Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/audit-discovery-preparation/data-sources/

AUDIT AND DISCOVERY PREPARATION

Where potentially relevant data can live

Explore 36 candidate data source categories, including cloud services, backups, archives, business systems and logs that may need separate requests.

Use this atlas as an interview menu. Each category is a candidate until its owner confirms the actual system, account, period and available records. Record both business content and separate metadata/logs. Counsel and the receiving specialist set relevance, preservation, lawful authority and proportionate scope.

D01 Laptops and desktops

Possible information
Local files, downloads, synced copies, browser records and user/application artifacts if retained.

Ask the owner
Which device IDs, user profiles, encryption/recovery arrangements and relevant dates exist? Is a scoped forensic collection needed?

Likely contact
IT asset owner and custodian

Details to confirm
The examiner checks whether a local synced folder holds full files or placeholders and collects cloud content from the cloud source.

Reference: NI04; MS01

NI04 MS01

D02 Mobile phones and tablets

Possible information
Messages, work apps, photographs, attachments and account links subject to device/app state.

Ask the owner
Company owned or personal? Which apps and accounts were used, who can authorize collection, and what is available now?

Likely contact
Custodian, MDM owner and legal

Details to confirm
The examiner confirms which app data MDM can reach and what counsel has authorized for personal information, and checks deletion and encryption status to plan any recovery work.

Reference: NI04; LG01

NI04 LG01

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

D03 External media and paper

Possible information
USB/external disks, removable media, notebooks, printouts and offsite files.

Ask the owner
Which media or physical locations were used and who has custody?

Likely contact
Custodian, facilities and records manager

Details to confirm
Records on physical media are traced through physical identifiers, custody records and interviews alongside any network access log, so preserve identifiers and custody from the start.

Reference: NI04; NY02

NI04 NY02

D04 Email and calendars

Possible information
Messages, attachments, drafts, calendars, tasks, shared/delegated mailboxes and groups where supported.

Ask the owner
Identify all primary/alias/legacy/shared addresses and relevant mail systems; what export includes attachments and metadata?

Likely contact
Messaging administrator and business owner

Details to confirm
The examiner extends an individual mailbox search to shared mailboxes, external mail, deleted or inactive users and cloud linked documents.

Reference: MS01; GO01

MS01 GO01

D05 OneDrive and personal work storage

Possible information
User owned work files, supported versions, sharing links and retained content.

Ask the owner
Which exact user/site URLs exist, including deleted/unlicensed accounts? What holds, licenses and deletion schedules apply?

Likely contact
SharePoint/OneDrive administrator

Details to confirm
The examiner reviews recycle bin content through its own route, apart from normal eDiscovery search, and confirms current archive and payment conditions for unlicensed accounts with the administrator.

Reference: MS03; MS05

MS03 MS05

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

D06 SharePoint and Teams files

Possible information
Team sites, libraries, lists and separate channel sites where used.

Ask the owner
Which site/library and private or shared channel locations are relevant? Where do linked files actually live?

Likely contact
Site and collaboration administrators

Details to confirm
Channel files, lists, versions and linked targets are collected from their own sites alongside the mailbox messages.

Reference: MS01; MS02; MS05

MS01 MS02 MS05

D07 Teams messages and meetings

Possible information
Searchable compliance records, chats/posts, recordings/transcripts and meeting artifacts where supported.

Ask the owner
Which chat/channel/meeting types, policies, organizers and storage locations apply? What known content exclusions exist?

Likely contact
Teams, messaging and site administrators

Details to confirm
eDiscovery uses compliance records rather than the live Teams database. The examiner locates files and recordings in their own storage locations and checks the features and channel behavior in effect for the period.

Reference: MS02

MS02

D08 Google Gmail and calendars

Possible information
Messages, attachments and calendar content supported by the actual Workspace/Vault setup.

Ask the owner
Which accounts/domains, delegated/group mail, licenses and retention/holds existed for the relevant period?

Likely contact
Workspace/Vault administrator

Details to confirm
Vault works on the live Workspace data of supported, licensed services under configured policies, so the examiner confirms licenses and policies first and keeps users and their licenses in place until preservation is complete.

Reference: GO01

GO01

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

D09 Google Drive and shared drives

Possible information
Owned/shared files, shared drive material and versions/exports as supported.

Ask the owner
Who owns each file/shared drive, including external owners? Which search and export settings were used?

Likely contact
Drive/Vault administrator and document owners

Details to confirm
The examiner follows shortcuts to their external targets, requests historical versions specifically and confirms the export scope with the provider.

Reference: GO01

GO01

D10 Google Chat Meet and Voice

Possible information
Supported messages, meeting artifacts, recordings and Voice records if used and retained.

Ask the owner
Which services, history settings, organizers and licenses were in use?

Likely contact
Workspace/Vault and communications administrators

Details to confirm
The examiner confirms coverage service by service.

Reference: GO01; GO02

GO01 GO02

D11 Slack and shared workspaces

Possible information
Channels, direct messages, files and preserved edits/deletions where the plan and tools support them.

Ask the owner
Which workspaces, plan, export authority, apps, retention and Slack Connect parties apply?

Likely contact
Workspace/org owner and legal

Details to confirm
Export and API access follow the Slack plan and permissions, and the examiner identifies which external organizations control shared content and its retention.

Reference: SL01; SL02

SL01 SL02

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

D12 Other messaging and meeting systems

Possible information
Business use of texts, WhatsApp, Signal, Zoom, chat, voice or other collaboration tools.

Ask the owner
Ask each custodian which actual accounts/apps were used, whether history/recording existed and who controls it.

Likely contact
Custodian, communications owner and counsel

Details to confirm
Candidate category: the examiner checks encryption, device state, disappearing message settings, contracts and legal authority for each app, and plans any export or recovery from those facts.

Reference: NI04; LG01

NI04 LG01

D13 Identity and access platforms

Possible information
Account, sign in, role, group, authentication and administrator records if logged.

Ask the owner
Which tenant/account IDs, role assignments, event sources and dates can be exported?

Likely contact
Identity administrator

Details to confirm
Tying a later action to a named person combines the sign in record with session, device and other corroboration. The examiner confirms log availability against actual coverage and retention.

Reference: NI04; MS04; GO02

NI04 MS04 GO02

D14 Security monitoring and endpoints

Possible information
SIEM, EDR, DLP, alerts, investigation cases and file/device activity if collected.

Ask the owner
Which agents, policies, sensors, fields, exclusions and retained periods cover the relevant event?

Likely contact
SOC, endpoint owner and providers

Details to confirm
The examiner reads each alert as a lead and interprets it against the underlying events.

Reference: NI04; MS04

NI04 MS04

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

D15 Network and remote access

Possible information
VPN, firewall, proxy, DNS, wireless and remote support records if enabled.

Ask the owner
Which identity/device/IP mappings and times are available; what NAT, clock or shared account issues exist?

Likely contact
Network team and remote access provider

Details to confirm
Network records capture connections; file contents and the human actor are corroborated from endpoint, application and identity records.

Reference: NI04

NI04

D16 Microsoft audit and export reports

Possible information
Activity logs, query/export job records, processing errors and source counts.

Ask the owner
What exact licenses, policies, event types, role filters, earliest dates and error reports apply?

Likely contact
Purview administrator

Details to confirm
Content retention and audit log retention are set separately, so the examiner confirms each. A zero result is checked against scope, indexing, permissions and filters before it is read as empty.

Reference: MS04; MS06

MS04 MS06

D17 Google audit and export reports

Possible information
Admin, login, Drive and other service events, job histories and errors as available.

Ask the owner
Which log type, time period, query, export mechanism and event delay apply?

Likely contact
Workspace security/Vault administrator

Details to confirm
Retention and delay vary by log. The examiner preserves activity logs on their own schedule, alongside the Vault content hold.

Reference: GO01; GO02

GO01 GO02

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

D18 Cloud infrastructure and storage

Possible information
Virtual machines, object stores, snapshots, databases, cloud keys and management or data access logs where configured.

Ask the owner
List accounts, subscriptions, regions, services, logging settings, bucket/container IDs, lifecycle rules and providers.

Likely contact
Cloud administrator and application owners

Details to confirm
AWS default Event history holds 90 days of regional management events; data events such as storage downloads are recorded through separately configured trails, which the examiner checks for.

Reference: AW01; NI04

AW01 NI04

D19 Email journals and compliance archives

Possible information
Journaled/ingested mail, attachments, other captured feeds and archive search histories.

Ask the owner
Which feeds/users/date ranges were captured, what failed, and does export preserve original fields and attachments?

Likely contact
Archive owner and provider

Details to confirm
Candidate category. The examiner verifies capture, deduplication and migration history and compares the archive with the source system for completeness.

Reference: NI04; LG01

NI04 LG01

D20 Backups snapshots and recovery replicas

Possible information
Point in time data, application/database copies, endpoint backups and old recovery media.

Ask the owner
Which systems/dates, catalogs, keys, overwrite dates, restore methods, cost and licensing are involved?

Likely contact
Backup administrator and provider

Details to confirm
Ask the specialist whether a justified isolated restoration is necessary; restorability is confirmed by a test restore, with job success reports as supporting records.

Reference: NI04; LG01

NI04 LG01

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

D21 Legacy systems and migrations

Possible information
Decommissioned servers, previous tenants/domains, migration staging, historical exports and transfer logs.

Ask the owner
What moved, when, from/to which system, with what reconciliation and known exclusions?

Likely contact
Former owners, integration/migration team and provider

Details to confirm
Earlier data is read from the legacy system or its exports, using the old schemas, software or keys where needed.

Reference: NI04; LG01

NI04 LG01

D22 CRM and sales systems

Possible information
Customer/contact records, opportunities, activities, attachments, quotes and field histories where supported.

Ask the owner
Which objects, IDs, fields, audit/history features, attachments and integrations cover the dispute?

Likely contact
Sales operations and CRM administrator

Details to confirm
Candidate category. The examiner requests history, deleted records, relationships and linked files specifically, beyond the standard reports, and confirms the vendor and version.

Reference: NI04; LG01

NI04 LG01

D23 ERP accounting and procurement

Possible information
Orders, invoices, payments, approvals, vendor/customer changes and journals where retained.

Ask the owner
Which transaction IDs, attachments, effective/posting dates, approval records and audit histories are needed?

Likely contact
Finance, procurement and application owner

Details to confirm
Approval, delivery, later adjustments and bank detail changes are traced through approval, logistics and audit records alongside the invoice.

Reference: NI04; LG01

NI04 LG01

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

D24 Contracts and electronic signatures

Possible information
Negotiation files, clause versions, signature envelopes, completion certificates and recipient events where available.

Ask the owner
Which CLM or electronic signature service, envelope/agreement IDs, history/certificates and linked exhibits exist?

Likely contact
Legal operations, contracting and signing service administrator

Details to confirm
A signature certificate is one part of the record; signer identity and the negotiation history are corroborated from account, email, device and negotiation records alongside it.

Reference: DS01; LG01

DS01 LG01

D25 Document management and deal rooms

Possible information
Matter/project files, version chains, comments, permissions, workspace activity and external shares where supported.

Ask the owner
Which workspaces, version policies, exports and external party copies should the specialist consider?

Likely contact
Records/legal operations and workspace owner

Details to confirm
Candidate category. Earlier drafts, annotations and workspace audit history are requested from the platform alongside the current document download.

Reference: NI04; LG01

NI04 LG01

D26 Tickets project and engineering tools

Possible information
Requests, task comments, approvals, attachments, release/change records, code and designs.

Ask the owner
Which project/repository IDs, branches, issue types, revisions and external integrations contain relevant work?

Likely contact
Engineering, service desk and project owners

Details to confirm
Candidate category. Export relationships and linked artifacts are requested separately where the platform stores them apart.

Reference: NI04; EA01; IT01

NI04 EA01 IT01

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

D27 HR payroll and offboarding

Possible information
Employment dates, role/device assignments, access change requests, separation and reimbursement records.

Ask the owner
Which relevant dates, devices, accounts and policy acknowledgments can be supplied lawfully?

Likely contact
HR, payroll, IT and legal

Details to confirm
Keep personnel and unrelated personal data restricted. Offboarding can trigger deletion, token changes or wiping, so coordinate preservation with the legal and security teams ahead of those steps.

Reference: LG01; NI04

LG01 NI04

D28 Legal practice management

Possible information
Matter metadata, documents, notes, billing, trust/accounting entries, communications, tasks and portals where used.

Ask the owner
Which modules, linked storage, client portal and separate exports are relevant?

Likely contact
Firm administrator, legal operations and provider

Details to confirm
Clio matter list export contains matter form data, and the examiner exports the other subtabs as the matter calls for.

Reference: CL01; CL02

CL01 CL02

D29 EHR or EMR clinical record

Possible information
Visits, notes, orders, results, medication records, amendments, addenda and signed/unsigned status as stored.

Ask the owner
Which systems, patient/encounter IDs, modules, authors, date types and export formats hold the relevant episodes?

Likely contact
Health information management and clinical application owner

Details to confirm
Candidate clinical locations are confirmed with the vendor and site. Audit data, versions, attachments and departmental systems are requested alongside the printed chart.

Reference: HE01; HE03; HE06

HE01 HE03 HE06

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

D30 Clinical audit and provenance

Possible information
Audit events, accesses, amendments, signatures, proxy activity and emergency overrides if recorded.

Ask the owner
Which events/fields, identifiers, clock settings, retention and reports exist? Ask for a legend and known gaps.

Likely contact
Clinical security/application owner and vendor

Details to confirm
Certification guidance describes capabilities, and the examiner confirms the site's actual configuration and retention.

Reference: HE01 164.312(b); HE06

HE01 HE06

D31 Imaging laboratory and pharmacy

Possible information
PACS/RIS images/reports, laboratory/pathology systems, medication and administration records if used.

Ask the owner
Which separate systems, identifiers, original files, result revisions and interfaces relate to the episode?

Likely contact
Radiology, laboratory, pharmacy and department IT

Details to confirm
Candidate categories, each confirmed with its department owner.

Reference: HE01; NI04

HE01 NI04

D32 Patient portals exchanges and telehealth

Possible information
Portal messages, upload/download records, referrals, health information exchange traffic and telehealth artifacts where retained.

Ask the owner
Which platform, patient/account IDs, sending/receiving organizations and interface messages are relevant?

Likely contact
Portal/HIE/telehealth owner and privacy lead

Details to confirm
The examiner interprets proxy account activity and imported records against the portal's account and interface records.

Reference: HE01; HE03; HE06

HE01 HE03 HE06

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

D33 Practice management billing and claims

Possible information
Scheduling, check in, referrals, coding, authorizations, claims/remittances and adjustments if used.

Ask the owner
Which clinical/financial IDs join the records and what does the billing export omit?

Likely contact
Practice administrator, billing and payer/clearinghouse contact

Details to confirm
The examiner reconciles billing, clinical and legal records, reading each in its own terms.

Reference: HE01; HE03; NI04

HE01 HE03 NI04

D34 Facilities and physical systems

Possible information
Badge/visitor events, CCTV, building controls and vehicle/location records if operated and retained.

Ask the owner
Which camera/door/location IDs, overwrite times, clocks and system owners relate to the matter?

Likely contact
Facilities, security, fleet and legal

Details to confirm
Candidate categories. Confirm privacy/authority and preserve time context; tying a badge event to the person who entered combines it with camera footage, schedules and other corroboration.

Reference: NI04; LG01

NI04 LG01

D35 Third parties insurers and outside professionals

Possible information
Vendors, brokers, advisers, counterparties, outsourced IT and external archives may hold distinct records.

Ask the owner
Who owns or controls each copy and what request/consent/order or contract right is needed?

Likely contact
Counsel, business owner and provider

Details to confirm
Counsel sets the authority for each third party request, by consent, contract right, subpoena or order, and coordinates lawful requests and restrictions.

Reference: LG01 Rules 34 and 45; HE03

LG01 HE03

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

D36 Automations AI tools and integration copies

Possible information
Prompts/outputs, connected data, workflow histories, generated summaries and intermediate files where actually retained.

Ask the owner
Which tools were actually used, with which organization/personal accounts, connectors and retention settings?

Likely contact
Application owner, users and provider

Details to confirm
Candidate category. Preserve provenance and verify the actual feature and export coverage.

Reference: MS01; GO01; NI04

MS01 GO01 NI04

Bring the completed pack to a free scoping call and a senior examiner sets the scope from it. Call (800) 868-8189.

Source review date: October 18 2026.

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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