PRACTITIONER RESOURCE

Verify Your Microsoft 365, Google Workspace and GoDaddy Controls

Review sign in protections, administrator access, email retention and audit records across Microsoft 365, Google Workspace and GoDaddy.

Edition 2026-11-03 · Updated November 3, 2026 · miami-computer-forensics.com/guides/cloud-controls/

The useful question is whether a control protects the accounts and records the business actually uses. A subscription invoice, an administrator's recollection and a screenshot of a proposed policy answer different questions. Begin with a named owner, an inventory of identities and a record of the current settings. Then establish which protections are enforced, which exceptions remain and what evidence will show that a change worked.

This guide is a verification and rollout sequence, built so changes land in a planned order rather than all at once. Identity changes can lock out administrators, stop scanners or interrupt business applications. Preserve relevant settings and logs first if compromise or litigation is suspected. Use an approved change window, a tested recovery path and a person authorized to stop the rollout. Product names and licensing vary, so confirm every setting in your own tenant.

Identify the service and the people who actually control it

Record the Microsoft tenant or Google Workspace organization, primary and secondary domains, subscription editions and responsible administrators. Identify the registrar, DNS host, email platform, reseller, backup provider and security provider separately. A domain registered with GoDaddy may use Microsoft 365, Google Workspace or another email service. The registrar account and the Microsoft tenant administrator are separate identities, and each needs its own protection.

Create an access register with one row per privileged role: person, named account, authority, authentication method, recovery owner and last review. Include outside providers and former administrators. Record who holds each password and recovery code, and keep the codes themselves in the approved vault. Confirm that the organization can regain access if its only consultant becomes unavailable. The output is a verified ownership and administration map, with control staying where it is today.

Plan strong sign in protections around business dependencies

Check MFA enrollment and actual enforcement separately. An enrolled user may still access an excluded application or an uncovered account. For Microsoft, determine whether security defaults or a deliberately configured Conditional Access policy set is responsible for protection. These are different approaches. Keep each working policy in place and record why it fits. Document approved exclusions and the controls that protect them. [1]

© 2026 Global Digital Forensics, Inc. All rights reserved.

Before enforcement, identify older clients, service identities, applications and equipment that depend on unattended authentication. Pilot the proposed policy with representative users and confirm the administrator recovery procedure. Prefer phishing resistant methods where the service and use case support them. For Google Workspace, inspect the organizational units, groups and enrollment settings that determine enforcement. A policy at the wrong organizational level can leave the intended users unprotected. [5]

Separate administrator work from everyday email

Use identifiable administrative accounts for privileged changes and ordinary accounts for normal correspondence and browsing. Review role assignments against current duties. Remove obsolete privileges through the approved process, while preserving records relevant to a dispute or incident. Treat shared administrator credentials as a gap requiring an accountable replacement rather than assuming that a list of people who know the password is an access record.

Prepare a recovery method that is both protected and usable. Identify who can approve emergency access, where recovery materials are secured and how access will be documented. Google recommends separate administrator and daily accounts and recovery readiness. Test the organizational process with the production recovery secrets kept in their secured location. After a personnel change, verify that recovery addresses and telephone numbers still belong to authorized people. [4]

Verify audit logging by producing a known record

Ask an authorized administrator to demonstrate a recent, harmless administrative event in the relevant audit search. Record the event time, search window, service, filters and result. Retain the exported record with its source and collection time. A setting that says auditing is enabled is useful configuration evidence, but a successful sample confirms something different: that the expected activity can be found through the available workflow.

Microsoft's documentation requires customers to verify auditing status and identifies exceptions for some business editions. Audit retention also depends on license, workload and policy. Confirm the retention period in this tenant rather than borrowing another tenant's figure. For both platforms, record the earliest returned activity, permissions needed to search, export limits and known gaps. Monitoring starts from what the provider records and retains, so capture the earliest available date now. [2] [3]

Inspect mail forwarding, delegation and application access

Review forwarding at the mailbox, rule, connector and organization levels appropriate to the platform. Identify delegated mailbox access, send permissions, shared mailboxes and third party applications that can read messages or files. Ask the business owner to explain each expected relationship. Preserve suspicious configurations and available activity before changing them during an active matter; the order of containment and evidence collection should follow the incident plan.

A password change closes one route of access; sessions, tokens, application grants and recovery settings each need their own review through the supported administrative process. Document what was revoked, what was left in place and why. A list of permissions shows potential reach, and observed activity is where we look for actual use. Report those two things separately when advising management or counsel.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Check external sharing and ownership of business information

Examine the sharing rules for OneDrive, SharePoint and Teams, or Google Drive and shared drives, according to the organization's actual use. Review representative sensitive repositories, guest access, public or broadly accessible links and externally owned files. Identify the owners who can approve a change. A tenant wide restriction can affect collaboration, while an exception can preserve unnecessary access if nobody owns its review.

Build a small evidence set for each significant repository: business purpose, owner, sharing setting, membership review and one example showing the effective access. Record whether the example is representative or an exception. Include files linked from messages rather than assuming that preserving a mailbox also preserves every linked document. When employment changes, transfer or preserve business information through an authorized process before deleting accounts or changing licenses.

Distinguish retention, legal holds, archives and backups

Ask what each service is supposed to accomplish. Retention rules govern specified content over time. A legal hold addresses preservation within its supported scope. An archive may preserve an additional copy. A backup is useful only within its actual coverage and recovery capability. Coverage for messages, collaboration history, activity logs and linked files has to be confirmed for each one.

Have the provider or administrator identify the protected locations, excluded services, retention settings, account dependencies and restore procedure. For a preservation matter, directing counsel sets the scope. For operational recovery, the business sets recovery needs and authorizes a safe restoration exercise. Keep the configuration record and the restoration result separate. A tenant level restoration exercise, beyond a single file restore, shows whether recovery fits the business's required time.

Secure the GoDaddy account as well as the email tenant

For Microsoft 365 purchased through GoDaddy, verify which administrative tasks are available through the Email and Office dashboard and which require supported Microsoft administration. Record the account owner and the tenant administrator. Protect the GoDaddy account itself, including its recovery details and domain control permissions. MFA on the Microsoft email account leaves the registrar and reseller accounts to be protected on their own. [6]

GoDaddy and Microsoft documentation may describe different rollout details as products change. Use the current workflow for the actual subscription and confirm the effective policy after a change. Confirm the grace period and the dependencies for the specific tenant before an older control is retired. Where a requested capability sits outside the current edition, ask the reseller to explain the available edition and the escalation path, and record the answer.

Establish monitoring, escalation and a record of control ownership

Assign someone to review significant sign in, administrator, application and sharing events appropriate to the service. Define the events that require immediate escalation and the people who can authorize containment. A working response process routes each notification to a current, monitored owner. Confirm that a representative alert reaches a person with a documented next step.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Maintain a change log linking the business reason, approved configuration, implementation time, operator and verification result. Record exceptions with an owner and review date. Keep rejected proposals and failed changes so the record explains what actually happened. This is more useful during an incident or examination than a policy document that describes controls nobody can demonstrate.

Work through a controlled first week sequence

On the first day, establish ownership, preserve relevant logs and settings, and identify urgent access risks. Next, verify privileged access, MFA coverage, recovery arrangements and active application grants. Then review representative sharing and retention settings, available audit records and the alert routing process. Sequence disruptive changes around the business, not around the order of this guide.

Close each action with a named owner, evidence of the effective setting and a remaining risk statement. Mark an item complete once its evidence is in hand, and keep the rest on the open list with an owner. If the team discovers suspected compromise, unexplained forwarding, disappearing records or a deadline that is shorter than the available retention, pause the routine review and call the 24/7 hotline at (800) 868-8189. The objective is an accountable set of controls whose operation can be shown, with a clear record of the open items and their owners.

Bring Your Tenant Review to a Scoping Call

Bring the access register, your MFA policy export and the open items list to a free scoping call with a GDF security lead. On that first call we walk through your Microsoft 365 or Google Workspace settings, mark the gaps that matter most and set out a review or testing scope with a timeline. Call (786) 219-1210 or the 24/7 hotline at (800) 868-8189, or write to info@evestigate.com. To keep preparing, browse the cybersecurity guide library.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Cloud Tenant Review Checklist

Work through these questions with the people who own the systems and the legal or business decisions. Mark unknown or not applicable answers plainly, and record an owner, a confirming source and the date for each one.

Record who controls each password, recovery key or unlock code and how a secure handoff can be arranged, and we collect the secrets themselves through that handoff. Keep completed copies in the location counsel or the company approves, and share the completed record through the secure transfer method agreed on the first call.

Who is directing the matter and who can authorize technical access?

Identify directing counsel, the business decision maker, the IT security owner and any outside administrator. Record the immediate deadline, relevant period and known preservation risk. Authority to examine comes from ownership, policy and counsel's instruction, so record each one; possession of a device and administrator access are separate facts.

Answer:

Owner, source, date and unresolved questions:

Who provides the email service and who administers it?

Identify Microsoft 365, Google Workspace, an internal Exchange environment, a hosted service or a combination. Record the tenant or organization reference, relevant domains, mailbox owners, aliases, shared mailboxes and the MSP or administrator responsible. Identify available preservation and export permissions and any licensing question that needs confirmation.

Answer:

Owner, source, date and unresolved questions:

Does the company have archiving, backups or preservation holds in place?

Name each service and distinguish an archive or journal from a backup, a retention policy and a matter specific hold. Identify what each covers, the available dates, deletion or rotation rules and who can export or restore records. Record whether someone has verified coverage with a test search or export, since a subscription record shows purchase rather than coverage.

Answer:

Owner, source, date and unresolved questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Which administrator roles exist, and who holds each one?

List every global, privileged and delegated administrator role in the tenant, the named account that holds it, the authentication method on that account and the date of the last access review. Include outside providers and emergency access accounts.

Answer:

Owner, source, date and unresolved questions:

How is MFA enforced, and which accounts or applications are excluded?

Record whether security defaults, Conditional Access or Google 2 Step Verification enforcement protects each group of users, the organizational units or groups covered, and every approved exclusion with its owner and compensating control.

Answer:

Owner, source, date and unresolved questions:

Which forwarding rules, mailbox delegations and third party applications are in place?

Export forwarding at the mailbox, rule and organization level, delegated and send as permissions, and consented applications with their permission scopes. Mark each one expected, unexpected or unknown, and name the business owner who can explain it.

Answer:

Owner, source, date and unresolved questions:

How are files shared outside the organization?

Record the tenant sharing settings, the guest access policy and the repositories that carry public or anyone links, with the owner who approves each exception and the date it was last reviewed.

Answer:

Owner, source, date and unresolved questions:

Who controls identity, administrator access and multifactor authentication?

Identify the identity provider, relevant privileged accounts, outside administrator and person who can approve an export or collection. Note access dependencies such as an unavailable administrator or authentication device, naming who holds them. Identify shared or delegated access, because attributing that account activity to one person takes corroborating evidence.

Answer:

Owner, source, date and unresolved questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Which cloud storage, collaboration and messaging services contain relevant work?

Identify shared drives, Teams, SharePoint, OneDrive, Slack, Google Chat and other platforms actually used for the relevant work. Note external ownership, linked documents, personal accounts used for business and any unsupported or unavailable source. Linked files and separate chat conversations live outside the mailbox, so list them as sources of their own.

Answer:

Owner, source, date and unresolved questions:

Which audit and sign in logs are available now, and for how long?

Ask the responsible administrator which email, identity, sign in, audit, cloud sharing and security records exist for the relevant period. Record actual date coverage, export permissions, known gaps and the next expiration or rotation point. Logging switched on today records activity from today forward, so note the date each source began recording.

Answer:

Owner, source, date and unresolved questions:

What has already changed in the tenant or its accounts?

Record password resets, role changes, MFA or conditional access changes, mailbox rules removed, retention or audit settings changed, accounts deleted and applications revoked. Identify who acted, when and why, so the review can separate the configuration you started with from changes made since.

Answer:

Owner, source, date and unresolved questions:

Which tenant, edition, reseller and DNS owner are involved?

Identify the actual platform and authorized administrators before using a product checklist.

Answer:

Owner, source, date and unresolved questions:

Which applications, service identities or devices could be affected by an identity control change?

Record dependencies, approved exceptions, recovery arrangements and a change owner.

Answer:

Owner, source, date and unresolved questions:

Primary sources and further reading

Sources checked November 3, 2026.

1: Microsoft Entra security defaults

© 2026 Global Digital Forensics, Inc. All rights reserved.

https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults

2: Microsoft Purview: turn auditing on or off
https://learn.microsoft.com/en-us/purview/audit-log-enable-disable

3: Microsoft audit log retention policies
https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

4: Google Workspace security best practices for administrators
https://knowledge.workspace.google.com/admin/users/security-best-practices-for-administrator-accounts

5: Google Workspace: deploy 2-Step Verification
https://knowledge.workspace.google.com/admin/security/deploy-2-step-verification

6: GoDaddy Microsoft 365 security defaults
https://www.godaddy.com/help/enable-or-disable-security-defaults-40128

Talk to a Senior GDF Security Lead

Bring this checklist to a free scoping call. We review your answers, confirm the systems and operating limits that matter and set out the testing depth, the timeline and the deliverables.

Miami office: (786) 219-1210 · **24/7 hotline:** (800) 868-8189 · **Email:** info@evestigate.com

miami-computer-forensics.com

© 2026 Global Digital Forensics, Inc. All rights reserved.