GOVERNANCE · RUNBOOK 03

User access review

A repeatable campaign for proving who has access to what, and removing what is no longer justified.

DOCUMENT	VERSION	REVIEW CYCLE
GOV-RB-03	1.0	Annual, or on material change
OWNER	APPROVER	CLASSIFICATION
IT Manager (identity and access)	Head of IT	Public reference copy

CONTROLS ADDRESSED

SOC 2 CC6.1, CC6.2, CC6.3 · ISO/IEC 27001:2022 A.5.15, A.5.18 · NIST SP 800-53 AC-2, AC-6, AC-6(7)

Why this exists

Common security frameworks require an organisation to demonstrate, periodically, that access is reviewed and that unnecessary access is removed. The obligation is not to believe this is true. It is to show evidence.

A review is only answerable if something has been keeping score. Where there is no system of record for what has been issued to whom, the review becomes a series of guesses collected under time pressure, and the evidence produced is worth very little.

Before the first campaign

- **Name a system of record** for entitlements: who holds which application, licence, device and privileged role.
- **Name an owner for every application.** Reviews are approved by the person accountable for the data, not by IT. IT runs the process; it does not decide who should see payroll.
- **Define what privileged means** for each application, so elevated access can be reviewed on a tighter cycle than ordinary access.
- **Agree the cycle**, and write it down as a commitment:

SCOPE	FREQUENCY
Privileged and administrative access	Quarterly
Systems holding regulated or personal data	Quarterly
All other application access	Twice yearly
Service and non-human accounts	Twice yearly, with a named human owner each time

Running a campaign

1. **Freeze a snapshot.** Export entitlements on a fixed date so reviewers are looking at the same picture and the evidence is reproducible.
2. **Group by owner**, not by application. A reviewer should receive one list, not seven.
3. **Distribute with a deadline** and state plainly what happens if the deadline passes.

4. **Reviewer decides per line:** keep, remove, or change. Force an explicit decision. Silence must never default to keep, which is how reviews become a formality.
5. **Collect exceptions with a reason and an end date.** An exception without an expiry is a permanent grant with extra steps.
6. **Action removals** within a defined window and record the date each was completed.
7. **Retain the evidence:** the snapshot, the decisions, the reviewer identity, the timestamps, and proof of the removals.

What a review reliably surfaces

- **Leavers who are not fully gone.** Where offboarding is automated this should be empty, and confirming it is empty is part of the value.
- **Role changes that only added.** Somebody moved team and gained the new access without losing the old. This is the single most common finding.
- **Dormant accounts**, including service accounts nobody claims.
- **Privileged access granted for one task**, two years ago.
- **Licences paid for and unused.** The same exercise that satisfies the auditor recovers budget, which is the argument that gets the review resourced.

Making the next one cheaper

Every campaign should reduce the cost of the following one.

- If a reviewer cannot tell what an entitlement grants, rename it. Reviewers approve what they do not understand, which defeats the exercise.
- If the same exception is requested every cycle, it is not an exception. Either write it into a role or withdraw it.
- If a whole application is approved wholesale every time, look at whether access should be derived from a role rather than reviewed line by line.
- Where a finding could have been prevented by automation, fix the automation. A review that keeps finding the same class of problem is reporting on a broken process rather than on people.

Service levels

STEP	TARGET
Reviewer window from distribution to deadline	10 business days
Reminder to non-responders	At 5 and 8 business days
Escalation to the reviewer's manager	1 business day after the deadline
Removals actioned after decision	Within 5 business days
Privileged access removals actioned	Within 1 business day
Evidence retained	Minimum 12 months, or one full audit period, whichever is longer
Maximum life of an approved exception	90 days

Non-response is not approval. Where a reviewer misses the deadline and the escalation, the default is removal of the access under review, and the reviewer is told that in advance.

Measure

METRIC	TARGET
Reviewer completion by the deadline	Above 95 per cent
Removals actioned as a share of removals decided	100 per cent
Median time from decision to removal	Under 3 business days
Repeat findings between consecutive campaigns	Falling

Flat repeat findings mean nothing upstream has changed.