Cloud Account Security Controls to Verify Now

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

Edition 2026-11-03 · Online at newyorkcomputerforensics.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 implementation sequence: confirm each control and its dependencies, then switch it on. Identity changes reach administrators, scanners and business applications, so schedule each one in an approved change window with a tested recovery path and a person authorized to pause the rollout. Where compromise or litigation is suspected, preserve the relevant settings and logs first. Product names and licensing vary, so confirm the settings of the current 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. Its registrar account is a separate identity from the Microsoft tenant administrator.

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. Confirm that the organization can regain access if its only consultant becomes unavailable. The output is a verified ownership and administration map.

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. Document approved exclusions and the controls that protect them. [Microsoft Entra security defaults]

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. [Google Workspace: deploy 2-Step Verification]

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

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. Replace shared administrator credentials with named, accountable accounts.

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 production recovery secrets kept in their secure store. After a personnel change, verify that recovery addresses and telephone numbers still belong to authorized people. [Google Workspace security best practices for administrators]

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 each tenant's actual retention. For both platforms, record the earliest returned activity, permissions needed to search, export limits and known gaps. [Microsoft Purview: turn auditing on or off] [Microsoft audit log retention policies]

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.

Alongside any password change, review sessions, tokens, application grants and recovery settings through the supported administrative process. Document what was revoked, what was left in place and why. A list of permissions shows potential reach; observed activity is needed to support a conclusion about use. Report those two things separately when advising management or the security lead.

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.

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

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, since linked documents are preserved separately from the mailbox. 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 covers what it was configured to capture and restore. Record which messages, collaboration history, activity logs and linked files each one actually protects.

Have the provider or administrator identify the protected locations, excluded services, retention settings, account dependencies and restore procedure. For operational recovery, the business sets recovery needs and authorizes a safe restoration exercise. Keep the configuration record and the restoration result separate. Test restoration at the scale the business relies on, measured against its required recovery 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, with its own MFA alongside the protection on the Microsoft email account. [GoDaddy Microsoft 365 security defaults]

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. Where a requested capability is missing from the reseller dashboard, ask the reseller to explain the available edition and escalation path.

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. Confirm that a representative alert reaches a person with a documented next step.

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.

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

Sequence disruptive changes around the business.

Close each action with a named owner and evidence of the effective setting, and keep any item awaiting evidence on the open list. If the team discovers suspected compromise, unexplained forwarding, disappearing records or a deadline shorter than the available retention, call the 24/7 hotline at (800) 868-8189 and we will set the preservation steps with you. The result is an accountable set of controls whose operation can be shown.

Information Gathering Q&A Checklist

Use this Q&A with the people who own the systems and the relevant legal or business decisions. Mark unknown or not applicable answers explicitly. Record an owner, a confirming source and the date.

Record who controls access to each source and how a secure handoff can be arranged, and keep completed copies with the matter records the company maintains.

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 open questions:

Who holds global administrator or super administrator roles today?

List every privileged account, its owner and whether it is used for everyday email. [Google Workspace security best practices for administrators]

Answer:

Owner, source, date and open questions:

Is multifactor authentication enforced for every account, and which accounts are excluded?

Record the enforcement method, each exclusion and the reason it exists. [Microsoft Entra security defaults] [Google Workspace: deploy 2-Step Verification]

Answer:

Owner, source, date and open questions:

Is audit logging on, and how long are records kept?

Produce a known test event, confirm it appears in the audit log and record the retention period. [Microsoft Purview: turn auditing on or off] [Microsoft audit log retention policies]

Answer:

Owner, source, date and open questions:

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

Which forwarding rules, mailbox delegations and third party application grants exist?

Export each one with its creator and date, and flag any external forwarding.

Answer:

Owner, source, date and open questions:

Which files and folders are shared externally or by open link?

List the owners, the sharing settings and any business record held only in a personal account.

Answer:

Owner, source, date and open 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 open questions:

Who controls the GoDaddy account, the domain registration and the DNS records?

Name the account owner, the recovery contacts and the people who can change DNS. [GoDaddy Microsoft 365 security defaults]

Answer:

Owner, source, date and open questions:

Primary sources and further reading

Sources checked November 3, 2026.

1. Microsoft Entra security defaults 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

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

Scope Your Assessment

The first call is a free consultation with a senior security lead. We review the systems, the review or audit you face and its timing, and recommend the assessment depth that answers it. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.

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