CLOUDSWITCHED

FREE RESOURCE — BEST PRACTICES CHECKLIST

Azure Security Best Practices

Audit your Microsoft Azure tenant against eight control areas covering Entra ID, RBAC and PIM, network security groups, encryption and Key Vault, storage and database hardening, Defender for Cloud, monitoring and Sentinel, and backup resilience. Score each area to surface the gaps Defender for Cloud and a real attacker will find first.

8	60+	/10	Fillable
CONTROL AREAS COVERED	AUDIT ITEMS TO CHECK	SCORE EACH SECTION	TICK & TYPE IN ANY VIEWER

ENTRA ID · PIM & JIT · DEFENDER · SENTINEL

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this checklist

Work through each of the eight sections with whoever owns your Azure estate — in-house cloud team, MSP, or both. Tick every checkpoint that is **fully in place** across every production subscription — not partially, not "we're scoping it", but with evidence visible in the portal, via Azure CLI, or in an Azure Policy compliance report. Then award each section a score out of 10 based on how many checkpoints you can confidently tick.

A score **below 6 in any section** is the kind of gap Defender for Cloud, a Microsoft Cloud Security Benchmark scan, or a real-world attacker will land on first. Use the action items page at the back to commit to your top three priorities. This is an **interactive PDF** — tick the boxes and type your scores and notes directly in any modern PDF viewer.

> **WHAT THIS CHECKLIST IS**
>
> A baseline self-assessment for UK SMEs and mid-market organisations running production workloads in Microsoft Azure. It maps to the **Microsoft Cloud Security Benchmark (MCSB)** and the Azure Well-Architected Security pillar, and covers the controls that drive your Defender for Cloud Secure Score. It is not a CIS Azure Foundations audit and does not replace an ISO 27001 review, but it surfaces the controls those regimes — and a real Azure intrusion — rely on.

Tenant & subscription under review

ENTRA TENANT ID _____

PRIMARY SUBSCRIPTION _____

DEFENDER SECURE SCORE BASELINE _____

The eight sections

- **01 Identity & Entra ID** — MFA, Conditional Access, legacy auth, sign-in risk policies.
- **02 RBAC & Privileged Access (PIM/JIT)** — least privilege, eligible roles, access reviews.
- **03 Network Security Groups & Hardening** — NSG rules, Bastion, Private Endpoints, WAF.
- **04 Encryption & Key Vault** — SSE, CMK, TLS, HSM keys, secret rotation, purge protection.
- **05 Storage & Database Security** — public blob, firewall, TDE, SQL Defender, auditing.
- **06 Defender for Cloud & Secure Score** — Defender plans, MCSB, regulatory compliance.
- **07 Monitoring, Logging & Sentinel** — diagnostic settings, Log Analytics, Sentinel, alerts.
- **08 Backup, Recovery & Resilience** — Recovery Services Vault, soft-delete, ASR, DR runbook.

01

Identity & Entra ID (Azure AD)

Identity is the perimeter in Azure — the overwhelming majority of cloud incidents begin with a credential, a token, or a legacy auth protocol. Audit Entra ID against the modern Conditional Access / MFA baseline before anything else.

- ☐ **MFA is enforced for every administrator** (Global Admin, Security Admin, Billing Admin, application admins) with no exceptions.
- ☐ **Conditional Access policies** require MFA for all users at all times, or Security Defaults are enabled tenant-wide.
- ☐ **Legacy authentication is blocked** (POP, IMAP, SMTP AUTH, legacy Exchange Web Services) via Conditional Access.
- ☐ There are **at least two break-glass Global Admin accounts**, excluded from CA, with monitored sign-ins and stored credentials.
- ☐ **Sign-in and user risk policies** (Identity Protection) are configured to block or require MFA on medium/high risk events.
- ☐ **Guest (B2B) access is restricted**: external invites limited to specific admins, guest access reviewed quarterly.
- ☐ **Self-service password reset (SSPR)** is enabled with strong authentication methods (no security questions).
- ☐ **App consent** is restricted to verified publishers or admin-approved apps; user consent for risky permissions is disabled.

WHAT GOOD LOOKS LIKE

Every interactive sign-in is gated by Conditional Access. Legacy auth is zero in the sign-in logs. Global Admins number fewer than five, are MFA-enforced, and only two break-glass accounts are excluded. Identity Protection risk events trigger blocks within seconds, not days.

SECTION 01 SCORE _____ / **10** *Aim for 9+. Below 6 = identity compromise risk.*

02

RBAC & Privileged Access (PIM / JIT)

Standing Owner / Contributor at subscription scope is the most common Azure misconfiguration. Verify that least privilege is enforced with named roles, that Privileged Identity Management is in production, and that JIT access is the only path to admin.

- **Role-Based Access Control** is used throughout — no classic co-administrators, no legacy management certificates.
- **No standing Owner or Contributor** at the subscription or management group root — only at the resource group level for specific workloads.
- **Entra PIM** is licensed (P2) and configured for all privileged Entra and Azure resource roles, with MFA on activation.
- **JIT VM access** via Defender for Cloud is enforced for any IaaS VM that ever needs RDP/SSH; no permanent inbound mgmt ports.
- **Custom roles** are reviewed and minimised; built-in least-privilege roles are preferred wherever possible.
- All **PIM activations are logged** to Log Analytics or Sentinel with alerting on high-risk role activations.

Quarterly access review log — complete after each PIM / JIT review

PRIVILEGED ROLE	REVIEW DATE	REVIEWER	NEXT REVIEW
Global Administrator	_____	_____	_____
Privileged Role Admin	_____	_____	_____
Subscription Owner / Contributor	_____	_____	_____
JIT VM access approvers	_____	_____	_____

SECTION 02 SCORE _____ / 10 *Aim for 9+. Below 6 = privilege sprawl risk.*

03

Network Security Groups & Hardening

Most Azure VMs are exposed to the public internet by an over-permissive NSG, not by an exotic exploit. Walk every NSG rule with the cloud team and verify management ports are never open to 0.0.0.0/0.

- ☐ No NSG inbound rule allows 0.0.0.0/0 to **port 22 (SSH), 3389 (RDP), 1433 (SQL), 3306 (MySQL)** or any other management port.
- ☐ Every NSG ends with an **explicit deny-all**; the default platform rules are not relied on for protection.
- ☐ **Azure Bastion** or Defender JIT VM Access is used for admin RDP/SSH — no public IPs on jump hosts.
- ☐ **Private Endpoints** are used for PaaS services (Storage, SQL, Key Vault) so traffic never traverses the public internet.
- ☐ **Azure DDoS Protection Standard** is enabled on production VNets carrying internet-facing workloads.
- ☐ **Azure Firewall Premium** or a partner NGFW protects egress from production subnets with TLS inspection.
- ☐ A **WAF** (Application Gateway or Front Door) sits in front of every public HTTP(S) workload with OWASP rule set enabled.
- ☐ **NSG flow logs** are enabled and shipped to Log Analytics via Traffic Analytics for visibility.

WATCH OUT FOR

Default NSGs with leftover `Allow 22 from Any` rules from the dev phase — they get inherited every time a new VM is built from the gold image. Run `az network nsg rule list` across every subscription and grep for 0.0.0.0/0.

SECTION 03 SCORE _____ / **10** *Aim for 9+. Below 6 = exposed management plane.*

04

Encryption & Key Vault

Azure encrypts most things at rest by default with platform-managed keys — but compliance, data residency, and a real BYOK story all need customer-managed keys, hardened Key Vaults, and a secrets-rotation discipline.

- **Storage Service Encryption (SSE)** is verified on every Storage account; **encryption with customer-managed keys (CMK)** is used where data classification demands it.
- **Azure Disk Encryption** or platform-managed SSE is enabled on every managed disk; OS and data disks are covered.
- **TLS 1.2+ minimum** is enforced on every Storage account, App Service, SQL DB, and Function; TLS 1.0 / 1.1 disabled.
- Key Vault uses **RBAC permission model** (not legacy access policies) with least-privilege role assignments.
- **Soft-delete and purge protection** are enabled on every Key Vault — with retention ≥ 90 days.
- Sensitive keys are **HSM-backed** (Premium tier) or in Managed HSM where regulatory scope demands it.
- **Secrets rotation** is automated (Event Grid + Function, or Managed Identity), with expiry alerts at 30/14/7 days.
- Key Vault is reachable only via **Private Endpoint or service-tag firewall** — not over the public internet.

SOFT-DELETE IS NON-NEGOTIABLE

Without soft-delete and purge protection, a compromised contributor can permanently delete a Key Vault and every key in it — a single-step path to data loss. Verify both flags via `az keyvault show` on every vault in scope.

SECTION 04 SCORE _____ / **10** *Aim for 9+. Below 6 = data exposure risk.*

05

Storage & Database Security

Anonymous blob containers and SQL servers exposed to 0.0.0.0/0 are still the headline cause of public Azure data breaches. Audit every Storage account and every database against the modern hardening baseline.

- **Allow Blob Anonymous Access** is disabled at the Storage account level for every account that does not specifically host public assets.
- Storage account **firewall is set to deny by default**; access is via Private Endpoint, service endpoint, or specific IP allow-list.
- Storage account **shared keys are disabled** where possible; Entra-based auth or short-lived SAS tokens are used instead.
- **Soft-delete on blobs, containers, and Storage accounts** is enabled with retention ≥ 14 days; versioning is on for critical data.
- **Transparent Data Encryption (TDE)** is on for every Azure SQL DB and Managed Instance; CMK used for regulated workloads.
- **Microsoft Defender for SQL** is enabled with vulnerability assessment and Advanced Threat Protection alerts wired to the SOC.
- **SQL auditing** writes to a Log Analytics workspace or immutable Storage; retention covers regulatory minimum (12+ months).
- No SQL server has **“Allow Azure services”** set without explicit business justification; firewall ranges are tight and reviewed.

CRITICAL — ANONYMOUS BLOB

A single misconfigured anonymous blob container has been the root cause of the most expensive Azure data breaches in the UK SME and public sector. Enforce `allowBlobPublicAccess: false` via Azure Policy across every subscription, not just on a checklist.

SECTION 05 SCORE _____ / **10** *Aim for 9+. Below 6 = data leak risk.*

06

Defender for Cloud & Secure Score

Defender for Cloud is the central posture-management and CWPP layer for Azure. Enabling the right plans and acting on the Secure Score is the highest-leverage thing a UK Azure tenant can do this quarter.

- ☐ **Microsoft Defender for Cloud** is enabled on every production subscription with the free CSPM tier as a minimum.
- ☐ Workload protection plans are enabled where used: **Servers (P2), App Service, Storage, SQL, Containers, Key Vault, DNS, ARM, APIs**.
- ☐ **Auto-provisioning** for Log Analytics agent / Azure Monitor agent and Defender agent is on across the management group root.
- ☐ The **Microsoft Cloud Security Benchmark (MCSB)** regulatory standard is assigned and reviewed monthly.
- ☐ Other applicable regulatory standards (**CIS Azure 2.0, ISO 27001, NIST 800-53, PCI DSS, UK Cyber Essentials**) are assigned where required.
- ☐ **Email notifications** for Defender alerts are configured for owners and on a high-severity escalation list.
- ☐ **Defender CSPM (Premium)** is enabled where attack-path analysis and external attack-surface management are needed.
- ☐ Secure Score has a **named owner**, a target band, and a quarterly trend review with the business sponsor.

Current Secure Score (per subscription)

THIS-MONTH SCORE	12-MONTH TREND	90-DAY TARGET

SECTION 06 SCORE _____ / **10** *Aim for 8+. Below 6 = posture blind.*

07

Monitoring, Logging & Sentinel

You cannot investigate what you have not logged. Verify that diagnostic settings exist on every resource, that activity and platform logs ship to a long-retention store, and that high-fidelity detections route to a 24/7 channel.

- ☐ **Diagnostic settings** are configured on every Azure resource to send logs and metrics to a central Log Analytics workspace.
- ☐ **Activity logs** for every subscription are exported to Log Analytics with retention ≥ 365 days, plus archive to immutable Storage.
- ☐ Entra ID **sign-in and audit logs** are streamed to Log Analytics / Sentinel; user risk events are alerted on in real time.
- ☐ **Microsoft Sentinel** (or another SIEM ingesting Azure connectors) is deployed; standard analytics rules and UEBA are enabled.
- ☐ Sentinel **data connectors** are on for Entra ID, Office 365, Defender XDR, Azure Activity, and key PaaS resources.
- ☐ High-severity alerts route to a **24/7 monitored channel** (in-house SOC, MSP, or MDR) with a defined response SLA.
- ☐ **Service Health, Resource Health** and budget alerts are configured; cost anomalies trigger investigation.

WATCH OUT FOR — MISSING DIAGNOSTIC SETTINGS

The single most common forensic dead-end after an Azure incident is “diagnostic settings were never configured on Key Vault / Storage / NSG”. Enforce diagnostic-setting policies at the management group level via **built-in Azure Policy DINE rules** so every new resource is logged by default.

SECTION 07 SCORE _____ / **10**

Aim for 8+. Below 6 = blind to intrusion.

08

Backup, Recovery & Resilience

Resilience is what carries you through the day everything else has already failed. Verify the Recovery Services Vault is hardened against tampering, that backup restores have actually been tested, and that DR is more than a spreadsheet.

- ☐ A **Recovery Services Vault** (or Backup Vault for newer SKUs) exists in every region, protecting every tier-1 workload.
- ☐ **Soft-delete on backups** is enabled with a 14-day minimum and Multi-User Authorization (MUA) protecting destructive operations.
- ☐ **Immutable backup vaults** are configured for ransomware-resilient retention on critical workloads.
- ☐ Storage and databases use **geo-redundant or zone-redundant** replication aligned with RPO; replication health is monitored.
- ☐ A **full restore test** for at least one tier-1 workload has been performed in the last 6 months with documented outcome.
- ☐ **Azure Site Recovery (ASR)** protects tier-1 VMs to a secondary region with a documented and rehearsed failover plan.
- ☐ **Resource locks** (CanNotDelete or ReadOnly) protect production resource groups, vaults, and management group landing zones.
- ☐ A written **disaster recovery runbook** exists with named roles, escalation, RTO/RPO and contact tree; tabletop in the last 12 months.

THE RESTORE TEST RULE

A backup that has never been restored is not a backup — it is a hope. Quarterly: pick a random tier-1 workload, restore it to a sandbox, document the timing, and update the runbook. The 30-minute drill saves the 24-hour outage.

SECTION 08 SCORE _____ / 10 *Aim for 9+. Below 6 = ransomware exposure.*

Σ

Posture score summary

Transfer the score for each section into the table. Set a priority (H/M/L) based on the gap to target. Anything below 6 is a candidate for the top-3 actions on the next page.

#	CONTROL AREA	SCORE / 10	PRIORITY
01	Identity & Entra ID	_____ / 10	☐ H ☐ M ☐ L
02	RBAC & Privileged Access (PIM/JIT)	_____ / 10	☐ H ☐ M ☐ L
03	Network Security Groups & Hardening	_____ / 10	☐ H ☐ M ☐ L
04	Encryption & Key Vault	_____ / 10	☐ H ☐ M ☐ L
05	Storage & Database Security	_____ / 10	☐ H ☐ M ☐ L
06	Defender for Cloud & Secure Score	_____ / 10	☐ H ☐ M ☐ L
07	Monitoring, Logging & Sentinel	_____ / 10	☐ H ☐ M ☐ L
08	Backup, Recovery & Resilience	_____ / 10	☐ H ☐ M ☐ L
Σ	**TOTAL SCORE**	_____ / 80	—

SCORING GUIDANCE

Award one point per checkpoint where you have evidence the control is in place — a portal screenshot, a policy assignment, a Defender recommendation passed, a KQL query result. Half-measures and "on the roadmap" do not score. Round each section to the nearest whole number out of 10.

Interpretation & priority actions

Translate your total score into a risk band, then commit to a small number of next steps. The goal is one page of decisions, not a wish list.

Score interpretation (out of 80)

65–80	**Strong.** Azure posture is mature. Focus on Defender CSPM tuning, attack-path remediation and DR drills.
48–64	**Foundational, gaps exist.** Prioritise any area scoring below 6 with named owners and Defender Secure Score deadlines.
Below 48	**Material risk.** Commission a formal Azure security review and an MCSB-aligned remediation plan.

Top 3 priority actions

01 _____

02 _____

03 _____

Additional notes

_____

_____

_____

ASSESSMENT COMPLETED BY _____ DATE _____ NEXT REVIEW DUE _____

CLOUDSWITCHED

CLOUD SECURITY & AZURE SERVICES

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom