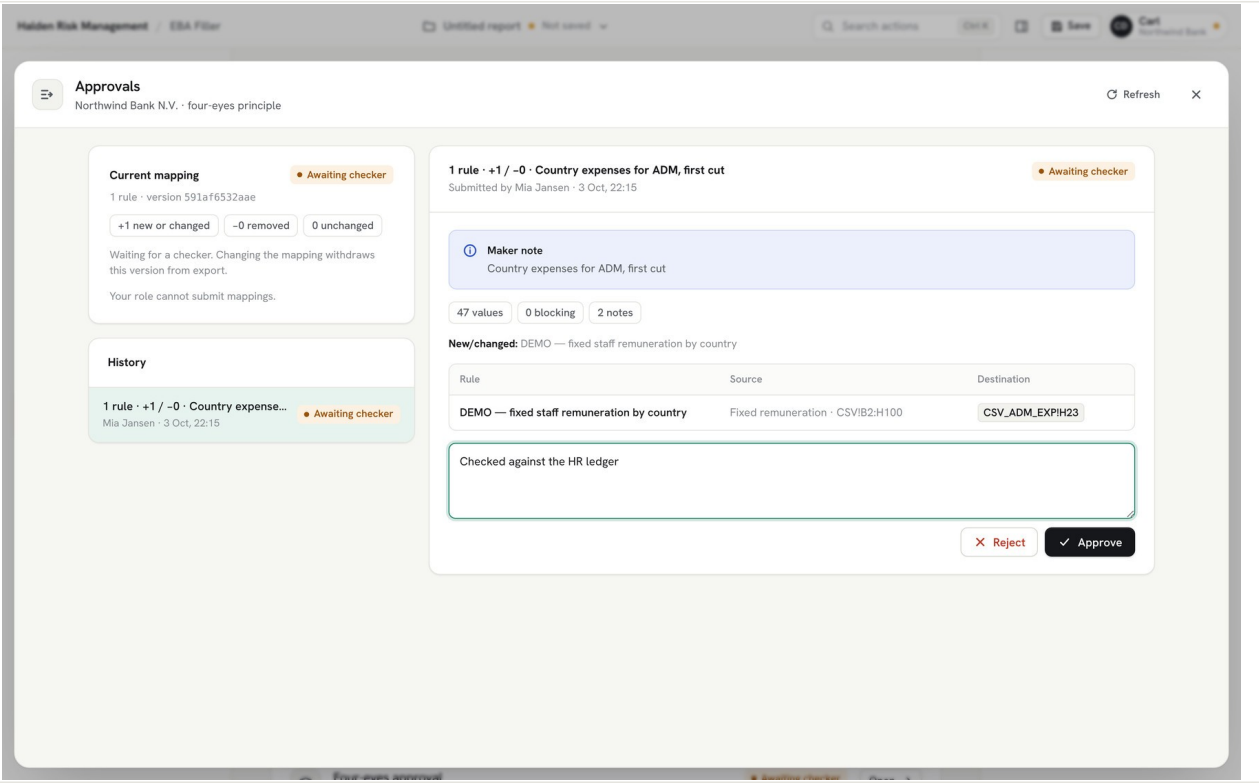


# EBA Filler

## IT & Security Pack

Architecture, data handling, identity, network, deployment and regulatory information for due diligence and rollout.



| VERSION | DATE         | APPLIES TO                                             | AUDIENCE                                       |
|---------|--------------|--------------------------------------------------------|------------------------------------------------|
| 0.9.0   | October 2026 | Halden EBA Filler<br>desktop app and<br>premium server | IT, information security,<br>outsourcing, DORA |

Independent software; not an official EBA product. Screenshots show fictitious example data.

# Contents

---

- Summary for IT and security teams..... 3
- 1 Architecture..... 4
- 2 Deployment options..... 5
- 3 Data handling..... 5
- 4 The AI assistant and your data..... 6
- 5 Identity and access..... 7
- 6 Cryptography and secrets..... 8
- 7 Logging, audit and monitoring..... 8
- 8 Network and firewall..... 9
- 9 Desktop rollout..... 9
- 10 Server operations..... 10
- 11 Resilience and continuity..... 10
- 12 Secure development and vulnerability management..... 10
- 13 Subprocessors..... 11
- 14 Regulatory support..... 11
- 15 Exit and data deletion..... 12
- 16 Certifications..... 12
- 17 Contacts..... 13

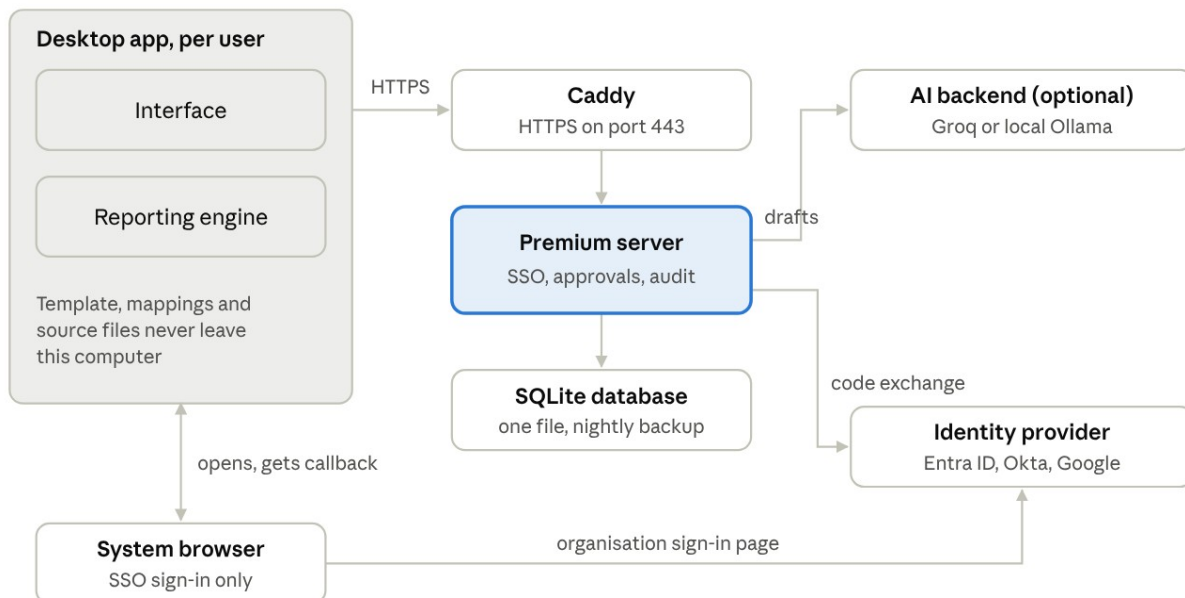
# Summary for IT and security teams

Halden EBA Filler is a desktop application that fills the EBA 2027 EU-wide stress test template from a bank's own Excel and CSV files. Report data is processed on the user's computer and is never sent to Halden. A small premium server adds sign-in, four-eyes approval, run records and a hash-chained audit log; it stores metadata about the work, not the figures.

| Question                            | Short answer                                                                                                                                                                        |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Where are report figures processed? | Only on the user's computer. Templates, source files and exported workbooks are read and written locally.                                                                           |
| What goes to the server?            | User accounts, roles, project names, rule definitions (no cell values), validation counts, file hashes and audit events.                                                            |
| Can it run without any server?      | Yes. Local mode needs no account and makes no network calls.                                                                                                                        |
| Who hosts the server?               | Your choice: Halden Cloud (EU), your own cloud subscription, or on-premise. Same software in each.                                                                                  |
| How do users sign in?               | Single sign-on with your identity provider (OpenID Connect), or e-mail and password. Roles can follow your identity-provider groups, and accounts can be provisioned with SCIM 2.0. |
| Is there AI, and is it optional?    | An optional assistant drafts mapping rules from a user-approved sample of at most 200 cells. It can be switched off, or run on a local model with no outbound calls.                |
| Network needs                       | Desktop to server: HTTPS (443). Nothing inbound to desktops.                                                                                                                        |
| Admin rights for installation?      | No. The Windows installer installs per user; no Python or other runtime is needed.                                                                                                  |
| Evidence for audits                 | Hash-chained audit log export (CSV / JSON Lines), periodic access review with sign-off, complete organisation export and a deletion receipt at exit.                                |

# 1 Architecture

Report data stays on the desktop; the server keeps the team record



**Figure 1** Deployment architecture: report data stays on the desktop; the server keeps the team record

| Component             | Technology                                                                                      | Runs where                                        | Holds                                                                                                         |
|-----------------------|-------------------------------------------------------------------------------------------------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Desktop app           | Electron 44 interface with a bundled reporting engine (Python, packaged as a native executable) | User's computer (Windows 10/11, macOS 12+, Linux) | Nothing persistent outside the user's own project and mapping files; session token in the OS credential vault |
| Premium server        | Python service, single process, SQLite database                                                 | Halden Cloud (EU), your cloud, or on-premise      | Accounts, roles, projects, reviews, runs, audit log, licenses, SSO and SCIM configuration, security policy    |
| TLS front end         | Caddy (bundled) or your reverse proxy / load balancer                                           | In front of the server                            | TLS certificates                                                                                              |
| Identity provider     | Your OpenID Connect provider (Entra ID, Okta, Google Workspace, Keycloak, ADFS 2019+)           | Yours                                             | Users' credentials and MFA                                                                                    |
| AI backend (optional) | Groq Cloud API, or a local Ollama model                                                         | Third party, or inside your network               | Nothing retained by Halden; see section 4                                                                     |

The desktop app talks to the server over HTTPS for sign-in, approvals, runs and the audit log. For single sign-on, the system browser visits your identity provider and returns a one-time code to the app on 127.0.0.1. Only the server calls the AI backend.

## 2 Deployment options

|                    | Halden Cloud (EU)                                               | Your cloud                                        | On-premise                                |
|--------------------|-----------------------------------------------------------------|---------------------------------------------------|-------------------------------------------|
| Server operated by | Halden                                                          | You (or Halden under contract)                    | You                                       |
| Location           | EU data centre <b>[TO CONFIRM: hosting provider and region]</b> | Your subscription and region                      | Your data centre                          |
| Tenancy            | Dedicated server instance per institution                       | Yours                                             | Yours                                     |
| Updates            | Managed by Halden                                               | You apply releases                                | You apply releases                        |
| AI assistant       | Groq Cloud or a Halden-hosted local model <b>[TO CONFIRM]</b>   | Groq, local Ollama, or off                        | Local Ollama or off; air-gapped supported |
| Encryption at rest | <b>[TO CONFIRM: volume encryption on the hosting platform]</b>  | Your platform's disk/volume encryption, your keys | Your disk encryption                      |

The desktop app is the same in every option; IT points it at the chosen server with a configuration file (section 9). Air-gapped installations run the server on-premise with the AI assistant switched off or on a local model, and issue licenses offline.

## 3 Data handling

**Report data never leaves the desktop.** The table lists every category of data, where it is stored, and whether it reaches the server.

| Data               | Example                                             | Stored                         | Sent to server                                                      |
|--------------------|-----------------------------------------------------|--------------------------------|---------------------------------------------------------------------|
| EBA template       | 2027 draft templates workbook                       | User's computer (read only)    | No; only its SHA-256 hash                                           |
| Source files       | Loan tapes, ledger extracts                         | User's computer (read only)    | No; only file names as source labels and SHA-256 hashes             |
| Exported workbook  | Filled template                                     | User's computer                | No; only its SHA-256 hash                                           |
| Mapping rules      | Rule name, operation, sheet and cell ranges, factor | Local JSON and project files   | Yes, when submitted for approval (definitions only, no cell values) |
| Project metadata   | Project name, institution, reference date           | Local project file             | Yes, for team projects                                              |
| Validation results | Counts of values, errors, warnings; tab names       | Local                          | Yes, as run records                                                 |
| Audit JSON         | Old and new cell values with hashes                 | Local, where the user saves it | No                                                                  |

| Data          | Example                                       | Stored                | Sent to server                                                                                 |
|---------------|-----------------------------------------------|-----------------------|------------------------------------------------------------------------------------------------|
| User accounts | Name, work e-mail, roles                      | Server                | Yes                                                                                            |
| Audit events  | Who did what, when, on which object           | Server                | Yes                                                                                            |
| AI evidence   | At most 200 source cells plus template labels | Not stored by the app | Yes, only after the user previews it and ticks consent; forwarded to the configured AI backend |

**Personal data.** The server processes users' names, work e-mail addresses, roles, sign-in times and actions (audit events). It does not log IP addresses, request bodies, passwords or tokens. Report data may contain personal data (for example in loan tapes); it stays on the desktop.

**Retention.** Sessions expire after 12 hours by default (an administrator can set 1–24 hours and an inactivity sign-out). Accounts, reviews, runs and audit events are kept until the organisation deletes them or the contract ends; expired SSO transactions and one-time codes are purged automatically.

[TO CONFIRM: contractual retention period for Halden Cloud]

## 4 The AI assistant and your data

The AI assistant is optional and only drafts rules; it never writes to a template.

1. A user selects one source range (max. 200 cells, 20 columns) and a template area, and writes an instruction.
2. The app shows the exact JSON that would be sent. Nothing is sent until the user ticks the consent box.
3. The server checks the license (10 drafts per hour per organisation, at most 2 at a time), forwards the evidence to the configured backend and logs the request in the audit trail.
4. Proposals come back as draft rules; each passes the same technical checks as a manual rule and is only added when the user accepts it. With a team account it still needs four-eyes approval.

| Backend            | Where data goes                    | Choose when                                                                       |
|--------------------|------------------------------------|-----------------------------------------------------------------------------------|
| Off                | Nowhere                            | Policy does not allow AI, or mapping is done by hand                              |
| Local Ollama model | A server inside your network       | No data may leave your network                                                    |
| Groq Cloud         | Groq's API (third-party processor) | The bank accepts that user-approved evidence is processed by Groq under its terms |

Halden does not use customer data to train models. Whether a third-party backend retains or trains on API data is governed by that provider's terms; banks that need certainty use the local model.

## 5 Identity and access

- **Single sign-on** with any OpenID Connect provider (Microsoft Entra ID, Okta, Google Workspace, Keycloak, Ping, ADFS 2016+, OneLogin, Auth0). The sign-in runs in the system browser (RFC 8252), never in an embedded window, so your provider's MFA and conditional access apply unchanged.
- **Flow security.** PKCE on both legs, a one-time code (60 seconds) delivered only to a loopback listener on 127.0.0.1, state and nonce checks, and ID-token validation: the signature is verified against the provider's published signing keys (JWKS; RS256/384/512 and ES256/384, or HS256 with the client secret), then issuer, audience, expiry, issued-at and nonce. Unsigned tokens and other algorithms are refused; rotated provider keys are picked up automatically. The client secret stays on the server and can be read from an environment variable.
- **Roles from your identity provider.** Map groups (or app roles) in the ID token to Halden roles, for example `Halden-Checkers = checker`. Roles are synchronised at every sign-in; a user in none of the mapped groups is refused. The last administrator always keeps the admin role, so an organisation cannot lock itself out.
- **Provisioning (SCIM 2.0).** Entra ID, Okta and other providers create, rename, deactivate and reactivate accounts through `/scim/v2/Users`, with a per-organisation bearer token (stored as a SHA-256 digest; revocable). Deactivation ends all sessions immediately. A SCIM delete deactivates the account so the audit trail keeps its meaning; organisation data is erased at exit (section 15). Groups are not provisioned; roles come from the `roles` attribute, a default role or the group mapping.
- **E-mail and password** as an alternative or fallback: PBKDF2-HMAC-SHA256 with 240,000 iterations and a per-user salt; minimum 12 characters with mixed case and a digit; lockout for 15 minutes after 5 failed attempts. Password sign-in can be switched off for everyone except administrators, who keep a break-glass password.
- **Sessions** last 12 hours by default; administrators set 1–24 hours and an optional sign-out after 5–480 minutes of inactivity. The token is stored on the desktop in the OS credential vault (Windows Credential Manager, macOS Keychain) and on the server only as a SHA-256 digest. Sign-out, deactivation, password resets and "Sign out everywhere" end sessions immediately.
- **Roles** per organisation: maker, checker, admin, viewer. No one can approve their own submission. Exports of team projects require an approved mapping version unless an administrator switches that control off (recorded in the audit log).
- **Administration in the app.** Administrators manage users, single sign-on (with a live configuration check), SCIM tokens, the session policy and the access review under *Account* → *Organisation settings*; every change is audited with old and new values.
- **Access review.** The access review lists every account with roles, source (manual, SSO or SCIM), last sign-in and method, and flags dormant accounts (no sign-in for 90 days), accounts that never signed in, maker-and-checker combinations and password access alongside SSO. An administrator records the review with a note; the audit event carries a fingerprint of the reviewed list, and recording is refused if users or roles changed in the meantime.
- **Not available:** SAML 2.0. Every provider listed above also offers OpenID Connect, which Halden uses instead.

## 6 Cryptography and secrets

| Item                            | Protection                                                                                                                          |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Data in transit                 | TLS 1.2 or higher at the HTTPS front end (Caddy defaults: TLS 1.2/1.3, HSTS); remote servers over plain HTTP are refused by the app |
| Passwords                       | PBKDF2-HMAC-SHA256, 240,000 iterations, 16-byte random salt                                                                         |
| Session tokens and license keys | 256-bit random values; only SHA-256 digests stored                                                                                  |
| SSO client secret               | Environment variable (env: reference) or database field; never sent to desktops                                                     |
| ID tokens                       | Signature verified against the provider's JWKS (RS256/384/512, ES256/384) or HS256; RSA keys under 2048 bits refused                |
| SCIM tokens                     | 256-bit random values; only SHA-256 digests stored; revocable per token                                                             |
| Database at rest                | SQLite file with mode 600, owned by an unprivileged service user; encrypt the volume with your platform (recommended)               |
| Desktop credentials             | OS credential vault                                                                                                                 |
| Integrity                       | SHA-256 for templates, sources, outputs, mapping versions and the audit chain                                                       |

## 7 Logging, audit and monitoring

Every state-changing action writes an audit event whose hash includes the previous event's hash, per organisation. Editing, inserting or deleting any event breaks the chain; `audit-verify` and the app's *Chain verified* badge recompute it.

Events include sign-in (with method), failed sign-in, sign-out after inactivity, user changes (with who made them: an administrator, SSO group synchronisation or SCIM), SSO and SCIM configuration, security-policy changes with old and new values, access reviews, project creation, submission, approval, rejection, withdrawal, validation runs, exports, data exports and AI draft requests.

**Export for auditors and SIEM.** Administrators export the full log as CSV or JSON Lines from the app (*Organisation settings* → *Audit & data export*) or the API (`GET /v1/audit/export?since=<seq>`). Every exported event carries its sequence number, previous hash and own hash, so a third party can verify the chain from the export alone. For continuous shipping, schedule `halden-admin audit-export --org ... --format jsonl --out /var/log/halden/audit.jsonl --state /var/lib/halden/audit.seq`; each run appends only events after the last exported sequence number, ready for your SIEM forwarder.

Health monitoring: `GET /v1/health` returns `{"ok": true, "version": "..."}`  and checks the database. Service logs contain start-up and error information only.

## 8 Network and firewall

| From              | To                | Port                   | Purpose                                               | Required                           |
|-------------------|-------------------|------------------------|-------------------------------------------------------|------------------------------------|
| Desktop           | Halden server     | 443/TCP                | API: sign-in, approvals, runs, audit                  | Team features only                 |
| Desktop (browser) | Identity provider | 443/TCP                | SSO sign-in page                                      | SSO only                           |
| Desktop (browser) | Halden server     | 443/TCP                | SSO start and callback pages                          | SSO only                           |
| Browser           | Desktop app       | 127.0.0.1, random port | One-time SSO callback (loopback only)                 | SSO only                           |
| Server            | Identity provider | 443/TCP                | OIDC discovery, signing keys (JWKS) and code exchange | SSO only                           |
| Identity provider | Halden server     | 443/TCP                | SCIM provisioning (/scim/v2)                          | SCIM only                          |
| Server            | api.groq.com      | 443/TCP                | AI drafts                                             | Groq backend only                  |
| Server            | Let's Encrypt     | 80, 443/TCP            | Certificate issuance                                  | Bundled Caddy with public DNS only |

No inbound connections to desktops are needed. The API refuses browser requests that carry an `Origin` header, so it cannot be called from web pages. SCIM requests from cloud identity providers arrive from the provider's published IP ranges; allow those, or skip SCIM and use group mapping at sign-in.

## 9 Desktop rollout

- **Installers:** Windows NSIS installer (per user, silent with /S), macOS DMG, Linux Applmage. The reporting engine is bundled; no Python is required. **[TO CONFIRM: code-signing certificate and notarisation status]**
- **Server address** is set centrally, so users never type it. Deploy a configuration file with Intune, Group Policy or your MDM:

```
{ "server": "https://halden.yourbank.eu", "lock_server": true }
```

| Platform | Location                                                   |
|----------|------------------------------------------------------------|
| Windows  | %ProgramData%\Halden\EBA Filler\config.json                |
| macOS    | /Library/Application Support/Halden/EBA Filler/config.json |
| Linux    | /etc/halden/eba-filler.json                                |

- **Local files:** settings in the user profile; projects, mappings and outputs wherever the user saves them. The app never modifies the template or source files.
- **Updates:** new versions are installed over the old one; settings and projects are kept. **[TO CONFIRM: automatic update channel]**

## 10 Server operations

| Topic        | Detail                                                                                                                                         |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Sizing       | 1 vCPU, 1 GB RAM, 10 GB disk serves a typical bank team                                                                                        |
| Installation | Docker Compose (server + Caddy) or a hardened systemd service; see the server guide                                                            |
| Hardening    | Read-only container, unprivileged user, no new privileges; systemd ProtectSystem=strict, private /tmp, write access only to the data directory |
| Backups      | Online, consistent <code>backup</code> command; nightly script with retention included                                                         |
| Restore      | Copy a backup over the database file and restart; <code>audit-verify</code> confirms integrity                                                 |
| Upgrades     | Back up, deploy the new release, restart; the schema upgrades itself and never removes data                                                    |
| Scale        | One instance per deployment (SQLite), sized for a bank's reporting and validation teams                                                        |

## 11 Resilience and continuity

- **Server unavailable:** users keep working in local mode, including validation and export, unless the organisation requires an approved mapping before export; in that case export waits until the server is back.
- **Recovery objectives:** with nightly backups, recovery point 24 hours; recovery time is the time to restore one file and restart (minutes). **[TO CONFIRM: contractual RPO/RTO for Halden Cloud]**
- **No lock-in of report data:** templates, sources, mappings and outputs are ordinary files on your systems.

## 12 Secure development and vulnerability management

- 58 automated tests cover the reporting engine, the app bridge, accounts, approvals, the audit chain and single sign-on (including tampered ID tokens and stolen codes).

- Small dependency footprint on the server: Python standard library plus openpyxl, lxml and keyring.
- Penetration tests: [TO CONFIRM: cadence and last test date]; summaries shared under NDA.
- Vulnerability reports: [TO CONFIRM: security contact address]. We acknowledge reports within [TO CONFIRM] working days.

## 13 Subprocessors

| Subprocessor                   | Service                 | Data                                    | When                                |
|--------------------------------|-------------------------|-----------------------------------------|-------------------------------------|
| [TO CONFIRM: hosting provider] | Hosting of Halden Cloud | Server data (section 3)                 | Halden Cloud only                   |
| Groq, Inc.                     | AI drafts               | User-approved evidence (max. 200 cells) | Only if the Groq backend is enabled |

Self-hosted deployments use no Halden subprocessors.

## 14 Regulatory support

**DORA register of information.** Input for your register, per deployment:

| Field                          | Halden EBA Filler                                                                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| ICT service                    | Software for preparing EBA stress test submissions; optional hosted collaboration server                                                    |
| Function supported             | Supervisory reporting (stress test)                                                                                                         |
| Data processed by the provider | Account and audit metadata (Halden Cloud only); no report figures                                                                           |
| Data location                  | EU (Halden Cloud) or customer-controlled                                                                                                    |
| Subcontractors                 | See section 13                                                                                                                              |
| Substitutability               | High: outputs are standard Excel files; mappings are open JSON                                                                              |
| Exit                           | Complete organisation export (JSON) from the app or org-export, deletion with receipt (org-delete); desktop data is already on your systems |

**Controls that support DORA and the EBA Guidelines on ICT and security risk management.**

| Requirement area                                        | How Halden supports it                                                                                       |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Access management: least privilege, joiners and leavers | Roles per organisation, roles from identity-provider groups, SCIM deactivation, immediate session revocation |

| Requirement area                   | How Halden supports it                                                                                             |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Periodic review of access rights   | Access review with flags, CSV export and an audited sign-off bound to a fingerprint of the reviewed list           |
| Strong authentication              | SSO through your provider's MFA and conditional access; password sign-in can be switched off                       |
| Logging and detection              | Hash-chained audit log, incremental export to your SIEM, integrity check (audit-verify)                            |
| Segregation of duties              | Four-eyes approval bound to the exact mapping version; maker-and-checker combinations flagged in the access review |
| Exit strategy and data portability | Organisation export, open mapping JSON, standard Excel outputs, deletion receipt                                   |

**EBA outsourcing guidelines.** Audit, access and termination rights are set out in the contract. **[TO CONFIRM: contract clause references]**

**GDPR.** For Halden Cloud, Halden acts as processor for account and audit data under a data processing agreement; for self-hosted deployments the bank is sole controller and Halden processes no personal data.

## 15 Exit and data deletion

1. Export the organisation's data: an administrator uses *Organisation settings* → *Audit & data export* → *Export organisation data* (one JSON file with users, team projects, approvals with their rule lists, runs, the audit log with its chain and the SSO settings, without secrets or password hashes), or the server administrator runs `halden-admin org-export --org ... --out export.json`.
2. Delete it from the server: `halden-admin org-delete --org ... --confirm "<organisation name>"` removes every record of the organisation (users, sessions, projects, reviews, runs, audit events, SSO and SCIM settings), revokes its licenses, compacts the database and prints a deletion receipt with counts and a timestamp. Backups taken earlier still contain the data until they expire under your backup retention.
3. Uninstall the desktop app; projects, mappings and outputs remain the bank's files.
4. For Halden Cloud, Halden performs steps 1–2, deletes the instance and its backups within **[TO CONFIRM]** days and confirms in writing with the deletion receipt.

## 16 Certifications

| Standard      | Status              |
|---------------|---------------------|
| ISO/IEC 27001 | <b>[TO CONFIRM]</b> |

| Standard                           | Status                 |
|------------------------------------|------------------------|
| SOC 2 Type II                      | [TO CONFIRM]           |
| GDPR data processing agreement     | Available              |
| DORA register-of-information input | Available (section 14) |
| EBA outsourcing contract terms     | Available              |

## 17 Contacts

| Topic                          | Contact                                |
|--------------------------------|----------------------------------------|
| Sales and contracts            | [TO CONFIRM: sales e-mail]             |
| Security questions and reports | [TO CONFIRM: security e-mail]          |
| Support                        | [TO CONFIRM: support e-mail and hours] |

Related documents: the User Guide, the Methodology and the server installation guide (SERVER.md).