Harborline stated control brief: identity lifecycle (current state)

This is **Harborline's current stated control**. It is a source document, not your proposed design. Your design lives on the 2C Control Design tab. This is the version written for SOC 2 binders. Use it in **Build** as the rule the monitor tests.

It is not automatically a good design. Complete **Assess** and **Design** before you treat this as the finished solution. After **Break**, you will say what should change.

The business problem

Access does not fail in policy binders. It fails in the handoff:

HR records a termination. Someone is supposed to disable the identity-provider (IdP) account. Applications that trust that IdP should stop working.

If you only sample a few IT tickets, you will miss leavers who never got a ticket, movers who kept old entitlements, IdP accounts HR does not know, contractors still marked active after the contract ended, and shared mailboxes with no owner.

A monitor is useful because the population is the **full file**, not a sample of five.

Authoritative sources (as stated today)

Question	Trust this file
Is this person employed, terminated, on leave, or contracted?	`employees.csv`
Is the *central IdP* account active, and what entitlements does it have?	`application_access.json`
What may this **current** role have?	`role_catalog.csv`
Was this privileged entitlement approved?	`privileged_approvals.csv`

If HR and the IdP disagree, that disagreement **is** a finding for this monitor. Do not “fix” the CSV to make them match.

Harborline's stated scope is the central IdP export. Your Assess and Design work should ask whether that scope is enough.

Review freeze

All monitor math uses:

`review_as_of` = `2026-08-15T12:00:00Z`

Do not use your laptop’s current time. A control test must be repeatable.

SLA (service level agreement) in this brief is the maximum time the stated control is allowed to take.

Pass / fail / watch (stated rules for the monitor)

Leaver SLA (24 hours) Elapsed time = `review_as_of` minus `termination_date`.

Situation	Classification
Terminated (or contract ended), IdP account still `active`, elapsed **> 24 hours**	**Exception** (`sla_breach`)
Terminated, IdP still `active`, elapsed **≤ 24 hours**	**Watch item** (`open_within_sla`). The control still has time.
Terminated, IdP `disabled`	**True negative** for current IdP access. Not an exception.

Mover SLA (7 days) If `role_change_date` is set and `previous_role_code` is set, any live entitlement **not** in the current role's catalog after 7 days is `mover_excessive_access`.

Privileged access Entitlements in the privileged list (below) on an **active** account require a row in `privileged_approvals.csv` for that `employee_id` + `entitlement` where `expires_on` is empty or ≥ `review_as_of`. Missing approval: `privileged_without_approval`.

Leave of absence `employment_status` = `leave_of_absence` and the person still has a **privileged** entitlement (from the list below) on an active account: `loa_with_privileged_access`. Stated policy is to reduce privileged access while someone is on leave. A person on leave is not a leaver, so no 24-hour clock applies, and an existing approval does not clear this flag.

Orphans IdP `account_type` = `user` and email not in HR: `orphaned_account`.

Non-human `account_type` is `shared` or `service` and `owner_employee_id` is empty: `unowned_nonhuman_account`. A service account with an owner is **not** an exception.

Contractors If `contract_end_date` < `review_as_of` and the IdP account is active: `contractor_past_end_date`, even when `employment_status` is `active`.

Privileged entitlements (monitor list)

- `okta_super_admin`
- `github_admin`
- `ehr_admin`
- `phi_full`
- `netsuite_admin`
- `netsuite_ap_approve`
- `finance_admin`
- `hr_admin`

Birthright in the role catalog does **not** replace the approval ticket.

Severity (for the report)

Severity	Typical use
high	Live privileged access that should already be gone (leaver SLA breach with privilege, unowned admin shared account, orphan with write access)
medium	Leaver SLA breach without extra privilege, mover leftover access, contractor past end, LOA with privilege
low	Process gaps with limited blast radius (document them anyway)

Watch items do not get a fail severity. They get a follow-up date.

Exception vs noise

You will see people who look interesting but should **not** be exceptions: a CFO with `finance_admin` **and** a valid approval; a leaver whose IdP account is already disabled. If you flag those, the control owner will not trust the report.

Why a monitor (spreadsheet or Python)

Spreadsheets can do this for 25 rows. The skill is encoding the **same rules** so that 2,500 rows would not change the logic. Keep it linear: load → classify → compare → SLA → flag → report.

Python is the recommended technical path. It is not required. Spreadsheet is a complete Build path and does not cap your score. See Stage 3 in START_HERE_Learner_Guide.pdf.