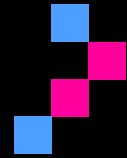


Cloud Security Best Practices



Initial
TECH

Overview

This simple, client-friendly guide helps small and mid-market organisations secure cloud services (SaaS, PaaS, IaaS). It follows recognised guidance from the UK NCSC 14 Cloud Security Principles, the ACSC Small Business Cloud Security Guides, CISA's SCuBA baselines, and Microsoft/AWS/Google shared responsibility models. Start with the quick wins, then work through each checklist.

How to use this guide

- 1) Decide what you are securing (Microsoft 365, Google Workspace, AWS/Azure workloads, specific SaaS apps).
- 2) For each section, complete the tasks, tick Status, and paste screenshots/links under Evidence.
- 3) Use a quarterly review to keep protections current and fix gaps.
- 4) Keep this simple: focus on identities, data, configuration, and logging.

Quick Wins (do these first)

- Turn on Multi-Factor Authentication (MFA) for all users/admins and block legacy/basic authentication.
- Apply secure presets/baselines (e.g., Microsoft 365 preset policies, CISA SCuBA baselines).
- Encrypt data at rest and in transit; manage keys securely.
- Enable central logging and alerts; review weekly.
- Back up critical data using 3-2-1-1-0 (one immutable/offline copy) and test restores.

Shared responsibility (who secures what?)

On-prem: YOU secure everything

IaaS: Provider secures hardware/network; YOU secure OS, apps, identities, data

PaaS: Provider secures platform; YOU secure identities, data, configs

SaaS: Provider secures app; YOU secure users, data, settings

1. Know your shared responsibility

Understand what your cloud provider secures and what you must configure. Responsibilities differ across SaaS, PaaS and IaaS.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Document your service types	List SaaS (e.g., M365), PaaS (databases), IaaS (VMs).		
Write a one-page “who secures what” summary	Use provider docs (AWS/Azure/Google) to note your duties for identities, configs, data and logging.		
Train your team on SRM basics	Include in onboarding; focus on identity, configuration, data, and monitoring.		

2. Identity & access (Zero Trust)

Strong identities stop most attacks. Enforce MFA, least privilege, and conditional access.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Enforce MFA for all users and admins	Prefer authenticator apps or passkeys; require phishing-resistant methods for admins.		
Block legacy/basic authentication	Disable protocols that bypass MFA; use conditional access templates.		
Apply least privilege and role-based access	Use roles, limit global admins, review access quarterly.		
Rotate keys/tokens and remove stale accounts	Audit service principals; rotate secrets regularly.		

3. Data protection (encryption & key management)

Encrypt data in transit and at rest; manage keys properly and classify sensitive data.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Enable TLS/HTTPS everywhere	Force HTTPS for sites and APIs; redirect HTTP to HTTPS.		
Turn on encryption at rest	Use provider KMS; encrypt storage, databases and backups.		
Define key management policies	Use customer-managed keys where required; rotate keys; restrict access.		
Classify sensitive data and apply labels/DLP	Mark confidential data; apply policies to stop oversharing.		

4. Secure configuration & baselines

Start from known baselines; use presets and policy-as-code to avoid misconfigurations.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Apply vendor baselines/presets	Use Microsoft presets/Defender policies or CISA SCuBA baselines for M365/GWS.		
Use configuration drift detection	Enable policy/compliance dashboards (e.g., Secure Score, Defender for Cloud).		
Harden SaaS settings	Disable risky sharing, require owner approval, limit external apps.		
Patch regularly	Keep services, agents and clients updated.		

5. Logging & monitoring

Centralise logs, enable alerts, and review findings weekly.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Enable unified audit logging	Turn on audit logs for M365/GWS/AWS/Azure; send to SIEM.		
Set priority alerts	Alert on admin changes, MFA disabled, external sharing, failed logins.		
Run weekly reviews	Assign owner to check dashboards and triage alerts.		
Test incident response	Tabletop exercise: simulate a compromised account and walk through steps.		

6. Backups & resilience (3-2-1-1-0)

Keep one immutable/offline copy and verify restores to survive ransomware or data loss.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Adopt 3-2-1-1-0	Three copies, two media, one offsite, one immutable/offline, zero-error restore tests.		
Separate backup identities	Use distinct credentials/tenants for backup systems.		
Quarterly restore tests	Measure RTO/RPO and fix bottlenecks.		

7. Vendor & supply chain (SaaS due diligence)

Ask cloud vendors for security evidence and align to a framework like CSA CCM.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Request a CAIQ/STAR or security summary	Ask for CCM control coverage, certifications and data location.		
Define app approval workflow	Route requests to security/IT; document allowed scopes/permissions.		
Review vendors yearly	Re-check security posture and contracts.		

Action plan (next steps)

Action	Owner	Due date	Resources	Status

References

- NCSC 14 Cloud Security Principles (shared responsibility, encryption, governance)
- ACSC Small Business Cloud Security Guides (M365/Chromebook)
- CISA SCuBA secure baselines & ScubaGear (M365/GWS)
- Shared responsibility model: AWS, Azure, Google
- CSA Cloud Controls Matrix (CCM v4)
- Backup best practice: 3-2-1-1-0 and immutable/offline copies