Azure Security Best Practices

Identity management, network security groups, encryption, monitoring, and compliance controls for Azure environments. Secure your cloud infrastructure with these essential practices.

6	50+	Defend	Free
SECURITY DOMAINS	SECURITY CONTROLS	IN DEPTH STRATEGY	SECURITY CHECKLIST

How to Use This Checklist

Work through each section with your cloud administrator. These practices align with the Azure Security Benchmark and CIS Controls. Score each section to identify gaps. Prioritise high-impact controls first.

1 Identity & Access Management

Identity is the new perimeter in cloud security. Control who can access what and under what conditions.

- [ ] Enable **Azure AD MFA** for all users, with no exceptions for admin accounts
- [ ] Implement **Conditional Access** policies restricting sign-ins by location, device, and risk level
- [ ] Use **Privileged Identity Management (PIM)** for just-in-time admin access with approval workflows
- [ ] Limit **Global Admin** accounts to maximum 2–3, with break-glass emergency account
- [ ] Enforce **RBAC (Role-Based Access Control)** with least-privilege principles for all Azure resources
- [ ] Disable **legacy authentication protocols** (Basic Auth) that cannot support MFA
- [ ] Enable **Azure AD Identity Protection** to detect and respond to risky sign-ins
- [ ] Review **access assignments** quarterly using Azure AD Access Reviews

Section Score: ____/10

2 Network Security

Protect your Azure network with layered security controls.

- [ ] Deploy **Network Security Groups (NSGs)** on all subnets with deny-all-inbound defaults
- [ ] Use **Azure Firewall** or third-party NVA for centralised traffic filtering and inspection
- [ ] Implement **hub-and-spoke** network topology for centralised security control
- [ ] Enable **NSG flow logs** and send to Log Analytics for traffic analysis
- [ ] Use **Azure Private Endpoints** for PaaS services to eliminate public internet exposure
- [ ] Implement **DDoS Protection Standard** on production virtual networks
- [ ] Disable **public IP addresses** on VMs unless absolutely required (use Azure Bastion for admin access)
- [ ] **Just-in-Time VM Access** is enabled to restrict management port access to when needed

Section Score: _____ /10

3 Data Protection & Encryption

- [ ] All storage accounts use **Azure Storage Service Encryption** (AES-256, enabled by default)
- [ ] **Azure Disk Encryption** (BitLocker) is enabled on all VM OS and data disks
- [ ] Database encryption is enabled: **Transparent Data Encryption (TDE)** for Azure SQL
- [ ] **Key Vault** is used to manage all encryption keys, secrets, and certificates centrally
- [ ] Key Vault access is restricted via **RBAC and network rules** (no public access)
- [ ] **TLS 1.2 minimum** is enforced on all Azure services and storage accounts
- [ ] **Customer-managed keys (CMK)** are used for sensitive workloads requiring additional key control

Section Score: ____ /10

4 Monitoring & Threat Detection

- [ ] **Microsoft Defender for Cloud** is enabled on all subscriptions with Security Posture management
- [ ] **Azure Monitor** and Log Analytics workspace collect logs from all resources
- [ ] **Diagnostic settings** are configured on all critical resources to send logs to Log Analytics
- [ ] **Azure Sentinel (SIEM)** or equivalent is deployed for security event correlation and response
- [ ] **Alert rules** are configured for: failed sign-ins, resource deletion, NSG changes, privilege escalation
- [ ] **Azure Activity Log** is retained for minimum 90 days and monitored for suspicious changes
- [ ] **Azure Advisor** recommendations are reviewed monthly for security improvements

Section Score: ____ /10

5 Backup & Recovery

- [ ] **Azure Backup** is configured for all VMs, databases, and file shares
- [ ] Backup policies enforce **appropriate retention** (daily 30 days, weekly 12 weeks, monthly 12 months)
- [ ] **Soft delete** is enabled on Azure Backup to prevent accidental or malicious backup deletion
- [ ] Backup **restore tests** are conducted monthly with documented results
- [ ] **Azure Site Recovery** is configured for critical workloads with cross-region replication
- [ ] **Immutable backup vaults** are used to protect against ransomware deleting backups

Section Score: ____ /10

#	AREA	SCORE	PRIORITY
1	Identity & Access Management	/ 10	H / M / L
2	Network Security	/ 10	H / M / L
3	Data Protection	/ 10	H / M / L
4	Monitoring & Threat Detection	/ 10	H / M / L
5	Backup & Recovery	/ 10	H / M / L
TOTAL SCORE		**/ 50**	

Score Interpretation

80–100: Excellent — well-managed with only minor improvements needed.
60–79: Good foundation but gaps exist. Prioritise areas scoring below 6.
Below 60: Significant gaps putting your business at risk. Seek specialist review.

! Action Items & Notes

Top 3 Priority Actions:

1.
2.
3.

Notes

Need Azure Security Hardening?

Our cloud security engineers audit and harden Azure environments to best-practice security standards.

info@cloudswitched.com

New London House, 6 London St, London EC3R 7LP

Completed by: Date: Next review:

© 2026 CloudSwitched Limited. All rights reserved. This resource is provided for informational purposes and does not constitute professional IT advice.