Read-only exports from tools you already run.

Your administrators export records and send us the encrypted files. We join them into one map of who delegated what to which agent, and what each agent then did. **A record that is missing, kept too briefly or editable is a finding, and so is a source you don't have.**

HOW IT WORKS

1 Kickoff, one hour.
We agree which systems are in scope, how files are sent, and who sends what.

2 Send the start set.
Nine items to get the review started.

3 Send the rest.
Eight required items, plus any optional ones you have.

THE LIST

1 Send first (9)

Gets the review started.

- D1.1 Users, groups, admin roles and last sign-in
- D1.2 Leavers, with exact cut-off times
- D2.1 Connected apps, their scopes and consents
- D2.4 AI platform accounts and key IDs (never keys)
- D3.2 App and token sign-ins acting for people
- D4.2 Audit log for your main productivity suite
- D5.1 Short list of your crown-jewel systems
- D6.1 Logging and retention settings
- D7.3 Our 20-minute questionnaire

2 Send next (8)

Per system in scope.

- D2.2 Service accounts, workload IDs and cloud keys
- D2.3 Developer tokens, bots and CI runners
- D2.5 Agents built in business platforms, and their tools
- D2.7 AI tools on employee computers
- D3.1 Role-assumption and impersonation events
- D3.3 Role trust and organization policies
- D4.1 Cloud audit logs, with crown-jewel data events
- D6.3 Limits on agents: rate limits, approvals, token lifetimes

3 If you have it (8)

Sharpens the map, not needed to start.

- D1.3 Role and group changes
- D2.6 Secrets inventory, names only
- D4.3 Access history for sensitive data stores
- D4.4 Agent run traces, the only direct view of sub-agents
- D5.2 Data labels and data-loss alerts
- D6.2 Detection rules and token or key incidents
- D7.1 Network traffic to AI services
- D7.2 AI subscriptions bought outside procurement

BEFORE YOU SEND

Never send secrets

No passwords, API keys, tokens or connection strings. We need each credential's name, owner, scopes and last use. Remove any column holding a secret value.

Leave out content

We need who acted, when and on what, never the content itself. Drop prompts, message bodies and file contents. If anything is CUI or export-controlled, we can work inside your GCC High or GovCloud tenant instead, and only the report leaves.

Keep the IDs that link records

We join records on user principal names, app and client IDs, and role names. To pseudonymize people, use one keyed hash (HMAC) across every export.

THE DETAILS

Scope.

One identity tenant (Entra ID, Okta or Google Workspace) plus the connected systems you pick at kickoff. Commercial, GCC High and GovCloud tenants count separately. HR, device and network inputs don't count as systems.

Window and format.

The last 90 days for every source, 30 at minimum. CSV or JSON as the system exports it, or a time-limited read-only audit role agreed at kickoff.

Transfer and deletion.

We agree the channel and encryption at kickoff. We delete everything at the end and confirm it in writing.