OLSON TECH SERVICES

Business Security Checkup

A practical, fillable self-assessment for Microsoft 365, Google Workspace, SaaS, AI, devices, data, network, backup, monitoring, and incident readiness.

BUILT TO BE USED - NOT JUST READ

Check controls, record findings, assign owners, add notes, save your progress, and reuse the workbook as your organization improves.

Vendor-agnostic security advisory resource | Interactive PDF edition

Start here

This is not another checklist that says 'use MFA' or 'keep systems updated.' It is designed to help a business verify whether important controls actually exist, understand why they matter, and identify where deeper technical work may be needed.

HOW TO READ EACH CONTROL

BUSINESS	A business owner or manager should be able to help answer this.
TECHNICAL	An administrator or IT provider will likely need to verify configuration.
SPECIALIST	Interpretation, architecture, or remediation can require deeper expertise.

STATUS OPTIONS

- [ ] Meets Baseline
- [ ] Needs Attention
- [ ] Unable to Verify
- [ ] Not Applicable

IMPORTANT

"Unable to Verify" is a useful finding. If nobody can prove an important control exists or is operating, that uncertainty deserves attention.

Contents

Click any domain or control to jump directly to that part of the workbook.

Organization profile

Complete this first so the workbook reflects the environment you are actually assessing.

ORGANIZATION

ASSESSMENT OWNER

ASSESSMENT STARTED

EMPLOYEES / USERS

COMPANY-OWNED ENDPOINTS

ENDPOINT MANAGEMENT PLATFORM

ENDPOINT SECURITY / EDR

BACKUP SOLUTION

FIREWALL / NETWORK PLATFORM

KNOWN COMPLIANCE / CONTRACTUAL REQUIREMENTS

PRIMARY PRODUCTIVITY PLATFORM

- [ ] Microsoft 365
- [ ] Google Workspace
- [ ] Both / Hybrid
- [ ] Other

AI USED FOR BUSINESS

- [ ] Microsoft Copilot
- [ ] Google Gemini
- [ ] ChatGPT
- [ ] Claude
- [ ] Other / Unknown

10 questions every business should answer

- ☐ 01 Is MFA actually required for every active user?
- ☐ 02 Do you know exactly who has administrator access?
- ☐ 03 What happens to access the day an employee leaves?
- ☐ 04 Can employees create public or anonymous file-sharing links?
- ☐ 05 Do you know which third-party apps can access company data?
- ☐ 06 Do you know which devices currently access company resources?
- ☐ 07 When was the last successful backup restore test?
- ☐ 08 Who receives and reviews security alerts?
- ☐ 09 What happens if an executive's email is compromised today?
- ☐ 10 Who is ultimately responsible for cybersecurity decisions?

How many can you confidently answer? _____ out of 10

Security checkup dashboard

Use this after completing the detailed sections. Avoid reducing security to a single misleading score.

AREA	MEETS	ATTENTION	UNKNOWN
Identity & Access	○	○	○
Email Security	○	○	○
Devices & Endpoint Security	○	○	○
Files, Sharing & Sensitive Data	○	○	○
SaaS & Third-Party Applications	○	○	○
AI Security & Governance	○	○	○
Network & Remote Access	○	○	○
Backup & Recovery	○	○	○
Monitoring & Detection	○	○	○
Incident Readiness	○	○	○
Governance & Employee Practices	○	○	○

Executive notes

CONTENTS

01

Identity & Access

Who can access your environment, how they authenticate, and whether access is still appropriate.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 01

MFA is enforced for every active user

CRITICAL TECHNICAL

WHY THIS MATTERS

Password compromise remains one of the most common paths into business systems. MFA should be required, not merely available.

WHAT TO CHECK

- [ ] Confirm MFA/2-Step Verification is required for every active interactive user.
- [ ] Identify users or groups excluded from MFA and document why.
- [ ] Confirm administrator accounts are also protected by MFA.
- [ ] Review whether older or alternate authentication paths can bypass the intended control.

WHERE TO LOOK

Microsoft 365: Microsoft Entra admin center - Authentication methods, Conditional Access, sign-in logs.
Google Workspace: Admin console - Security - Authentication / 2-Step Verification and login/security reporting.

WHAT GOOD LOOKS LIKE

Every normal user is protected by MFA, exceptions are rare and documented, and privileged users receive stronger protection where appropriate.

WATCH FOR

Ask for evidence of enforcement - not just a screenshot showing users enrolled.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 02

Privileged administrator access is limited

CRITICAL TECHNICAL

WHY THIS MATTERS

Administrator roles can change security controls, access information, create users, and alter the environment.

WHAT TO CHECK

- [ ] Identify every Global Administrator, Super Administrator, and equivalent privileged role.
- [ ] Confirm each assignment still has a current business need.
- [ ] Look for inactive, former, vendor, or shared accounts with privileged access.
- [ ] Determine whether routine daily accounts are being used for high-impact administration.

WHERE TO LOOK

Microsoft 365: Entra admin center - Roles and administrators.
Google Workspace: Admin console - Account - Admin roles.

WHAT GOOD LOOKS LIKE

Privileged access is limited, intentional, reviewed, and separate from routine activity when practical.

WATCH FOR

Do not accept 'only IT has admin.' Ask to see the actual list.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 03

Emergency access is planned

HIGH SPECIALIST

WHY THIS MATTERS

If normal authentication or identity controls fail, the organization still needs a safe, controlled recovery path.

WHAT TO CHECK

- [ ] Confirm whether emergency/break-glass administrator access exists.
- [ ] Confirm emergency access is protected differently from normal accounts.
- [ ] Verify credentials and procedures are stored securely.
- [ ] Confirm emergency access is monitored and periodically tested.

WHERE TO LOOK

Platform-specific emergency access approaches vary. Review identity administration and documented recovery procedures.

WHAT GOOD LOOKS LIKE

Emergency access is documented, secured, monitored, and tested without becoming a permanent bypass.

WATCH FOR

Emergency access that is never tested may fail when it is actually needed.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 04

Former employee access is removed promptly

CRITICAL BUSINESS

WHY THIS MATTERS

Offboarding gaps can leave email, files, SaaS applications, VPN access, and privileged access available after employment ends.

WHAT TO CHECK

- [ ] Confirm there is a repeatable offboarding process.
- [ ] Review a recent departure and verify account access was removed promptly.
- [ ] Confirm groups, SaaS access, VPN, shared resources, and administrator roles are included.
- [ ] Confirm ownership of files/mail/data is transferred where necessary.

WHERE TO LOOK

Microsoft 365: Microsoft 365 admin center / Entra users and groups.
Google Workspace: Admin console - Directory - Users / Groups / Apps.

WHAT GOOD LOOKS LIKE

A defined process removes access consistently and transfers required business information without leaving orphaned access.

WATCH FOR

A disabled mailbox alone does not prove access to every connected SaaS or remote system was removed.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 05

Dormant and unused accounts are reviewed

HIGH TECHNICAL

WHY THIS MATTERS

Old accounts create attack surface and are often overlooked because nobody actively uses them.

WHAT TO CHECK

- [ ] Identify accounts with no recent legitimate sign-in activity.
- [ ] Review dormant guest, shared, service, and administrator accounts.
- [ ] Confirm every non-human account has an owner and purpose.
- [ ] Disable or remove accounts that no longer have a business need.

WHERE TO LOOK

Microsoft 365: Entra users, sign-in activity and reports.
Google Workspace: Directory and login/audit reporting.

WHAT GOOD LOOKS LIKE

Unused access is removed, and exceptions have a named owner and documented purpose.

WATCH FOR

Dormant accounts often survive reorganizations, vendor changes, and old projects.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 06

Guest and external access is reviewed

HIGH TECHNICAL

WHY THIS MATTERS

External collaborators can retain access long after a project or business relationship ends.

WHAT TO CHECK

- [ ] Inventory guest/external identities.
- [ ] Identify guests with access to sensitive sites, drives, teams, or groups.
- [ ] Review inactive external users.
- [ ] Confirm someone inside the business owns each continuing external relationship.

WHERE TO LOOK

Microsoft 365: Entra External Identities; SharePoint/Teams sharing.
Google Workspace: Directory, Groups, Drive sharing and trusted-domain settings.

WHAT GOOD LOOKS LIKE

External access is intentional, time-bounded where possible, and periodically reviewed.

WATCH FOR

External sharing can be appropriate. The risk is unmanaged, ownerless, or forgotten access.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 07

Third-party app consent is controlled

HIGH SPECIALIST

WHY THIS MATTERS

Connected applications can retain broad access to mail, files, contacts, and directory data even when users rarely think about them.

WHAT TO CHECK

- [ ] Review applications connected through OAuth or delegated access.
- [ ] Identify applications with broad permissions or access to sensitive data.
- [ ] Remove abandoned or unnecessary integrations.
- [ ] Determine who can approve new high-risk application permissions.

WHERE TO LOOK

Microsoft 365: Entra enterprise applications / consent settings.
Google Workspace: Admin console - Security - Access and data control / API controls.

WHAT GOOD LOOKS LIKE

Application access is known, approved, minimally privileged, and removable.

WATCH FOR

An app can be 'trusted' by a user without being appropriate for the organization.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTENTS

02

Email Security

Reduce spoofing, account abuse, malicious content, and unauthorized routing of business email.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 08

SPF is present and accurately scoped

HIGH TECHNICAL

WHY THIS MATTERS

SPF helps receiving mail systems determine which services are authorized to send mail for your domain.

WHAT TO CHECK

- [ ] Confirm every production sending domain has an SPF record.
- [ ] Identify all legitimate third-party senders such as CRM, invoicing, ticketing, HR, and marketing tools.
- [ ] Confirm old or unused sending services have been removed.
- [ ] Confirm the record is not broken by excessive DNS lookups.

WHERE TO LOOK

Review public DNS and your mail platform's domain configuration.

WHAT GOOD LOOKS LIKE

SPF authorizes only legitimate senders and remains technically valid.

WATCH FOR

A record that exists can still be incomplete or invalid.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 09

DKIM signing is enabled

HIGH TECHNICAL

WHY THIS MATTERS

DKIM allows recipients to validate that a message was authorized by the sending domain and was not altered in transit.

WHAT TO CHECK

- [ ] Confirm DKIM is enabled for your primary mail platform.
- [ ] Confirm third-party senders support DKIM where practical.
- [ ] Verify selectors/keys are current and published correctly.
- [ ] Check whether messages from important systems actually contain valid DKIM signatures.

WHERE TO LOOK

Microsoft 365: Exchange/Microsoft 365 domain authentication settings.
Google Workspace: Admin console - Gmail - Authenticate email.

WHAT GOOD LOOKS LIKE

Legitimate senders sign mail with aligned, valid DKIM where supported.

WATCH FOR

Enabling DKIM in one platform does not automatically cover every third-party sender.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 10

DMARC is published and reviewed

HIGH TECHNICAL

WHY THIS MATTERS

DMARC helps protect your domain from spoofing and provides reporting about who is sending as your domain.

WHAT TO CHECK

- [ ] Confirm DMARC exists for every important sending domain.
- [ ] Determine whether the policy is monitoring, quarantine, or reject.
- [ ] Confirm aggregate reports are being collected and reviewed.
- [ ] Identify unauthorized or unexpected senders before increasing enforcement.

WHERE TO LOOK

Review the public _dmarc DNS record and your reporting process/provider.

WHAT GOOD LOOKS LIKE

DMARC reporting is active, legitimate senders are understood, and enforcement is increased deliberately when appropriate.

WATCH FOR

Do not blindly move to p=reject before identifying legitimate senders.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 11

Automatic external forwarding is controlled

CRITICAL TECHNICAL

WHY THIS MATTERS

Attackers often create forwarding rules after account compromise to silently copy business email outside the organization.

WHAT TO CHECK

- [ ] Determine whether users can automatically forward mail externally.
- [ ] Review current forwarding configurations.
- [ ] Review mail-flow/routing rules for external redirects.
- [ ] Document any legitimate exceptions.

WHERE TO LOOK

Microsoft 365: Exchange mail flow, mailbox forwarding, Defender outbound spam policy.
Google Workspace: Gmail forwarding, routing and compliance settings.

WHAT GOOD LOOKS LIKE

External forwarding is restricted by default and exceptions are known and reviewed.

WATCH FOR

Disabling forwarding without understanding business workflows can break legitimate integrations.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 12

Anti-phishing and impersonation protections are reviewed

CRITICAL TECHNICAL

WHY THIS MATTERS

Modern phishing often impersonates executives, vendors, domains, and trusted relationships rather than relying only on obvious spam.

WHAT TO CHECK

- [ ] Review anti-phishing protections.
- [ ] Determine whether executive/domain impersonation protections are available and enabled.
- [ ] Review treatment of suspicious links and attachments.
- [ ] Confirm quarantine and alerting are actually monitored.

WHERE TO LOOK

Microsoft 365: Microsoft Defender - Email & collaboration - Policies & rules.
Google Workspace: Gmail Safety / spam, phishing and malware settings.

WHAT GOOD LOOKS LIKE

High-risk impersonation, malicious links, and attachments are detected and handled without broad bypasses.

WATCH FOR

Security tools that generate alerts nobody reviews provide much less protection than expected.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 13

Mail routing, connectors, and relay are known

HIGH SPECIALIST

WHY THIS MATTERS

Legacy connectors and relay settings can unintentionally create bypasses or alternate sending paths.

WHAT TO CHECK

- [ ] Inventory inbound/outbound connectors or routing rules.
- [ ] Identify SMTP relay use and the systems that depend on it.
- [ ] Review broad allowlists or bypass rules.
- [ ] Remove unused connectors and document required exceptions.

WHERE TO LOOK

Microsoft 365: Exchange admin center - Mail flow / Connectors.
Google Workspace: Gmail routing, hosts, relay and compliance settings.

WHAT GOOD LOOKS LIKE

Every alternate mail path has an owner, purpose, and security rationale.

WATCH FOR

Old migration or appliance rules frequently survive long after the original project.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTENTS

03

Devices & Endpoint Security

Know which devices access business resources and whether they are patched, encrypted, managed, and monitored.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 14

Business devices are inventoried

HIGH BUSINESS

WHY THIS MATTERS

You cannot consistently secure devices you do not know exist.

WHAT TO CHECK

- [ ] Maintain a list of company-owned laptops, desktops, and mobile devices.
- [ ] Identify the assigned user and device owner.
- [ ] Identify unmanaged devices accessing company resources.
- [ ] Identify unsupported or end-of-life operating systems.

WHERE TO LOOK

Microsoft 365: Intune / Defender device inventories if used.
Google Workspace: Admin console - Devices / Endpoint management.

WHAT GOOD LOOKS LIKE

Every business device has an owner, lifecycle state, and security management path.

WATCH FOR

Inventory is not the same as purchasing records. It should reflect devices actually in use.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 15

Full-disk encryption is verified

HIGH TECHNICAL

WHY THIS MATTERS

Encryption reduces data exposure when a laptop or storage device is lost or stolen.

WHAT TO CHECK

- [ ] Confirm supported company laptops use full-disk encryption.
- [ ] Confirm recovery keys are securely escrowed where applicable.
- [ ] Identify devices that report encryption failures or unknown status.
- [ ] Define how lost/stolen devices are handled.

WHERE TO LOOK

Microsoft environments commonly use BitLocker reporting through device management. Other platforms should use their supported native encryption controls.

WHAT GOOD LOOKS LIKE

Portable business devices are encrypted and recovery information is controlled.

WATCH FOR

Do not rely only on a policy being assigned; verify actual device status.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 16

Endpoint protection/EDR is healthy

CRITICAL TECHNICAL

WHY THIS MATTERS

Security software provides little value if agents are missing, disabled, unhealthy, or not reporting.

WHAT TO CHECK

- [ ] Confirm endpoint protection/EDR is deployed to supported devices.
- [ ] Identify devices that have stopped reporting.
- [ ] Review current high-severity detections.
- [ ] Confirm someone owns alert triage and response.

WHERE TO LOOK

Microsoft 365: Microsoft Defender portal / Intune where deployed.

Google Workspace environments: review the organization's endpoint security platform plus Google endpoint controls.

WHAT GOOD LOOKS LIKE

Supported devices actively report healthy protection status and alerts have an owner.

WATCH FOR

'Installed' is not the same as healthy, current, and monitored.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 17

Security patching is measured

HIGH TECHNICAL

WHY THIS MATTERS

Known vulnerabilities are frequently exploited after fixes are publicly available.

WHAT TO CHECK

- [ ] Define how quickly critical operating-system patches should be deployed.
- [ ] Review current patch compliance rather than relying on automatic updates alone.
- [ ] Identify devices repeatedly missing updates.
- [ ] Include common third-party applications in the patching strategy.

WHERE TO LOOK

Use your endpoint management / patch platform and vulnerability data where available.

WHAT GOOD LOOKS LIKE

Critical updates are deployed within a defined timeframe and exceptions are visible.

WATCH FOR

A few perpetually offline or unmanaged devices can materially increase risk.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 18

Local administrator access is controlled

HIGH TECHNICAL

WHY THIS MATTERS

Permanent local admin rights make malware and credential theft more damaging.

WHAT TO CHECK

- [ ] Identify who has local administrator rights on company endpoints.
- [ ] Remove unnecessary permanent access.
- [ ] Document approved exceptions.
- [ ] Use separate elevation or managed approaches where appropriate.

WHERE TO LOOK

Review endpoint management policy, local group membership, or privileged endpoint tooling.

WHAT GOOD LOOKS LIKE

Administrative rights are limited to users and workflows that require them.

WATCH FOR

Many organizations discover that local admin was granted years ago and never revisited.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 19

Device screen lock and firewall controls are enforced

MEDIUM TECHNICAL

WHY THIS MATTERS

Basic local controls reduce exposure from unattended devices and untrusted networks.

WHAT TO CHECK

- [ ] Confirm automatic screen lock is configured.
- [ ] Confirm host firewall is enabled.
- [ ] Review sleep/lock behavior on portable devices.
- [ ] Identify users or devices exempt from baseline controls.

WHERE TO LOOK

Review endpoint configuration/compliance policy.

WHAT GOOD LOOKS LIKE

Portable endpoints lock automatically and maintain local firewall protection.

WATCH FOR

A written policy is not evidence that endpoints actually received the setting.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 20

Lost or stolen device response is defined

HIGH BUSINESS

WHY THIS MATTERS

Speed matters when a device containing company data is lost or stolen.

WHAT TO CHECK

- [ ] Employees know exactly who to contact.
- [ ] IT can identify the device and associated account quickly.
- [ ] Remote lock/wipe capabilities are understood where available.
- [ ] The organization knows when incident or legal escalation is required.

WHERE TO LOOK

Review device management capabilities and incident procedures.

WHAT GOOD LOOKS LIKE

Lost-device reporting and containment are simple enough to execute immediately.

WATCH FOR

If employees hesitate because they fear blame, reporting delays can worsen the impact.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTENTS

04

Files, Sharing & Sensitive Data

Control who can access business information, how it is shared, and how sensitive data is handled.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 21

External file sharing is intentionally configured

HIGH TECHNICAL

WHY THIS MATTERS

Cloud collaboration makes external sharing easy; default settings can be broader than leadership expects.

WHAT TO CHECK

- [ ] Review organization-wide external sharing settings.
- [ ] Determine whether anonymous/public links are allowed.
- [ ] Identify sensitive sites, teams, or shared drives with stronger requirements.
- [ ] Review stale external shares and guests.

WHERE TO LOOK

Microsoft 365: SharePoint admin center / OneDrive / Teams sharing.
Google Workspace: Admin console - Apps - Google Workspace - Drive and Docs - Sharing settings.

WHAT GOOD LOOKS LIKE

External sharing supports business collaboration without allowing uncontrolled public access.

WATCH FOR

Public/anonymous links deserve special attention because they can be forwarded beyond the intended recipient.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 22

Sensitive information categories are understood

HIGH BUSINESS

WHY THIS MATTERS

Technical controls cannot protect sensitive data effectively if the business has never identified what matters most.

WHAT TO CHECK

- [ ] Identify major categories such as financial, customer, employee, health, legal, or regulated data.
- [ ] Determine where those categories are commonly stored.
- [ ] Identify teams that handle the most sensitive information.
- [ ] Document any regulatory or contractual handling requirements.

WHERE TO LOOK

Business-led activity; technical platforms can assist with classification and discovery.

WHAT GOOD LOOKS LIKE

The organization knows what information requires stronger protection and where it generally lives.

WATCH FOR

Do not start with tool configuration before the business agrees on what data matters.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 23

Data Loss Prevention is used where risk justifies it

HIGH SPECIALIST

WHY THIS MATTERS

DLP can help detect or restrict inappropriate sharing of sensitive information, but poorly designed rules can disrupt legitimate work.

WHAT TO CHECK

- [ ] Determine whether DLP capabilities are licensed and used.
- [ ] Review what sensitive data types or labels are in scope.
- [ ] Review recent matches and exceptions.
- [ ] Confirm policy behavior was tested before broad enforcement.

WHERE TO LOOK

Microsoft 365: Microsoft Purview DLP.
Google Workspace: DLP / classification capabilities where supported by edition.

WHAT GOOD LOOKS LIKE

DLP focuses on meaningful risks, is tested, and has a process for exceptions and false positives.

WATCH FOR

Broad 'block everything sensitive' rules often fail operationally without design and testing.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 24

Shared repositories have clear owners

MEDIUM BUSINESS

WHY THIS MATTERS

Ownerless sites and shared drives tend to accumulate stale permissions and data indefinitely.

WHAT TO CHECK

- [ ] Identify owners for major SharePoint sites, Teams, shared drives, and departmental repositories.
- [ ] Review repositories whose owners left the business.
- [ ] Define who approves new external access.
- [ ] Archive or retire abandoned repositories.

WHERE TO LOOK

Microsoft 365: SharePoint/Teams ownership and permissions.
Google Workspace: Shared Drive managers and membership.

WHAT GOOD LOOKS LIKE

Every important shared repository has an accountable owner.

WATCH FOR

Ownership is a governance control, not just a technical setting.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 25

Retention and deletion are intentional

MEDIUM SPECIALIST

WHY THIS MATTERS

Keeping everything forever can increase legal, privacy, and breach exposure; deleting too aggressively can create operational or regulatory problems.

WHAT TO CHECK

- [ ] Identify important retention obligations.
- [ ] Review whether retention policies exist.
- [ ] Confirm critical repositories are covered appropriately.
- [ ] Document exceptions and legal hold processes where relevant.

WHERE TO LOOK

Microsoft 365: Microsoft Purview retention/records capabilities.
Google Workspace: Google Vault retention where licensed.

WHAT GOOD LOOKS LIKE

Retention reflects business/legal requirements and is periodically reviewed.

WATCH FOR

Retention should be designed with legal/business stakeholders, not set solely by IT convenience.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 26

Highly sensitive sharing has an approval path

HIGH BUSINESS

WHY THIS MATTERS

Some data warrants stronger controls than ordinary collaboration.

WHAT TO CHECK

- [ ] Identify information that should not be shared externally without approval.
- [ ] Determine who can approve exceptions.
- [ ] Confirm employees know the approval process.
- [ ] Review whether technical controls support the intended rule.

WHERE TO LOOK

Use platform sharing, labeling, DLP, and access controls as appropriate.

WHAT GOOD LOOKS LIKE

High-risk sharing decisions are explicit rather than accidental.

WATCH FOR

If the business rule is unclear, technical enforcement will also be unclear.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTENTS

05

SaaS & Third-Party Applications

Understand which cloud services and integrations have access to company information.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 27

A SaaS application inventory exists

HIGH BUSINESS

WHY THIS MATTERS

Modern businesses often have dozens of cloud services outside the primary productivity suite.

WHAT TO CHECK

- [ ] List material SaaS applications used for company work.
- [ ] Identify a business owner for each application.
- [ ] Record what data the application handles.
- [ ] Identify abandoned, duplicate, or unsanctioned services.

WHERE TO LOOK

Use procurement, finance, SSO, browser/security discovery, and administrator records together.

WHAT GOOD LOOKS LIKE

Material SaaS usage is known, owned, and periodically reviewed.

WATCH FOR

Credit-card statements and SSO logs often reveal apps nobody remembered to include.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 28

Critical SaaS uses MFA or SSO

HIGH TECHNICAL

WHY THIS MATTERS

A secure Microsoft 365 or Google Workspace tenant does not protect separate SaaS accounts that still rely on passwords alone.

WHAT TO CHECK

- [ ] Identify high-impact SaaS applications without MFA.
- [ ] Use SSO where it improves centralized lifecycle control.
- [ ] Confirm administrators of SaaS systems receive strong authentication.
- [ ] Review recovery methods and backup administrator accounts.

WHERE TO LOOK

Review each application's identity/security settings and your SSO platform.

WHAT GOOD LOOKS LIKE

Important cloud applications use strong authentication and centralized access where practical.

WATCH FOR

Do not assume 'Sign in with Google/Microsoft' automatically means the application is fully governed.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 29

Vendor access is time-bounded and owned

HIGH BUSINESS

WHY THIS MATTERS

Vendors often retain access beyond the project or support engagement that originally required it.

WHAT TO CHECK

- [ ] List vendors with administrative or data access.
- [ ] Identify an internal owner for each vendor relationship.
- [ ] Review access when contracts or projects end.
- [ ] Require individual identities rather than generic shared vendor accounts where practical.

WHERE TO LOOK

Review application, identity, VPN, remote-support, and platform access records.

WHAT GOOD LOOKS LIKE

Vendor access exists only while needed and is attributable to a person or managed account.

WATCH FOR

Vendor access frequently crosses multiple systems and must be removed in more than one place.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 30

Third-party security expectations are documented

MEDIUM BUSINESS

WHY THIS MATTERS

Your organization can inherit risk from vendors that store important information or operate critical systems.

WHAT TO CHECK

- [ ] Identify vendors that process sensitive data or critical operations.
- [ ] Collect appropriate security documentation or contractual commitments.
- [ ] Understand incident-notification obligations.
- [ ] Review material vendors periodically.

WHERE TO LOOK

Business/vendor management process; technical evidence varies by service.

WHAT GOOD LOOKS LIKE

Higher-risk vendors receive proportionate review rather than identical questionnaires for every supplier.

WATCH FOR

Vendor review should focus on business impact, not paperwork volume.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTENTS

06

AI Security & Governance

Understand which AI tools are being used, what company information they can access, and whether appropriate safeguards and oversight exist.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 31

Approved AI tools and Shadow AI are understood

HIGH BUSINESS

WHY THIS MATTERS

Employees can adopt consumer AI assistants, browser extensions, meeting tools, and embedded AI features without IT or leadership realizing company information is being processed elsewhere.

WHAT TO CHECK

- [ ] Identify the AI tools officially approved for business use.
- [ ] Determine whether employees use personal AI accounts for company work.
- [ ] Identify AI browser extensions, meeting/transcription assistants, writing tools, coding assistants, and embedded SaaS AI features.
- [ ] Define who approves new AI tools and who maintains the approved-use list.

WHERE TO LOOK

Microsoft environment: Review Microsoft 365/Copilot administration, Entra applications, and sanctioned SaaS usage.
Google environment: Review Workspace/Gemini administration, connected apps, and sanctioned SaaS usage.
Other AI platforms: Review enterprise administration, identity, and organization controls.

WHAT GOOD LOOKS LIKE

The organization knows which AI services are used for business purposes and has a practical process for approving, reviewing, and retiring them.

WATCH FOR

Do not accept 'we do not use AI' without checking. Employees may already use AI features embedded in tools the business owns.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 32

Company data entered into AI is governed

CRITICAL BUSINESS

WHY THIS MATTERS

AI prompts and uploads can contain customer information, confidential business data, credentials, source code, regulated information, or intellectual property.

WHAT TO CHECK

- [ ] Define what company information employees may provide to approved AI tools.
- [ ] Define what information must not be submitted, including credentials, secrets, and restricted data.
- [ ] Address customer data, personal information, source code, contracts, financial information, and regulated data as applicable.
- [ ] Make the rule understandable when an employee is unsure how information is classified.

WHERE TO LOOK

Review the organization's acceptable-use, data-classification, privacy, and AI-use guidance together with the controls available in each approved AI service.

WHAT GOOD LOOKS LIKE

Employees can distinguish acceptable AI use from prohibited or higher-risk use, and sensitive information handling reflects the actual service and business risk.

WATCH FOR

A blanket statement such as 'never put sensitive data into AI' may be too vague to operate. Enterprise and consumer AI offerings can have materially different data-handling terms and controls.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 33

Business AI uses organization-managed identities

HIGH TECHNICAL

WHY THIS MATTERS

Personal AI accounts can make access, offboarding, auditability, and administrative control difficult or impossible for the business.

WHAT TO CHECK

- [ ] Determine whether business AI use occurs through organization-managed accounts where available.
- [ ] Identify personal AI accounts being used for company work.
- [ ] Verify SSO and MFA protections where supported.
- [ ] Confirm AI access can be removed during offboarding.
- [ ] Review who holds administrator access to enterprise AI platforms.

WHERE TO LOOK

Microsoft: Review Entra identity and Microsoft 365/Copilot administration.
Google: Review Workspace identity and Gemini administration.
Other enterprise AI: Review SSO, MFA, user lifecycle, and administrative roles.

WHAT GOOD LOOKS LIKE

Business AI access is tied to managed identities where practical and follows normal onboarding, access review, and offboarding processes.

WATCH FOR

Buying an enterprise AI license does not automatically mean identity lifecycle and administrator access are well governed.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 34

AI retention, training, and privacy terms are understood

HIGH SPECIALIST

WHY THIS MATTERS

Organizations can make incorrect assumptions about whether prompts, files, outputs, or conversation history are retained, reviewed, or used to improve a service.

WHAT TO CHECK

- [ ] Determine how each approved AI provider handles prompts, files, and generated content.
- [ ] Determine whether business data may be used for model training or service improvement under the organization's plan and settings.
- [ ] Identify configurable retention, history, deletion, and privacy controls.
- [ ] Understand who can access stored AI interactions and how deletion works.
- [ ] Document meaningful differences between consumer and enterprise offerings.

WHERE TO LOOK

Review the administrative controls, contractual terms, privacy documentation, and data-use settings for each approved AI service.

WHAT GOOD LOOKS LIKE

The organization can explain how approved AI services handle business data and has intentionally selected settings and service tiers that match its risk requirements.

WATCH FOR

Do not accept 'the vendor says our data is secure' as the entire review. Ask how it is retained, used, accessed, deleted, and governed.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 35

AI access to Microsoft 365 or Google Workspace data is reviewed

CRITICAL TECHNICAL

WHY THIS MATTERS

AI can make information that users already have permission to access dramatically easier to discover, exposing long-standing oversharing or permission problems.

WHAT TO CHECK

- [ ] Identify AI services that can access organizational email, files, chats, calendars, contacts, or directory data.
- [ ] Review broadly shared repositories before expanding AI access.
- [ ] Review guest and external access to sensitive collaboration spaces.
- [ ] Identify sensitive repositories and excessive permissions.
- [ ] Review application permissions granted to AI integrations.

WHERE TO LOOK

Microsoft: Review Microsoft 365 Copilot readiness, SharePoint/OneDrive/Teams permissions, Entra applications, and relevant data-governance controls.

Google: Review Gemini/Workspace access, Drive/Shared Drive permissions, connected applications, and relevant data controls.

WHAT GOOD LOOKS LIKE

Underlying permissions and sharing are intentionally governed before AI makes organizational information easier to search, summarize, and combine.

WATCH FOR

AI does not need to bypass permissions to expose a governance problem. It can surface information a user technically had access to but previously could not easily find.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 36

AI plugins, connectors, and OAuth permissions are controlled

HIGH TECHNICAL

WHY THIS MATTERS

AI integrations can receive broad delegated or application access to mail, files, calendars, messages, CRM data, and other business systems.

WHAT TO CHECK

- [ ] Inventory AI applications connected to business systems.
- [ ] Review OAuth/API permissions granted to AI applications.
- [ ] Identify integrations with access to sensitive data or high-impact permissions.
- [ ] Remove unused plugins, connectors, and integrations.
- [ ] Assign an internal owner to material AI integrations and define approval for new ones.

WHERE TO LOOK

Microsoft: Entra enterprise applications, consent, connected applications, and relevant Copilot connectors.
Google: Admin console API controls, connected apps, Workspace Marketplace, and relevant Gemini integrations.
Other systems: Review API keys, OAuth grants, plugins, and service connections.

WHAT GOOD LOOKS LIKE

AI integrations are known, owned, minimally privileged, approved, and removable.

WATCH FOR

An AI tool may look harmless in the user interface while its connector has broad access behind the scenes.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 37

AI agents and automated actions are constrained

CRITICAL SPECIALIST

WHY THIS MATTERS

An AI agent that can take actions creates a different risk than an assistant that only generates text. Excessive permissions can turn an AI error or compromised workflow into a business-impacting action.

WHAT TO CHECK

- [ ] Identify AI agents capable of taking actions in business systems.
- [ ] Document what each agent can read and what actions it can perform.
- [ ] Review credentials, service identities, and permissions used by agents.
- [ ] Require human approval for high-impact actions where appropriate.
- [ ] Define actions that should never occur autonomously.
- [ ] Confirm meaningful agent actions are logged and access can be revoked quickly.

WHERE TO LOOK

Review the agent platform, connected systems, service identities, permissions, approval gates, logs, and kill/disable procedures.

WHAT GOOD LOOKS LIKE

Agents operate with explicit, least-privilege permissions, appropriate human approval, useful logging, and a reliable way to stop or revoke access.

WATCH FOR

Ask whether the AI can only recommend an action or can actually perform it. That distinction materially changes the risk.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 38

AI-generated output receives appropriate human validation

HIGH BUSINESS

WHY THIS MATTERS

AI can produce confident but incorrect content, unsafe code, fabricated citations, or recommendations that are inappropriate for the business context.

WHAT TO CHECK

- [ ] Define when AI-generated information requires human review.
- [ ] Require qualified review before AI output drives consequential legal, financial, HR, security, or customer decisions.
- [ ] Require technical review and testing of AI-generated scripts or code before production use.
- [ ] Verify important factual claims against authoritative sources.
- [ ] Teach employees that confident AI output can still be wrong.

WHERE TO LOOK

Review business procedures, development/change controls, quality assurance, and AI acceptable-use guidance.

WHAT GOOD LOOKS LIKE

AI assists people rather than silently becoming the final authority for consequential business decisions or production changes.

WATCH FOR

The right level of review depends on consequence. A draft meeting summary and a production firewall script should not have the same approval standard.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 39

AI security awareness and acceptable use are established

MEDIUM BUSINESS

WHY THIS MATTERS

Employees need practical rules for approved tools, sensitive data, unexpected behavior, and accidental disclosure - not a policy nobody can translate into daily work.

WHAT TO CHECK

- [ ] Teach employees which AI tools are approved for business use.
- [ ] Explain whether personal AI accounts may be used for company work.
- [ ] Explain what information may and may not be submitted.
- [ ] Provide a process for requesting a new AI tool.
- [ ] Define how to report accidental sensitive-data disclosure or suspicious AI behavior.
- [ ] Include AI output verification in relevant training.

WHERE TO LOOK

Review employee security awareness, acceptable-use guidance, onboarding materials, and reporting channels.

WHAT GOOD LOOKS LIKE

Employees can explain the organization's basic AI rules and know where to ask questions or report a mistake.

WATCH FOR

A policy is not effective if employees cannot quickly answer 'Can I put this information into this AI tool?'

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 40

AI governance has an owner and review process

HIGH BUSINESS

WHY THIS MATTERS

AI adoption can spread across departments faster than security, privacy, legal, procurement, and IT processes can keep up.

WHAT TO CHECK

- [ ] Assign ownership for AI governance and risk decisions.
- [ ] Maintain an inventory of approved material AI services and owners.
- [ ] Establish a review path for new AI tools and significant new capabilities.
- [ ] Include AI access in employee offboarding and periodic access reviews.
- [ ] Consider regulatory, contractual, customer, privacy, and security requirements.
- [ ] Review AI governance as capabilities and business usage change.

WHERE TO LOOK

Review governance ownership, procurement/security review, vendor inventory, acceptable-use policy, access review, and risk-management processes.

WHAT GOOD LOOKS LIKE

AI adoption is visible to the organization, material services have owners, and new capabilities receive proportionate review rather than appearing independently across departments.

WATCH FOR

AI changes quickly. A one-time policy without an ongoing review process can become obsolete while the document still looks current.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTENTS

07

Network & Remote Access

Reduce unnecessary Internet exposure and separate trusted, guest, management, and higher-risk devices.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 41

Internet-facing services are inventoried

CRITICAL TECHNICAL

WHY THIS MATTERS

Unnecessary exposed services create direct attack paths into the organization.

WHAT TO CHECK

- [ ] Identify services intentionally reachable from the Internet.
- [ ] Review exposed remote administration such as RDP or SSH.
- [ ] Confirm management interfaces are not broadly Internet-accessible.
- [ ] Remove old port forwards and publishing rules.

WHERE TO LOOK

Review firewall, cloud, remote-access, and external scanning information.

WHAT GOOD LOOKS LIKE

Only required services are exposed and each has an owner and security rationale.

WATCH FOR

Old firewall rules often survive after the server or project they supported is gone.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 42

Firewall administration is protected

CRITICAL TECHNICAL

WHY THIS MATTERS

Compromise of a firewall or network-management account can undermine many other controls.

WHAT TO CHECK

- [ ] Confirm unique administrator identities are used where supported.
- [ ] Require MFA for cloud-managed network platforms where available.
- [ ] Restrict management access to trusted sources where practical.
- [ ] Review firmware/support status and administrative logs.

WHERE TO LOOK

Vendor-specific firewall/network management console.

WHAT GOOD LOOKS LIKE

Network administration is strongly authenticated, supported, and monitored.

WATCH FOR

Default or shared administrator credentials are especially risky.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 43

Guest wireless is separated

MEDIUM TECHNICAL

WHY THIS MATTERS

Guest and personal devices should not automatically receive the same trust as managed business devices.

WHAT TO CHECK

- [ ] Confirm guest Wi-Fi exists where visitors need access.
- [ ] Verify guest clients cannot freely access internal business resources.
- [ ] Review whether IoT or unmanaged devices need separate segmentation.
- [ ] Use modern wireless encryption and remove obsolete protocols.

WHERE TO LOOK

Review wireless controller, access points, VLANs, and firewall policies.

WHAT GOOD LOOKS LIKE

Network access reflects device trust and business need.

WATCH FOR

A separate SSID is not meaningful segmentation if firewall policy still allows internal access.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 44

Remote access is intentional

HIGH TECHNICAL

WHY THIS MATTERS

Remote connectivity can bypass the protection expected from an office network if poorly governed.

WHAT TO CHECK

- [ ] Inventory VPN, remote desktop, remote-support, and zero-trust access tools.
- [ ] Confirm MFA for remote administration where supported.
- [ ] Remove stale remote-access accounts.
- [ ] Review who can reach administrative or sensitive systems remotely.

WHERE TO LOOK

Review VPN/ZTNA/remote-support platform and identity controls.

WHAT GOOD LOOKS LIKE

Remote access is limited, strongly authenticated, and periodically reviewed.

WATCH FOR

Multiple overlapping remote-access tools can create blind spots.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 45

Network equipment is supported and updated

HIGH TECHNICAL

WHY THIS MATTERS

Unsupported routers, firewalls, access points, and switches may contain unpatched vulnerabilities.

WHAT TO CHECK

- [ ] Inventory critical network equipment and firmware versions.
- [ ] Identify end-of-support devices.
- [ ] Review security update practices.
- [ ] Back up critical configuration where appropriate.

WHERE TO LOOK

Vendor-specific management platforms and support lifecycle information.

WHAT GOOD LOOKS LIKE

Security infrastructure remains supported and recoverable.

WATCH FOR

A reliable firewall policy does not compensate for permanently unsupported hardware/software.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTENTS

08

Backup & Recovery

Make sure critical information can actually be recovered after deletion, failure, ransomware, or account compromise.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 46

Critical systems and data have a recovery strategy

CRITICAL BUSINESS

WHY THIS MATTERS

Organizations often discover after an incident that important SaaS or cloud data was never included in a real recovery plan.

WHAT TO CHECK

- [ ] Identify systems and data the business cannot operate without.
- [ ] Document how each is recovered.
- [ ] Include Microsoft 365/Google Workspace data, critical SaaS, servers, and endpoints as appropriate.
- [ ] Identify data that currently has no recovery method.

WHERE TO LOOK

Review native recovery/retention capabilities plus any dedicated backup platform.

WHAT GOOD LOOKS LIKE

Every critical workload has an intentional recovery approach aligned to business need.

WATCH FOR

Cloud service availability and retention are not automatically the same as an independent backup strategy.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 47

Backup failures are monitored

CRITICAL TECHNICAL

WHY THIS MATTERS

A backup system can silently fail for weeks if nobody owns alerts and capacity problems.

WHAT TO CHECK

- [ ] Identify who receives backup failure notifications.
- [ ] Review recent failures and unresolved warnings.
- [ ] Check storage/capacity health.
- [ ] Confirm backup credentials and integrations are still valid.

WHERE TO LOOK

Review backup platform monitoring and notification settings.

WHAT GOOD LOOKS LIKE

Failures are visible, owned, and remediated promptly.

WATCH FOR

Green dashboards are meaningful only if every intended workload is actually enrolled.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 48

Restore testing is performed

CRITICAL BUSINESS

WHY THIS MATTERS

A completed backup job does not prove usable data can be restored within the time the business needs.

WHAT TO CHECK

- [ ] Identify the date of the last successful restore test.
- [ ] Confirm the test included representative business data.
- [ ] Record whether restored data was usable.
- [ ] Compare actual restore time to business expectations.

WHERE TO LOOK

Use the backup/recovery platform and written recovery procedure.

WHAT GOOD LOOKS LIKE

Restore tests occur periodically and failures create remediation work.

WATCH FOR

Do not accept 'our backups run every night' as evidence of recoverability.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 49

Backups resist destructive attacks

CRITICAL SPECIALIST

WHY THIS MATTERS

Ransomware operators often try to delete backups before encrypting production systems.

WHAT TO CHECK

- [ ] Determine whether production administrators can delete all recovery copies.
- [ ] Use immutability/offline/logical separation where appropriate.
- [ ] Protect backup administration with strong authentication.
- [ ] Monitor deletion, retention, or configuration changes.

WHERE TO LOOK

Review backup architecture and administrator permissions.

WHAT GOOD LOOKS LIKE

A compromise of normal production credentials cannot trivially destroy every recovery copy.

WATCH FOR

This is an architectural question, not just a backup checkbox.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 50

Recovery priorities are documented

HIGH BUSINESS

WHY THIS MATTERS

During a major outage, teams need to know what comes back first and how long the business can tolerate disruption.

WHAT TO CHECK

- [ ] Identify the most critical services.
- [ ] Define acceptable outage duration for those services.
- [ ] Define how much recent data loss is tolerable.
- [ ] Ensure technical recovery expectations align with leadership expectations.

WHERE TO LOOK

Business continuity / disaster recovery documentation.

WHAT GOOD LOOKS LIKE

Business priorities drive recovery design and testing.

WATCH FOR

If leadership expects a four-hour recovery but the backup design requires two days, the gap should be known before an incident.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTENTS

09

Monitoring & Detection

Determine whether suspicious activity would be noticed and who is responsible for acting on it.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 51

Security alerts have an owner

CRITICAL BUSINESS

WHY THIS MATTERS

Alerts that nobody reviews are not an effective security control.

WHAT TO CHECK

- [ ] Identify who receives identity, email, endpoint, and platform security alerts.
- [ ] Confirm coverage for vacations, nights, or weekends as appropriate to risk.
- [ ] Review a recent real alert and what happened after it fired.
- [ ] Define escalation for high-severity events.

WHERE TO LOOK

Microsoft 365: Defender / Entra / Purview alerting.
Google Workspace: Security alerts / investigation tools plus endpoint/security platforms.

WHAT GOOD LOOKS LIKE

High-impact alerts reach a responsible person and have a clear escalation path.

WATCH FOR

Ask: 'Show me one security alert from the last 90 days and what happened next.'

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 52

Audit logging is available for investigations

HIGH TECHNICAL

WHY THIS MATTERS

Without sufficient logs, teams may be unable to determine what an attacker changed or accessed.

WHAT TO CHECK

- [ ] Confirm administrative actions are logged.
- [ ] Confirm identity/sign-in activity is available.
- [ ] Review retention periods.
- [ ] Restrict access to sensitive audit information.

WHERE TO LOOK

Microsoft 365: Purview Audit, Entra sign-in/audit logs, Defender.
Google Workspace: Admin audit and investigation/reporting tools.

WHAT GOOD LOOKS LIKE

Security-relevant actions are retained long enough to support likely investigations.

WATCH FOR

The right retention period depends on licensing, risk, and legal requirements.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 53

High-risk identity events are reviewed

HIGH TECHNICAL

WHY THIS MATTERS

Unusual sign-ins, repeated failures, impossible travel, or risky authentication patterns may indicate compromise.

WHAT TO CHECK

- [ ] Review available risky/suspicious login reporting.
- [ ] Confirm high-severity events generate action.
- [ ] Review repeated MFA failures or suspicious device/location activity.
- [ ] Document the containment path for a suspected account compromise.

WHERE TO LOOK

Microsoft 365: Entra sign-in/identity protection capabilities where licensed.
Google Workspace: Login/security investigation and alerting capabilities.

WHAT GOOD LOOKS LIKE

High-risk identity signals are reviewed and connected to an incident process.

WATCH FOR

Risk detections need context; do not treat every unusual location as proof of compromise.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 54

Security responsibilities are documented

MEDIUM BUSINESS

WHY THIS MATTERS

Small and midsize organizations often assume 'the IT company handles security' without defining what that actually includes.

WHAT TO CHECK

- [ ] Identify who owns identity security.
- [ ] Identify who owns endpoint security.
- [ ] Identify who owns backup/recovery.
- [ ] Identify who makes security risk decisions.

WHERE TO LOOK

Business governance activity.

WHAT GOOD LOOKS LIKE

There is no ambiguity about who is responsible for monitoring, decisions, and escalation.

WATCH FOR

Shared responsibility is fine; undefined responsibility is not.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTENTS

10

Incident Readiness

Make sure the organization can contain common incidents without inventing the process during the crisis.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 55

CEO/executive email compromise has a response path

CRITICAL BUSINESS

WHY THIS MATTERS

Executive mailbox compromise can lead to payment fraud, sensitive-data exposure, password resets, and impersonation.

WHAT TO CHECK

- [ ] Employees know who to call immediately.
- [ ] IT knows how to restrict/disable the account and revoke active sessions.
- [ ] Mail rules, delegates, forwarding, and sign-in activity are reviewed.
- [ ] Leadership/finance communication responsibilities are defined.

WHERE TO LOOK

Platform-specific containment steps should be documented for Microsoft 365 or Google Workspace.

WHAT GOOD LOOKS LIKE

The organization can contain the account quickly and preserve enough evidence to understand what happened.

WATCH FOR

Do not wait until the incident to decide who has authority to disable an executive account.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 56

Ransomware response is documented

CRITICAL SPECIALIST

WHY THIS MATTERS

Ransomware response requires rapid decisions about isolation, identity, backups, communications, and recovery.

WHAT TO CHECK

- [ ] Define who can isolate affected devices/systems.
- [ ] Define who decides whether to shut down broader services.
- [ ] Know how backup administrators are contacted.
- [ ] Define leadership, legal, insurance, and communications escalation as appropriate.

WHERE TO LOOK

Incident response and recovery plan; endpoint/network/identity tooling.

WHAT GOOD LOOKS LIKE

Containment and recovery responsibilities are known before an incident occurs.

WATCH FOR

A ransomware plan should be exercised, not just stored in a binder.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 57

Lost/stolen device procedure exists

HIGH BUSINESS

WHY THIS MATTERS

A delayed report can increase the time a lost device or account remains usable.

WHAT TO CHECK

- [ ] Employees know the reporting channel.
- [ ] IT can identify the device quickly.
- [ ] Account/device containment actions are documented.
- [ ] The organization knows when privacy/legal review is needed.

WHERE TO LOOK

Device management and incident procedures.

WHAT GOOD LOOKS LIKE

Employees can report immediately and IT knows the next actions.

WATCH FOR

Reporting should be easy enough to use outside business hours if your risk requires it.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 58

Security contacts are current

HIGH BUSINESS

WHY THIS MATTERS

Incident plans fail when contact information is stale or only available inside systems that are down.

WHAT TO CHECK

- [ ] Maintain current internal escalation contacts.
- [ ] Include IT/MSP, cyber insurance, legal, leadership, and key vendors where appropriate.
- [ ] Store a protected copy that is accessible during an outage.
- [ ] Review contacts periodically.

WHERE TO LOOK

Business continuity / incident documentation.

WHAT GOOD LOOKS LIKE

Critical contacts remain available even when normal systems are unavailable.

WATCH FOR

Do not store the only copy of your incident contacts inside the system you may lose access to.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 59

Tabletop exercises are performed

MEDIUM BUSINESS

WHY THIS MATTERS

A short scenario exercise reveals missing decisions and dependencies before a real incident.

WHAT TO CHECK

- [ ] Choose a realistic scenario such as business email compromise or ransomware.
- [ ] Walk through who would make each decision.
- [ ] Record gaps and unclear responsibilities.
- [ ] Assign follow-up actions.

WHERE TO LOOK

Business-led exercise; technical teams participate as needed.

WHAT GOOD LOOKS LIKE

The organization periodically practices high-impact scenarios and tracks lessons learned.

WATCH FOR

A tabletop does not need to be elaborate to be valuable.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTENTS

11

Governance & Employee Practices

Create repeatable expectations for security ownership, employee behavior, and ongoing review.

Use the controls in this section to identify what you can confirm, what needs attention, and what you cannot yet verify.

CONTROL 60

Security policies match real practices

MEDIUM BUSINESS

WHY THIS MATTERS

Policies that nobody follows provide little practical value and can create false confidence.

WHAT TO CHECK

- [ ] Maintain core acceptable-use, access, incident, and data-handling expectations.
- [ ] Confirm employees can actually follow the documented process.
- [ ] Review policies after material technology/process changes.
- [ ] Document meaningful exceptions.

WHERE TO LOOK

Business governance activity.

WHAT GOOD LOOKS LIKE

Policies are short enough to use, accurate enough to matter, and periodically reviewed.

WATCH FOR

A five-year-old policy referencing systems you no longer use is a warning sign.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 61

Employees can report phishing quickly

HIGH BUSINESS

WHY THIS MATTERS

Fast reporting gives defenders a chance to remove similar messages and investigate compromised accounts.

WHAT TO CHECK

- [ ] Employees know exactly how to report suspicious email.
- [ ] The reporting method is simple and visible.
- [ ] Employees receive feedback or acknowledgement when practical.
- [ ] IT/security knows what happens after a report.

WHERE TO LOOK

Use the platform's reporting features and your incident process.

WHAT GOOD LOOKS LIKE

Reporting is easier than deleting/ignoring the message.

WATCH FOR

Training should emphasize reporting, not punishing people for uncertainty.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 62

Unexpected MFA prompts are treated as suspicious

HIGH BUSINESS

WHY THIS MATTERS

Repeated MFA prompts can be part of account takeover attempts or social engineering.

WHAT TO CHECK

- [ ] Employees know not to approve unexpected prompts.
- [ ] Employees know where to report them.
- [ ] Help desk/IT understands how to investigate the affected account.
- [ ] Authentication methods reduce blind 'approve' behavior where practical.

WHERE TO LOOK

Review your identity platform and security-awareness content.

WHAT GOOD LOOKS LIKE

Unexpected authentication prompts trigger caution and reporting.

WATCH FOR

MFA is not foolproof when users can be socially engineered into approving access.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

CONTROL 63

Payment and bank-detail changes are independently verified

CRITICAL BUSINESS

WHY THIS MATTERS

Business email compromise frequently targets invoices, payroll, and bank-detail changes.

WHAT TO CHECK

- [ ] Require an independent verification channel for unusual payment instructions.
- [ ] Do not rely solely on replying to the same email thread.
- [ ] Train finance and leadership on impersonation tactics.
- [ ] Document how suspected fraud is escalated.

WHERE TO LOOK

Business process control; technical email protections provide supporting defense.

WHAT GOOD LOOKS LIKE

High-risk financial changes require verification outside the original request channel.

WATCH FOR

This simple operational control can stop attacks that bypass technical email filtering.

YOUR ASSESSMENT

○ Meets Baseline ○ Needs Attention ○ Unable to Verify ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

☐ Reviewed ☐ Planned ☐ Remediated ☐ Verified

CONTROL 64

Security reviews occur on a defined cadence

MEDIUM BUSINESS

WHY THIS MATTERS

Cloud environments change constantly as users, apps, devices, vendors, and settings evolve.

WHAT TO CHECK

- [ ] Set a recurring review cadence for identity, privileged access, guests, sharing, devices, and backups.
- [ ] Assign an owner for each review.
- [ ] Record findings and due dates.
- [ ] Reassess after major migrations, acquisitions, incidents, or vendor changes.

WHERE TO LOOK

Business governance plus platform reports.

WHAT GOOD LOOKS LIKE

Security review is an operating process, not a one-time project.

WATCH FOR

A strong baseline can degrade quietly as the environment changes.

YOUR ASSESSMENT

- ○ Meets Baseline
- ○ Needs Attention
- ○ Unable to Verify
- ○ N/A

OWNER

TARGET DATE

NOTES / FINDINGS

- [ ] Reviewed
- [ ] Planned
- [ ] Remediated
- [ ] Verified

Findings register

Capture the issues that require follow-up. Keep descriptions clear enough for another team member to understand.

FINDING 01

FINDING / GAP	PRIORITY	OWNER

NEXT ACTION	TARGET	STATUS

FINDING 02

FINDING / GAP	PRIORITY	OWNER

NEXT ACTION	TARGET	STATUS

FINDING 03

FINDING / GAP	PRIORITY	OWNER

NEXT ACTION	TARGET	STATUS

FINDING 04

FINDING / GAP	PRIORITY	OWNER

NEXT ACTION	TARGET	STATUS

FINDING 05

FINDING / GAP	PRIORITY	OWNER

NEXT ACTION	TARGET	STATUS

Findings register

Capture the issues that require follow-up. Keep descriptions clear enough for another team member to understand.

FINDING 06

FINDING / GAP	PRIORITY	OWNER

NEXT ACTION	TARGET	STATUS

FINDING 07

FINDING / GAP	PRIORITY	OWNER

NEXT ACTION	TARGET	STATUS

FINDING 08

FINDING / GAP	PRIORITY	OWNER

NEXT ACTION	TARGET	STATUS

FINDING 09

FINDING / GAP	PRIORITY	OWNER

NEXT ACTION	TARGET	STATUS

FINDING 10

FINDING / GAP	PRIORITY	OWNER

NEXT ACTION	TARGET	STATUS

30 / 60 / 90 day security plan

Prioritize risk and dependencies rather than trying to fix everything at once.

FIRST 30 DAYS

ACTION	OWNER / DATE

31-60 DAYS

ACTION	OWNER / DATE

61-90 DAYS

ACTION	OWNER / DATE

Questions to ask your IT team or provider

- [ ] 01 Show me the actual list of users with administrator access.
- [ ] 02 Is MFA required for everyone, or only enabled/enrolled?
- [ ] 03 Which users or systems are excluded from our normal authentication controls?
- [ ] 04 Can employees create public or anonymous file-sharing links?
- [ ] 05 Which third-party applications currently have access to our Microsoft 365 or Google Workspace data?
- [ ] 06 Which business devices are not managed or not reporting security health?
- [ ] 07 Show me a recent high-severity security alert and what happened after it fired.
- [ ] 08 When was our last successful backup restore test, and what exactly was restored?
- [ ] 09 Can the same administrator who manages production also delete every backup copy?
- [ ] 10 Which systems can be reached directly from the Internet?
- [ ] 11 How quickly is access removed when someone leaves the company?
- [ ] 12 Who is responsible for security monitoring after hours or during vacations?
- [ ] 13 If an executive mailbox were compromised today, what are the first five actions?
- [ ] 14 Which security controls depend on licenses or products we do not currently own?
- [ ] 15 Which AI tools are employees currently using with company information?
- [ ] 16 Which AI applications or agents can access our Microsoft 365, Google Workspace, or other business data?
- [ ] 17 What are the top three security risks you believe we should address next?

Questions discovered during the checkup

Unanswered questions are useful outputs. Capture them here instead of guessing.

01

02

03

04

05

06

07

NEXT REVIEW DATE

You found a gap. What happens next?

Identifying a security gap is only the first step. Some findings are straightforward; others have dependencies involving users, licensing, applications, vendors, business processes, compliance obligations, testing, monitoring, and recovery.

ASSESS	Validate what is actually happening and how much risk it creates.
ARCHITECT	Determine the right design for the business rather than applying a generic setting.
IMPLEMENT	Make changes safely with testing, communication, and rollback planning.
VALIDATE	Confirm the control actually operates as intended.
DOCUMENT	Create repeatable operational knowledge instead of one-time fixes.
ADVISE	Help leadership prioritize risk, cost, and business impact.

OLSON TECH SERVICES

Architecture, security, and technology advisory for secure, scalable enterprise environments.

olsontech.dev

Important notes & limitations

This workbook is an educational security baseline and self-assessment aid. It is not a penetration test, vulnerability assessment, legal opinion, compliance certification, or guarantee of security.

Security requirements vary by organization, industry, regulation, contractual obligation, licensing, architecture, and risk tolerance.

Microsoft 365 and Google Workspace navigation, licensing, and product capabilities change over time. Menu references are intentionally directional rather than a substitute for current vendor documentation.

Before broad production changes, consider business dependencies, emergency/service accounts, application compatibility, user impact, testing, monitoring, and rollback.

For the best interactive experience, download this PDF and open it in a PDF application that supports standard AcroForm fields. Save a working copy before beginning.