checks ensures a holistic evaluation, giving you the confidence to secure your environment effectively.



POWERING
TRANSFORMATION

C-MSA REPORTS CASES

- The reports will be available within 15 minutes, detailing the pass/fail status.

CISA Entra ID Compliance and Recommendations

The below section represents the current CISA Entra ID Compliance and Recommendations

Legacy Authentication

Control ID	Requirement	Result	Criticality	Details
MS.AAD.1.1v1	Legacy authentication SHALL be blocked.	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. View all CA policies.

Risk Based Policies

Control ID	Requirement	Result	Criticality	Details
MS.AAD.2.1v1	Users detected as high risk SHALL be blocked.	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. View all CA policies.
MS.AAD.2.2v1	A notification SHOULD be sent to the administrator when high-risk users are detected.	N/A	Should/Not-Implemented	This product does not currently have the capability to check compliance for this policy. See Secure Configuration Baseline policy for instructions on manual check
MS.AAD.2.3v1	Sign-ins detected as high risk SHALL be blocked.	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. View all CA policies.

Strong Authentication and a Secure Registration Process

Control ID	Requirement	Result	Criticality	Details
MS.AAD.3.1v1	Phishing-resistant MFA SHALL be enforced for all users.	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. View all CA policies.
MS.AAD.3.2v1	If phishing-resistant MFA has not been enforced, an alternative MFA method SHALL be enforced for all users.	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. View all CA policies.
MS.AAD.3.3v1	If phishing-resistant MFA has not been enforced and Microsoft Authenticator is enabled, it SHALL be configured to show login context information.	N/A	Shall/Not-Implemented	This policy is only applicable if phishing-resistant MFA is not enforced and MS Authenticator is enabled. See Secure Configuration Baseline policy for more info

POWERING TRANSFORMATION

C-MSA REPORTS CASES

- Reports prioritize configuration changes and provide recommendations for fixing them.

MS.AAD.7.1v1	A minimum of two users and a maximum of eight users SHALL be provisioned with the Global Administrator role.	Fail	Shall	11 global admin(s) found: Aboubakr Mostafa, Ahmed Nasser, Alaa Samir, Dina Khalafawy, Hesham El Zoghby, Mina Mikhael, Mohamed A. Eid, Mohamed Magdy, Sagda Moussa, Security Demo, Shrouq Turkey
MS.AAD.7.2v1	Privileged users SHALL be provisioned with finer-grained roles instead of Global Administrator.	Fail	Shall	Requirement not met: Policy MS.AAD.7.1 failed so score not computed
MS.AAD.7.3v1	Privileged users SHALL be provisioned cloud-only accounts separate from an on-premises directory or other federated identity providers.	Pass	Shall	0 admin(s) that are not cloud-only found
MS.AAD.7.4v1	Permanent active role assignments SHALL NOT be allowed for highly privileged roles.	Fail	Shall	4 role(s) that contain users with permanent active assignment: Exchange Administrator, Global Administrator, SharePoint Administrator, User Administrator
MS.AAD.7.5v1	Provisioning users to highly privileged roles SHALL NOT occur outside of a PAM system.	Fail	Shall	4 role(s) assigned to users outside of PIM: Exchange Administrator, Global Administrator, SharePoint Administrator, User Administrator
MS.AAD.7.6v1	Activation of the Global Administrator role SHALL require approval.	Fail	Shall	1 role(s) or group(s) allowing activation without approval found: Global Administrator(Directory Role)

- Reports include The required manual checks within your tenant.

Control ID	Requirement	Result	Criticality	Details
MS.AAD.8.1v1	Guest users SHOULD have limited or restricted access to Azure AD directory objects.	Pass	Should	Permission level set to "Limited access" (authorizationPolicy)
MS.AAD.8.2v1	Only users with the Guest Inviter role SHOULD be able to invite guest users.	Pass	Should	Permission level set to "adminsAndGuestInviters" (authorizationPolicy)
MS.AAD.8.3v1	Guest invites SHOULD only be allowed to specific external domains that have been authorized by the agency for legitimate business purposes.	N/A	Should/Not-Implemented	This product does not currently have the capability to check compliance for this policy. See Secure Configuration Baseline policy for instructions on manual check

POWERING
TRANSFORMATION

SECURITY ASSESSMENT TYPES

	Manual Assessment	Automatic Assessment
Approach	Configurations are manually checked one by one.	Utilizes a script to perform the assessment.
Duration	Up to 3 hours.	Completes in just a few minutes
Use Case	Not ideal for initial assessments but useful for detailed reviews.	Ideal for initial assessments, providing rapid insights.

THANK YOU

GLOBAL BRANDS GROUP®

POWERING TRANSFORMATION

EGYPT OFFICE

67 Road 90, New Cairo, Egypt

+20 111 333 7800

SAUDI ARABIA OFFICE

Anas Ibn Malik Street, Al Malqa Dist.,
Riyadh, Saudi Arabia

+96 6564 1908 19

contactus@gbrands.com

www.gbrands.com