

# Quarterly access review — Q3 2026

|         |                              |
|---------|------------------------------|
| doc id  | RECORD-ACCESS-REVIEW-Q3-2026 |
| version | 2 (closed 2026-09-09)        |
| status  | record                       |
| owner   | Olaf Jacobson                |

**Reviewed 2026-09-09 by Olaf Jacobson (Information Security Manager).** First review under ISMS-DOC-A05-18-1. Access enumerated directly from the AWS IAM and GitHub APIs rather than from a maintained list, so this is the actual state, not the intended one.

## 1. GitHub — organisation SoonHQ

| Member                             | Role before | Decision                                                     | Role after                                 |
|------------------------------------|-------------|--------------------------------------------------------------|--------------------------------------------|
| OlafJacobson                       | admin       | Keep — CEO / ISM                                             | admin                                      |
| picaulegend (Thomas Picauly)       | member      | <b>Promoted</b> — CTO had less access than his role requires | <b>admin (owner), confirmed 2026-09-09</b> |
| A13SSANDRO (Alessandro Cardinali)  | admin       | Keep — CPO                                                   | admin                                      |
| Melv (Melvin Jacobson)             | admin       | <b>Keep — see §4, break-glass</b>                            | admin                                      |
| CybearSquad (outside collaborator) | —           | Keep — external ISMS consultant                              | outside collaborator                       |

Two-factor authentication is enforced organisation-wide (2026-09-08) and **no member or outside collaborator lacks it**.

## 2. AWS — IAM Identity Center

Permission sets: `SoonDevDatabaseAccess`, `SoonInfraPlan`, `SoonInfraApply`, `PowerUserAccess`.  
Identities: Olaf, Thomas, Melvin (plus two `+udev2` test identities — **action: confirm whether these are still needed**).

## 3. AWS — legacy IAM users

| User       | Console | MFA | Privilege                       | Decision                                 |
|------------|---------|-----|---------------------------------|------------------------------------------|
| Olaf       | yes     | 1   | Admins (AdministratorAccess)    | Keep                                     |
| Thomas     | yes     | 0   | Admins (AdministratorAccess)    | <b>Enable MFA immediately</b> — see §5   |
| Alessandro | yes     | 1   | Billing, evidence-capture       | Keep                                     |
| Melvin     | yes     | 2   | Admins (AdministratorAccess)    | Keep as break-glass — §4                 |
| SoonDev0   | yes     | 0   | SoonDevs (AWSLambda_FullAccess) | <b>Shared account — open, §6</b>         |
| Auditor    | no      | 0   | ReadOnlyUsers                   | <b>Identify owner and purpose — open</b> |

## 4. Melvin Jacobson — deliberate retention

Melvin holds no operating role (ISMS-DOC-05-2 v0.3). His administrative access is **retained deliberately** as a break-glass measure: he is a founder and shareholder, has the technical background, is already vetted, and is the continuity plan if Olaf or Thomas becomes unavailable. Retaining him materially improves the bus factor for a company whose production estate is otherwise administered by two people.

This is an accepted risk, not an oversight. Conditions attached:

- Access is for **emergency continuity**, not routine work.
- MFA is present (2 devices) and must remain.
- **His long-lived access key (created 2018-04-24, 3,060 days old) was removed on 2026-09-09** — deactivated, verified, then deleted. A continuity account does not need programmatic credentials, and it was the oldest credential in the estate. Console access, both MFA devices and Admins membership are intact, so break-glass still works.
- Reviewed again next quarter.

## 5. Findings

| # | Finding                                                                                                                                                                                          | Severity | Owner  | Status                                                                                                     |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|--------|------------------------------------------------------------------------------------------------------------|
| 1 | <b>Thomas holds AdministratorAccess with console login and no MFA device.</b> Contradicts the Access Control Policy and the published DPA (Annex II: "protected by multi-factor authentication") | High     | Thomas | Open — steps issued 2026-09-09                                                                             |
| 2 | Thomas was member on GitHub while less operationally involved people were admins                                                                                                                 | Medium   | Olaf   | <b>Closed</b> — promoted to organisation owner 2026-09-09                                                  |
| 3 | SoonDev0 shared account: console login, no MFA, AWSLambda_FullAccess                                                                                                                             | High     | Thomas | Open                                                                                                       |
| 4 | Unused access key on SoonDev0 (created 2022-08-28, <b>never used</b> )                                                                                                                           | Medium   | Olaf   | <b>Closed</b> — deactivated and deleted 2026-09-09                                                         |
| 5 | Long-lived access keys: serverless (3,068d), SES-Key (3,052d), Terraform-Cloud (1,673d), Thomas (1,689d and 467d)                                                                                | Medium   | Thomas | Open — rotate those in use. <b>Melvin's 3,060d key removed 2026-09-09</b>                                  |
| 6 | eb-deployer key last used against Elastic Beanstalk; the platform runs on ECS                                                                                                                    | Low      | Thomas | Open — likely removable                                                                                    |
| 7 | Auditor IAM user with an active key that accessed RDS; owner and purpose unrecorded                                                                                                              | Medium   | Olaf   | <b>Key deactivated 2026-09-09</b> , user retained so it is reversible. Purpose still unidentified — see §8 |
| 8 | Two +udev2 Identity Center identities of unclear purpose                                                                                                                                         | Low      | Thomas | Open                                                                                                       |

## 6. Actions taken during this review

All on 2026-09-09, each deactivated and verified before deletion where deletion applied:

- **Thomas promoted** to GitHub organisation owner.
- **SoonDev0 key AKIA2Z42KZFEWR4XNP70 deleted** — created 2022-08-28, never used in 1,472 days.
- **Melvin key AKIAJEASGVJXX5PETSQ deleted** — created 2018-04-24, the oldest credential in the estate. Console access and MFA retained (break-glass, §4).
- **Auditor key AKIA2Z42KZFEYGN3ZJXL deactivated**, not deleted, so it can be restored in one command if its purpose surfaces.
- **Andrea Cardinali (CybearSquad) downgraded from write to read on isms**. An independent internal auditor should not hold write access to the evidence and policy repository; read is sufficient to review, and anything she authors can come through a pull request.

## 7. GitHub collaborator sweep — all 88 repositories

---

Every SoonHQ repository was enumerated and checked for outside collaborators and pending invitations. **Andrea Cardinali is the only outside collaborator, on isms alone.** No pending invitations anywhere.

**A false positive worth recording.** An initial pass appeared to show Andrea with read access to `WebexSoon`, `MarsTime`, `onboarding-agent` and `soon-claude-plugin`. She does not have it. Those four repositories are **public**, and GitHub's permission endpoint returns `read` for *any* user on a public repository — a control test with two unrelated GitHub accounts returned the same result. The authoritative collaborator check confirms she is an explicit collaborator on `isms` only. Method note for the next review: use the collaborator membership endpoint, not the permission endpoint, on public repositories.

Separately noted for classification review rather than access: those four repositories are public. The owner confirmed `onboarding-agent` is harmless and may be linked from the website. Whether each is deliberately public is an A.5.12 question, not an access one.

## 8. Still open after this review

---

## 9. Next review

---

**Thomas has AdministratorAccess with console login and no MFA device** (finding 1). This is the one finding that leaves the review open. It contradicts the Access Control Policy and the published Data Processing Agreement, which states that production access is protected by multi-factor authentication. Two acceptable resolutions: enrol an MFA device, or delete the console login profile on the legacy IAM user if he works through IAM Identity Center, where he already has an identity. The second is preferable — it removes a standing route to administrator rather than protecting one.

Also open: the `SoonDev0` shared account (console, no MFA, `AWSLambda_FullAccess`); the purpose of `Auditor`; two `+udev2` Identity Center identities; and rotation of the four remaining long-lived keys in use.

## 9. Next review

---

Q4 2026. The carry-over is the register of long-lived access keys in §5: the target is that no human user holds a static access key, with programmatic access moving to IAM roles and short-lived credentials.

---

Rendered from SoonHQ/isms — .../.../private/tmp/claude-501/-Users-olafjacobson-s-isms--claude-worktrees-iso-soc2-evidence-system-3febee/e3e18e8e-8a07-47cd-99b6-574311482138/scratchpad/access-review-q3-2026.md — source SHA-256 9ec657dfa4f5fde02f302ab79e882f0b7bf80188a722defa2eef36533faa7266