CMMC Practical Implementation Guide

Aligned to the BK17 assessment workbook

This guide is written for organisations that are new to CMMC. It explains, control by control, what each requirement is trying to achieve, what needs to be put in place, and what a sensible end state looks like in practice. The control labels in this guide follow the workbook format so customers can move between the guide and the workbook easily.

How to use this guide

1. Read the control purpose so you understand what problem the control is trying to solve.
2. Use the implementation line as a practical to-do list.
3. Compare the good outcome to your current environment and note the gap in the workbook.

Important

Controls in the same domain are not the same. For example, one Access Control requirement is about getting users into systems, another is about limiting what they can do, another is about locking sessions, and another is about removing access when it is no longer needed.

Access Control (AC)

AC.1 - Account approval and creation
What this control is doing: Stops unapproved people getting into systems.
What you need to put in place: Use a formal joiner process, named accounts, manager approval, and MFA before access is granted.
What good looks like: Every active account has an owner, approval, and a valid business reason.

AC.2 - Least privilege
What this control is doing: Prevents users having more access than they need.
What you need to put in place: Build role-based access profiles and remove admin rights from standard users.
What good looks like: Most users are standard users and permissions match job role.

AC.3 - Control internal information flow
What this control is doing: Stops data moving freely between systems and teams.
What you need to put in place: Use network segmentation, firewall rules, and restricted shares between environments.
What good looks like: Systems only talk to other systems when there is a defined need.

AC.4 - Separation of duties
What this control is doing: Reduces fraud and error by splitting critical tasks.
What you need to put in place: Separate request, approval, implementation, and review for sensitive actions.
What good looks like: No single person can approve and execute the same critical action alone.

AC.5 - Control privileged functions
What this control is doing: Limits who can perform administrator actions.
What you need to put in place: Use separate admin accounts and restrict privileged tools to authorised staff.
What good looks like: You know exactly who has elevated rights and why.

AC.6 - Use non-privileged accounts for daily work
What this control is doing: Stops admins working with unnecessary elevated rights all day.
What you need to put in place: Give IT staff a normal account for routine work and a separate admin account for elevated tasks.
What good looks like: Admin accounts are only used when a privileged task is actually required.

AC.7 - Prevent unauthorised privilege escalation
What this control is doing: Stops users making themselves admins.
What you need to put in place: Remove local admin rights and block unauthorised elevation or software installation.
What good looks like: Users cannot elevate privileges without an approved path.

AC.8 - Protect against repeated failed logins
What this control is doing: Reduces brute-force password attacks.
What you need to put in place: Set lockout thresholds, delay controls, and alerts for repeated failures.
What good looks like: Accounts lock or trigger alerts after repeated bad passwords.

AC.9 - Display acceptable use warning
What this control is doing: Makes it clear systems are for authorised use only.
What you need to put in place: Configure a login banner on laptops, servers, VPN, and other business systems.
What good looks like: Users see a warning before they sign in.

AC.10 - Lock unattended sessions
What this control is doing: Stops someone using a device left open on a desk.
What you need to put in place: Set automatic screen lock after a short period of inactivity.
What good looks like: Idle devices lock automatically without relying on user discipline.

AC.11 - Terminate stale sessions
What this control is doing: Prevents old sessions remaining active indefinitely.
What you need to put in place: Use session timeouts on web apps, admin consoles, and remote access tools.
What good looks like: Long-idle sessions end automatically and require re-authentication.

AC.12 - Secure remote access
What this control is doing: Protects access from outside the office.
What you need to put in place: Use VPN or zero-trust remote access with MFA and device checks.
What good looks like: Remote access is encrypted, approved, and restricted to trusted users and devices.

AC.13 - Secure wireless access
What this control is doing: Protects corporate Wi-Fi from weak or shared access.
What you need to put in place: Use WPA2/3 Enterprise, separate guest Wi-Fi, and unique authentication.
What good looks like: Corporate wireless is authenticated and isolated from guest access.

AC.14 - Control mobile devices
What this control is doing: Reduces risk from phones, tablets, and laptops used off-site.
What you need to put in place: Use MDM, encryption, screen lock, and remote wipe for managed devices.
What good looks like: Only managed and compliant mobile devices can access business systems.

AC.15 - Control external system connections
What this control is doing: Stops unknown third-party connections to your environment.
What you need to put in place: Approve and document partner links, remote support paths, and integrations.
What good looks like: Every external connection is known, justified, and controlled.

AC.16 - Protect public-facing systems
What this control is doing: Prevents public systems exposing internal resources or sensitive data.
What you need to put in place: Place public services in segregated zones and restrict backend access.
What good looks like: Public websites or portals cannot be used as a bridge into internal systems.

AC.17 - Restrict access to sensitive data
What this control is doing: Ensures CUI is only available to the right people.
What you need to put in place: Apply data-level permissions, secure folders, and need-to-know access rules.
What good looks like: Sensitive data is not visible to general users.

AC.18 - Review access regularly
What this control is doing: Cleans up access that is no longer needed.
What you need to put in place: Run scheduled access reviews for users, admins, and shared resources.
What good looks like: Unused or excessive access is identified and removed on a routine basis.

AC.19 - Monitor account use
What this control is doing: Helps spot misuse, compromise, or unusual user activity.
What you need to put in place: Use alerts for unusual logins, impossible travel, mass downloads, or dormant account use.
What good looks like: Suspicious account behaviour is detected and investigated.

AC.20 - Monitor privileged account activity
What this control is doing: Provides oversight of administrator actions.
What you need to put in place: Log admin actions, use PAM where possible, and review privileged activity.
What good looks like: High-risk admin actions are visible and attributable to a named person.

AC.21 - Remove access when no longer needed
What this control is doing: Closes accounts quickly when people leave or change role.
What you need to put in place: Tie offboarding and role changes to IT deprovisioning and access updates.
What good looks like: Leavers and movers do not retain legacy access.

AC.22 - Control temporary and emergency access
What this control is doing: Stops short-term access quietly becoming permanent.
What you need to put in place: Use expiry dates, approvals, and post-use reviews for temporary access.
What good looks like: Temporary access expires automatically and is reviewed after use.

Awareness and Training (AT)

AT.1 - Security awareness training
What this control is doing: Builds baseline security behaviour across the organisation.
What you need to put in place: Deliver mandatory annual training on phishing, passwords, data handling, and reporting.
What good looks like: All staff complete training and understand core security expectations.

AT.2 - Role-based security training
What this control is doing: Gives higher-risk roles the extra depth they need.
What you need to put in place: Provide additional training for admins, developers, helpdesk, and managers.
What good looks like: People in sensitive roles understand the risks and controls relevant to their job.

AT.3 - Insider threat awareness
What this control is doing: Helps staff recognise harmful behaviour from within the organisation.
What you need to put in place: Include insider risk indicators and reporting routes in training and policy.
What good looks like: Staff know how to report suspicious internal behaviour or misuse.

Audit and Accountability (AU)

AU.1 - Generate audit logs
What this control is doing: Creates a record of important activity on systems.
What you need to put in place: Enable logging on key systems, applications, identity platforms, and security tools.
What good looks like: You can tell who did what, when, and on which system.

AU.2 - Retain logs
What this control is doing: Keeps logs available long enough to investigate issues.
What you need to put in place: Define retention periods and ensure storage supports them.
What good looks like: Required logs are still available when needed for review or investigation.

AU.3 - Review logs
What this control is doing: Turns collected logs into useful detection and oversight.
What you need to put in place: Assign ownership for log review and define what must be checked.
What good looks like: Important events are routinely reviewed rather than ignored.

AU.4 - Alert on audit logging failures
What this control is doing: Stops blind spots caused by broken logging.
What you need to put in place: Set alerts when logging services stop, storage fills, or agents fail.
What good looks like: You know quickly when your visibility has degraded.

AU.5 - Synchronise time
What this control is doing: Makes events line up properly across different systems.
What you need to put in place: Use a central time source such as NTP across servers, endpoints, and network devices.
What good looks like: Timestamps are consistent enough to reconstruct events accurately.

AU.6 - Protect audit logs
What this control is doing: Stops attackers or admins tampering with the evidence.
What you need to put in place: Restrict access, prevent unauthorised deletion, and store logs securely.
What good looks like: Logs cannot be altered without detection or privileged approval.

AU.7 - Reduce and report audit data
What this control is doing: Turns large volumes of logs into meaningful security information.
What you need to put in place: Use filtering, dashboards, or SIEM rules to highlight significant events.
What good looks like: Reviewers see relevant signals instead of being buried in noise.

AU.8 - Correlate events across systems
What this control is doing: Helps identify attacks that span multiple systems.
What you need to put in place: Use central logging or SIEM correlation to connect identity, endpoint, and network events.
What good looks like: Related activity from different sources can be viewed as one incident trail.

AU.9 - Maintain enough log storage
What this control is doing: Prevents logs being lost because storage runs out.
What you need to put in place: Size storage correctly and monitor capacity thresholds.
What good looks like: Logs are retained as planned and not overwritten too early.

Configuration Management (CM)

CM.1 - Establish secure baselines
What this control is doing: Defines the approved secure state for systems.
What you need to put in place: Create baseline configurations for servers, workstations, cloud services, and network devices.
What good looks like: Systems start from a documented secure standard rather than ad hoc setup.

CM.2 - Control changes formally
What this control is doing: Prevents undocumented or risky changes.
What you need to put in place: Use change requests, approvals, testing, and scheduling for material changes.
What good looks like: You can trace why a change happened, who approved it, and when.

CM.3 - Deploy approved changes consistently
What this control is doing: Ensures authorised changes are actually applied correctly.
What you need to put in place: Use controlled deployment methods and validation after release.
What good looks like: Systems reflect the approved change and not an improvised variation.

CM.4 - Assess security impact of changes
What this control is doing: Stops change activity introducing new weaknesses.
What you need to put in place: Check each significant change for security, access, logging, and resilience impact.
What good looks like: Security is considered before changes go live, not after problems appear.

CM.5 - Restrict who can change configurations
What this control is doing: Limits configuration changes to authorised people.
What you need to put in place: Use privileged roles and restricted admin access for change tools.
What good looks like: Only approved staff can alter critical settings.

CM.6 - Define secure configuration settings
What this control is doing: Locks down key settings such as passwords, protocols, and hardening options.
What you need to put in place: Document required settings and push them via tooling where possible.
What good looks like: Essential security settings are standardised and enforced.

CM.7 - Enable only necessary functionality
What this control is doing: Reduces the attack surface of systems.
What you need to put in place: Disable unused services, ports, software, and features.
What good looks like: Systems run only what is needed for business use.

CM.8 - Maintain asset inventory
What this control is doing: Ensures you know what hardware and software exists.
What you need to put in place: Keep an up-to-date inventory with owner, location, and purpose.
What good looks like: There are no unknown systems carrying business data or connecting to the network.

CM.9 - Track configuration history
What this control is doing: Lets you see how systems changed over time.
What you need to put in place: Retain version history, backup configs, and change records.
What good looks like: You can compare current configuration to previous states and understand drift.

Identification and Authentication (IA)

IA.1 - Use unique user identities
What this control is doing: Makes every action attributable to one person or service.
What you need to put in place: Give each user a unique account and stop shared credentials.
What good looks like: Every login can be traced to a specific named owner.

IA.2 - Authenticate users securely
What this control is doing: Confirms users are who they claim to be.
What you need to put in place: Use strong passwords and MFA where required.
What good looks like: Access depends on more than a weak password alone.

IA.3 - Identify devices
What this control is doing: Ensures only known devices interact with managed services.
What you need to put in place: Use device registration, certificates, or MDM enrolment.
What good looks like: You can tell whether a device is approved before granting access.

IA.4 - Control account identifier lifecycle
What this control is doing: Manages the creation, change, and removal of identities cleanly.
What you need to put in place: Use processes for account naming, updates, disablement, and deletion.
What good looks like: Account identifiers are created consistently and retired promptly.

IA.5 - Manage authenticators securely
What this control is doing: Protects passwords, secrets, keys, and tokens.
What you need to put in place: Use password rules, secret storage, and secure reset processes.
What good looks like: Credentials are not weak, exposed, or handled informally.

IA.6 - Limit authentication feedback
What this control is doing: Prevents login messages helping attackers guess accounts or passwords.
What you need to put in place: Use generic sign-in failures rather than detailed error hints.
What good looks like: Attackers do not learn whether a username or password was correct.

IA.7 - Use secure authentication protocols
What this control is doing: Stops credentials being exposed in transit.
What you need to put in place: Use encrypted protocols and disable insecure authentication methods.
What good looks like: Authentication happens over modern protected channels only.

IA.8 - Protect against replay
What this control is doing: Stops captured authentication material being reused.
What you need to put in place: Use modern session handling, nonce/token controls, and secure auth flows.
What good looks like: An intercepted login exchange cannot simply be replayed to gain access.

IA.9 - Require MFA for privileged accounts
What this control is doing: Raises protection on the most dangerous accounts.
What you need to put in place: Enforce MFA on all admin and elevated accounts without exception.
What good looks like: Administrator sign-in always needs more than one factor.

IA.10 - Require MFA for network access
What this control is doing: Improves protection when users access systems over networks.
What you need to put in place: Apply MFA to key business systems and network-access points.
What good looks like: Sensitive system access is not protected by password alone.

IA.11 - Require MFA for remote access
What this control is doing: Hardens access from outside trusted locations.
What you need to put in place: Enforce MFA on VPN, remote desktop gateways, and remote admin tools.
What good looks like: Remote access is strongly protected across all approved methods.

Incident Response (IR)

IR.1 - Establish incident response capability
What this control is doing: Ensures the organisation can respond in a structured way when something goes wrong.
What you need to put in place: Create an incident response plan with roles, escalation paths, severity levels, and communications steps.
What good looks like: The organisation knows how to respond instead of improvising during a crisis.

IR.2 - Report incidents
What this control is doing: Gets security issues raised quickly and consistently.
What you need to put in place: Define how staff report incidents and where reports are received and tracked.
What good looks like: People know exactly how to raise a security issue and incidents are captured formally.

IR.3 - Test incident response
What this control is doing: Checks the plan actually works before a real event.
What you need to put in place: Run tabletop exercises or simulations and record lessons learned.
What good looks like: The plan has been practised and improved, not just written.

Maintenance (MA)

MA.1 - Control system maintenance
What this control is doing: Keeps maintenance activity safe and accountable.
What you need to put in place: Document scheduled and reactive maintenance and approve significant work.
What good looks like: Maintenance happens in a controlled way and can be traced afterwards.

MA.2 - Control maintenance tools
What this control is doing: Stops engineers using unknown or risky tools.
What you need to put in place: Maintain an approved list of tools and restrict unauthorised software.
What good looks like: Only trusted tools are used to service systems.

MA.3 - Control maintenance access
What this control is doing: Limits who can access systems while maintenance is being performed.
What you need to put in place: Use temporary access, supervision, and time-bounded permissions for maintenance tasks.
What good looks like: Maintenance access is tightly controlled and removed when the task ends.

MA.4 - Secure remote maintenance
What this control is doing: Protects maintenance performed from outside the site.
What you need to put in place: Use secure remote channels, MFA, and session logging for remote maintenance.
What good looks like: Remote maintenance is protected and not an unmonitored back door.

MA.5 - Authorise maintenance personnel
What this control is doing: Ensures only approved people carry out maintenance.
What you need to put in place: Verify identity and approval of internal and external maintenance staff.
What good looks like: You know exactly who carried out maintenance and why.

MA.6 - Retain maintenance records
What this control is doing: Keeps evidence of what work was done to systems.
What you need to put in place: Store maintenance logs, tickets, and related approvals.
What good looks like: You can reconstruct system maintenance history when needed.

Media Protection (MP)

MP.1 - Restrict access to media
What this control is doing: Stops unauthorised people handling removable media or stored copies of data.
What you need to put in place: Limit who can use, view, or store media containing sensitive information.
What good looks like: Only approved people can access sensitive media.

MP.2 - Label sensitive media
What this control is doing: Makes it obvious which media needs stronger handling.
What you need to put in place: Use clear labels or equivalent identification for sensitive physical or removable media.
What good looks like: Staff can distinguish sensitive media from ordinary business material.

MP.3 - Store media securely
What this control is doing: Protects media when not in use.
What you need to put in place: Keep media in locked storage or similarly controlled locations.
What good looks like: Sensitive media is not left unsecured in offices, drawers, or vehicles.

MP.4 - Protect media in transit
What this control is doing: Stops loss or exposure while media is being moved.
What you need to put in place: Use secure couriers, tamper controls, encryption, and documented transfer steps.
What good looks like: Media remains protected from pickup to destination.

MP.5 - Sanitise or destroy media before disposal
What this control is doing: Prevents old data being recovered from discarded media.
What you need to put in place: Use wiping, degaussing, or certified destruction based on the media type.
What good looks like: Disposed media cannot be used to recover business data.

MP.6 - Control media use
What this control is doing: Reduces casual or uncontrolled use of removable storage.
What you need to put in place: Set rules for when removable media may be used and by whom.
What good looks like: Media use is an exception that is controlled, not a free-for-all.

MP.7 - Track media
What this control is doing: Maintains accountability for physical items containing data.
What you need to put in place: Keep issue, return, and location records for media where appropriate.
What good looks like: Sensitive media is not lost because nobody knew where it was.

MP.8 - Restrict portable media
What this control is doing: Reduces risks from USB sticks and similar devices.
What you need to put in place: Block or tightly control the use of portable media on endpoints.
What good looks like: Portable media use is limited and monitored.

MP.9 - Protect backup media
What this control is doing: Ensures backups are not the weakest link.
What you need to put in place: Encrypt, store, and transport backup media securely and test recovery.
What good looks like: Backups are both protected and usable when needed.

Physical Protection (PE)

PE.1 - Control facility access
What this control is doing: Stops unauthorised people entering business premises.
What you need to put in place: Use locks, badges, reception controls, and restricted entry points.
What good looks like: People cannot wander into sensitive areas unchallenged.

PE.2 - Control visitors
What this control is doing: Ensures non-staff are identified and managed.
What you need to put in place: Use sign-in, badges, escort rules, and sign-out procedures for visitors.
What good looks like: Visitors are visible, logged, and only where they are meant to be.

PE.3 - Monitor physical access
What this control is doing: Creates oversight of who enters sensitive areas.
What you need to put in place: Use CCTV, guards, or other monitoring where appropriate.
What good looks like: You can review who accessed sensitive areas and when.

PE.4 - Keep physical access records
What this control is doing: Provides traceability for entry to controlled areas.
What you need to put in place: Maintain door logs, visitor books, or access control system records.
What good looks like: Physical access history can be reviewed after an incident.

PE.5 - Control physical access devices
What this control is doing: Prevents badges, keys, and tokens becoming weak points.
What you need to put in place: Issue, track, disable, and replace keys/cards/fobs under controlled processes.
What good looks like: Lost or returned access devices are handled promptly and recorded.

PE.6 - Protect equipment physically
What this control is doing: Reduces theft, tampering, and environmental damage.
What you need to put in place: Use secure rooms, cabinet locks, and suitable environmental protection for critical equipment.
What good looks like: Important systems are protected from casual access and physical harm.

Planning (PL)

PL.1 - Maintain a security plan
What this control is doing: Defines how the organisation protects its systems and sensitive data.
What you need to put in place: Create and maintain a system security plan that reflects the real environment.
What good looks like: The organisation has a clear documented approach rather than informal assumptions.

PL.2 - Define rules of behaviour
What this control is doing: Sets expectations for how users should use systems.
What you need to put in place: Publish acceptable use and security behaviour rules and make users acknowledge them.
What good looks like: People understand the boundaries for using company systems and data.

Personnel Security (PS)

PS.1 - Screen personnel
What this control is doing: Reduces risk from bringing people into sensitive roles without checks.
What you need to put in place: Perform pre-employment screening appropriate to the role and risk.
What good looks like: People with sensitive access have been vetted to an appropriate level.

PS.2 - Manage termination and transfer
What this control is doing: Closes security gaps when employment changes.
What you need to put in place: Use joiner-mover-leaver controls for assets, access, and responsibilities.
What good looks like: People do not keep access or equipment they no longer need.

Risk Assessment (RA)

RA.1 - Assess risk
What this control is doing: Helps the organisation understand what could go wrong and what matters most.
What you need to put in place: Use a repeatable risk assessment process with likelihood, impact, and treatment decisions.
What good looks like: Security decisions are based on known risks rather than guesswork.

RA.2 - Scan for vulnerabilities
What this control is doing: Finds technical weaknesses before attackers do.
What you need to put in place: Run regular vulnerability scans on relevant systems and services.
What good looks like: Technical weaknesses are identified on a planned basis.

RA.3 - Remediate vulnerabilities
What this control is doing: Turns scan results into action.
What you need to put in place: Prioritise and fix vulnerabilities within defined timeframes and track closure.
What good looks like: Known weaknesses are not left open indefinitely without a decision.

System and Services Acquisition (SA)

SA.1 - Define security requirements for new systems
What this control is doing: Ensures security is considered when buying or building technology.
What you need to put in place: Include security requirements and acceptance criteria in procurement and project work.
What good looks like: New systems are expected to be secure from the outset, not patched in later.

SA.2 - Control external system services
What this control is doing: Makes sure outsourced or hosted services meet your security needs.
What you need to put in place: Review suppliers, contracts, and shared responsibility for security controls.
What good looks like: Third-party services are understood and governed, not blindly trusted.

SA.3 - Use secure development practices
What this control is doing: Reduces flaws introduced during software development.
What you need to put in place: Apply secure coding, code review, and testing in development work.
What good looks like: Software is built with security in mind rather than added afterwards.

SA.4 - Maintain supporting system documentation
What this control is doing: Keeps essential design and operating information available.
What you need to put in place: Retain architecture, configuration, and support documentation for systems.
What good looks like: Teams can understand and support systems without relying on tribal knowledge.

SA.5 - Test systems before release
What this control is doing: Stops untested systems going live.
What you need to put in place: Use functional, security, and change testing before deployment or major updates.
What good looks like: Systems are checked before release and not pushed live on hope.

System and Communications Protection (SC)

SC.1 - Protect network boundaries
What this control is doing: Controls traffic entering and leaving trusted environments.
What you need to put in place: Use firewalls, gateways, and boundary rules to restrict communications.
What good looks like: Perimeter traffic is filtered rather than allowed by default.

SC.2 - Protect data in transit
What this control is doing: Stops sensitive data being exposed while moving across networks.
What you need to put in place: Use encryption such as TLS, VPN, or secure tunnels where needed.
What good looks like: Sensitive data is protected while travelling between users and systems.

SC.3 - Segment networks
What this control is doing: Limits spread of attacks and unnecessary connectivity.
What you need to put in place: Separate user, server, admin, production, and guest networks where appropriate.
What good looks like: A compromise in one area does not automatically expose everything else.

SC.4 - Deny traffic by default
What this control is doing: Prevents broad implicit trust on networks.
What you need to put in place: Use rulesets that block traffic unless there is an approved need.
What good looks like: Allowed traffic is deliberate and documented, not accidental.

SC.5 - Control public access
What this control is doing: Protects public-facing services from exposing internal resources.
What you need to put in place: Separate public services and restrict what they can reach internally.
What good looks like: Public systems cannot be used as an easy route into core systems.

SC.6 - Use cryptographic protection appropriately
What this control is doing: Ensures encryption is applied where it matters.
What you need to put in place: Define when to encrypt data and use approved methods and key handling.
What good looks like: Encryption is used deliberately and managed properly.

SC.7 - Control split tunnelling
What this control is doing: Stops remote users bypassing corporate protections while connected.
What you need to put in place: Disable or tightly manage split tunnelling on remote access solutions.
What good looks like: Remote sessions do not silently expose both networks at once.

SC.8 - Monitor network traffic
What this control is doing: Creates visibility into communications and threats on the network.
What you need to put in place: Use network monitoring, IDS/IPS, or equivalent tooling.
What good looks like: Network events and unusual traffic are visible rather than invisible.

SC.9 - Enforce data flow rules
What this control is doing: Controls how information moves between systems and zones.
What you need to put in place: Define and implement approved data paths and restrictions.
What good looks like: Sensitive information follows controlled routes only.

SC.10 - Terminate network connections appropriately
What this control is doing: Stops stale or unauthorised connections lingering.
What you need to put in place: Use timeouts and disconnection rules for sessions and links.
What good looks like: Inactive or abnormal connections do not remain open indefinitely.

SC.11 - Protect session authenticity
What this control is doing: Reduces session hijacking and misuse.
What you need to put in place: Use secure session tokens, re-authentication, and protected cookies where relevant.
What good looks like: Sessions cannot be easily stolen or reused by others.

SC.12 - Use host-based communication controls
What this control is doing: Adds security controls on endpoints and servers themselves.
What you need to put in place: Use host firewalls and local communication restrictions.
What good looks like: Even if network controls fail, systems still enforce basic communication rules.

SC.13 - Control mobile code
What this control is doing: Reduces risk from scripts, macros, and active content.
What you need to put in place: Restrict or manage browser scripts, macros, and other mobile code as appropriate.
What good looks like: Active content is not allowed to run unchecked.

SC.14 - Separate voice and data services where needed
What this control is doing: Reduces exposure between different service types.
What you need to put in place: Segregate voice platforms and data networks where risk justifies it.
What good looks like: One service does not create unnecessary exposure for the other.

SC.15 - Control collaborative and shared tools
What this control is doing: Manages risks in shared workspaces, meetings, and collaboration platforms.
What you need to put in place: Configure sharing, guest access, recording, and retention controls appropriately.
What good looks like: Collaboration tools are useful without being wide open.

SC.16 - Restrict network access
What this control is doing: Limits who and what can connect to networks and services.
What you need to put in place: Use access controls based on user, device, role, and need.
What good looks like: Network access is granted deliberately and not assumed.

System and Information Integrity (SI)

SI.1 - Remediate system flaws
What this control is doing: Keeps systems up to date against known weaknesses.
What you need to put in place: Use patching and remediation processes for operating systems, apps, and firmware.
What good looks like: Known flaws are corrected within sensible timescales.

SI.2 - Protect against malicious code
What this control is doing: Stops malware gaining a foothold or spreading easily.
What you need to put in place: Use endpoint protection, anti-malware, and related controls on relevant systems.
What good looks like: Malware is blocked, detected, or contained quickly.

SI.3 - Receive and act on security alerts
What this control is doing: Ensures threat information leads to action.
What you need to put in place: Monitor vendor alerts, advisories, and intelligence relevant to your environment.
What good looks like: Important warnings are noticed and acted on promptly.

SI.4 - Use trusted update mechanisms
What this control is doing: Stops updates becoming a security weakness.
What you need to put in place: Use approved update channels and verify updates before deployment where appropriate.
What good looks like: Systems are updated through controlled and trusted mechanisms.

SI.5 - Validate inputs
What this control is doing: Reduces application abuse from bad or malicious data.
What you need to put in place: Use input validation and secure development controls on applications and interfaces.
What good looks like: Systems reject malformed or dangerous input safely.

SI.6 - Handle errors safely
What this control is doing: Prevents systems exposing sensitive details through failures.
What you need to put in place: Configure applications and services to avoid leaking technical detail in errors.
What good looks like: Error messages do not give attackers useful information.

SI.7 - Verify integrity
What this control is doing: Checks whether systems or files have been altered unexpectedly.
What you need to put in place: Use integrity checking, file monitoring, or similar controls where appropriate.
What good looks like: Unauthorised changes can be detected instead of going unnoticed.