

Azure security checklist (MCSB v2)

Groupe Conseil GRD. Official source: Microsoft Learn, Microsoft cloud security benchmark v2 (preview), accessed October 29, 2026: <https://learn.microsoft.com/en-us/security/benchmark/azure/overview> . Microsoft states that v2 is in preview and replaces v1.

How to use: for each control, tick Compliant, Partial or Non-compliant and record the evidence (e.g., a Defender for Cloud recommendation, an Azure Policy assignment). Control IDs and titles are quoted as published by Microsoft. Details for each control (principle, implementation, Azure Policy) are on the domain's source page.

NIST CSF codes: this column shows the "NIST CSF v2.0" codes that Microsoft lists for each control (per Microsoft). Note: several of these codes (e.g., PR.AC, PR.IP, PR.PT, DE.DP, RS.RP, ID.SC) look like CSF version 1.1 identifiers and do not exist in CSF 2.0, published by NIST on February 26, 2024. Microsoft also states that these mappings do not equal full compliance.

1. Network Security (NS)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-network-security>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
NS-1	Establish network segmentation boundaries	PR.IR-01, PR.AC-05	☐	☐	☐	
NS-2	Secure cloud native services with network controls	PR.AC-05, PR.DS-05	☐	☐	☐	
NS-3	Deploy firewall at the edge of enterprise network	PR.AC-05, PR.PT-04, DE.CM-01	☐	☐	☐	
NS-4	Deploy intrusion detection/intrusion prevention systems (IDS/IPS)	DE.CM-01, DE.CM-04, DE.CM-07	☐	☐	☐	
NS-5	Deploy DDoS protection	PR.PT-05, DE.CM-01	☐	☐	☐	
NS-6	Deploy web application firewall	PR.AC-05, PR.PT-05, DE.CM-04	☐	☐	☐	
NS-7	Manage network security centrally and effectively	PR.IP-01, DE.CM-01, DE.CM-07	☐	☐	☐	
NS-8	Detect and disable insecure services and protocols	PR.DS-02, PR.IP-01, DE.CM-04	☐	☐	☐	
NS-9	Connect on-premises or cloud network privately	PR.AC-05, PR.DS-02	☐	☐	☐	
NS-10	Ensure Domain Name System (DNS) security	DE.CM-01, DE.CM-04, DE.AE-02	☐	☐	☐	

2. Identity Management (IM)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-identity-management>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
IM-1	Centralize identity and authentication while ensuring isolation	PR.AA-1, PR.AC-1, PR.AC-7	☐	☐	☐	
IM-2	Protect identity and authentication systems	PR.AA-1, PR.AC-1, DE.CM-1	☐	☐	☐	
IM-3	Manage application identities securely and automatically	PR.AA-1, PR.AC-1, PR.DS-1	☐	☐	☐	
IM-4	Authenticate server and services	PR.DS-2, PR.DS-5	☐	☐	☐	
IM-5	Use single sign-on (SSO) for application access	PR.AA-1, PR.AC-1	☐	☐	☐	
IM-6	Use strong authentication controls	PR.AA-1, PR.AC-1	☐	☐	☐	
IM-7	Restrict resource access based on conditions	PR.AC-1, PR.AC-4, PR.AA-1	☐	☐	☐	
IM-8	Restrict the exposure of credentials and secrets	DE.CM-8, PR.DS-1, PR.AC-1	☐	☐	☐	

3. Privileged Access (PA)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-privileged-access>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
PA-1	Separate and limit highly privileged/administrative users	PR.AC-4, PR.AA-1	☐	☐	☐	
PA-2	Avoid standing access for user accounts and permissions	PR.AC-4, PR.AA-1	☐	☐	☐	
PA-3	Manage lifecycle of identities and entitlements	PR.AA-3, PR.AC-1, PR.AC-4	☐	☐	☐	
PA-4	Review and reconcile user access regularly	PR.AA-3, PR.AC-6, DE.CM-3	☐	☐	☐	
PA-5	Set up emergency access	PR.IP-10, RS.CO-3, RS.RP-1	☐	☐	☐	
PA-6	Use privileged access solution	PR.AC-7, PR.PT-3, DE.CM-1	☐	☐	☐	
PA-7	Follow just enough administration (least privilege) principle	PR.AC-4, PR.AC-7, PR.AA-1	☐	☐	☐	
PA-8	Determine access process for cloud provider support	PR.AC-4, PR.PT-2, DE.AE-3	☐	☐	☐	

4. Data Protection (DP)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-data-protection>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
DP-1	Discover, classify, and label sensitive data	PR.DS-1, PR.DS-5	☐	☐	☐	
DP-2	Monitor anomalies and threats targeting sensitive data	DE.CM-1, PR.DS-5	☐	☐	☐	
DP-3	Encrypt sensitive data in transit	PR.DS-2	☐	☐	☐	
DP-4	Enable data at rest encryption by default	PR.DS-1	☐	☐	☐	
DP-5	Use customer-managed key option in data at rest encryption when required	PR.DS-1, ID.AM-3	☐	☐	☐	
DP-6	Use a secure key management process	PR.AC-1, PR.DS-1	☐	☐	☐	
DP-7	Use a secure certificate management process	PR.AC-1, ID.AM-3	☐	☐	☐	
DP-8	Ensure security of key and certificate repository	PR.AC-1, PR.DS-1	☐	☐	☐	

5. Asset Management (AM)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-asset-management>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
AM-1	Track asset inventory and their risks	ID.AM-1, ID.AM-2, ID.AM-4	☐	☐	☐	
AM-2	Use only approved services	ID.AM-3, PR.IP-1, PR.PT-3	☐	☐	☐	
AM-3	Ensure security of asset lifecycle management	PR.IP-1, PR.IP-3, PR.MA-1	☐	☐	☐	
AM-4	Limit access to asset management	PR.AC-4, PR.AC-7, PR.PT-3	☐	☐	☐	
AM-5	Use only approved applications in virtual machine	PR.DS-6, PR.PT-2, DE.CM-4	☐	☐	☐	

6. Logging and Threat Detection (LT)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-logging-threat-detection>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
LT-1	Enable threat detection capabilities	DE.CM-1, DE.CM-4, DE.CM-7	☐	☐	☐	
LT-2	Enable threat detection for identity and access management	DE.CM-1, PR.AC-4, PR.IP-8	☐	☐	☐	
LT-3	Enable logging for security investigation	DE.AE-3, DE.CM-1, DE.CM-6, PR.PT-1	☐	☐	☐	

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
LT-4	Enable network logging for security investigation	DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-6, DE.CM-7	☐	☐	☐	
LT-5	Centralize security log management and analysis	DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-6, DE.CM-7, RS.AN-1	☐	☐	☐	
LT-6	Configure log storage retention	PR.PT-1, DE.CM-1	☐	☐	☐	
LT-7	Use approved time synchronization sources	DE.CM-1, PR.PT-1	☐	☐	☐	

7. Incident Response (IR)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-incident-response>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
IR-1	Preparation - update incident response plan and handling process	PR.IP-9, PR.IP-10, RS.CO-1	☐	☐	☐	
IR-2	Preparation - setup incident notification	RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4	☐	☐	☐	
IR-3	Detection and analysis - create incidents based on high-quality alerts	DE.CM-1, DE.CM-4, DE.CM-7, DE.AE-1, DE.AE-2	☐	☐	☐	
IR-4	Detection and analysis - investigate an incident	DE.AE-2, DE.AE-3, RS.AN-1, RS.AN-2, RS.AN-3	☐	☐	☐	
IR-5	Detection and analysis - prioritize incidents	DE.AE-1, RS.AN-1, RS.AN-5	☐	☐	☐	
IR-6	Containment, eradication and recovery - automate the incident handling	RS.RP-1, RS.MI-1, RS.MI-2, RS.MI-3	☐	☐	☐	
IR-7	Post-incident activity - conduct lessons learned and retain evidence	RS.RP-1, RS.IM-1, RS.IM-2	☐	☐	☐	

8. Posture and Vulnerability Management (PV)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-posture-vulnerability-management>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
PV-1	Define and establish secure configurations	PR.IP-1, PR.DS-6	☐	☐	☐	
PV-2	Audit and enforce secure configurations	DE.CM-7, PR.IP-1	☐	☐	☐	
PV-3	Define and establish secure configurations for compute resources	PR.IP-1, PR.DS-6, PR.PT-3	☐	☐	☐	

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
PV-4	Audit and enforce secure configurations for compute resources	DE.CM-7, DE.CM-8, PR.IP-1	☐	☐	☐	
PV-5	Perform vulnerability assessments	DE.CM-8, ID.RA-1	☐	☐	☐	
PV-6	Rapidly and automatically remediate vulnerabilities	PR.IP-12, RS.MI-3	☐	☐	☐	
PV-7	Conduct regular red team operations	DE.DP-4, ID.RA-10	☐	☐	☐	

9. Endpoint Security (ES)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-endpoint-security>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
ES-1	Use Endpoint Detection and Response (EDR)	DE.CM-1, DE.CM-4, DE.CM-7, RS.AN-1	☐	☐	☐	
ES-2	Use modern anti-malware software	DE.CM-4, PR.DS-6	☐	☐	☐	
ES-3	Ensure anti-malware software and signatures are updated	DE.CM-4, PR.IP-1	☐	☐	☐	

10. Backup and Recovery (BR)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-backup-recovery>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
BR-1	Ensure regular automated backups	PR.IP-4, RC.RP-1	☐	☐	☐	
BR-2	Protect backup and recovery data	PR.DS-1, PR.DS-5, PR.IP-4	☐	☐	☐	
BR-3	Monitor backups	DE.AE-3, DE.CM-1, RS.AN-1	☐	☐	☐	
BR-4	Regularly test backup	PR.IP-9, RC.RP-1	☐	☐	☐	

11. DevOps Security (DS)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-devops-security>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
DS-1	Conduct threat modeling	ID.RA-3, PR.IP-2	☐	☐	☐	
DS-2	Secure the software supply chain	ID.SC-2, ID.SC-4, DE.CM-8	☐	☐	☐	

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
DS-3	Secure the DevOps infrastructure	PR.AC-4, PR.DS-5, DE.CM-7	☐	☐	☐	
DS-4	Integrate Static Application Security Testing (SAST)	PR.IP-2, DE.CM-4	☐	☐	☐	
DS-5	Integrate Dynamic Application Security Testing (DAST)	DE.CM-4, PR.IP-12	☐	☐	☐	
DS-6	Secure the workload lifecycle	PR.IP-1, PR.IP-3, DE.CM-8	☐	☐	☐	
DS-7	Implement DevOps logging and monitoring	DE.CM-1, DE.CM-7, RS.AN-1	☐	☐	☐	

12. Artificial Intelligence Security (AI)

Source: <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-artificial-intelligence-security>

Control	Title (Microsoft)	NIST CSF (per Microsoft)	Compliant	Partial	Non-compliant	Evidence
AI-1	Ensure use of approved models	: ID.SC-04, GV.SC-06	☐	☐	☐	
AI-2	Implement multi-layered content filtering	: PR.DS-05, DE.CM-04	☐	☐	☐	
AI-3	Adopt safety meta-prompts	: PR.IP-03, PR.AT-01	☐	☐	☐	
AI-4	Apply least privilege for agent functions	: PR.AC-04, PR.PT-03	☐	☐	☐	
AI-5	Ensure human-in-the-loop	: PR.AC-07, DE.AE-02	☐	☐	☐	
AI-6	Establish monitoring and detection	: DE.CM-01, DE.AE-03	☐	☐	☐	
AI-7	Perform continuous AI Red Teaming	: ID.RA-01, RS.AN-03	☐	☐	☐	

Need help assessing your Azure environment? Request a quote: info@grdinc.ca, 514 291-9003.