

Governance Blueprint Illustrative Assessment

Cedarline Workflow Services Ltd

An original fictional assessment sample

The selected evidence in this sample produces 16 open findings across security, governance, compliance readiness and bounded AI oversight. Management should prioritize privileged-access exceptions, release decisions and demonstrated business recovery before expanding the internal AI pilot.

All entity, system, evidence, observation and management records are invented. No client engagement, real technical test or corrective action took place. This sample demonstrates reporting detail and evidence traceability; a contracted engagement specifies its own boundary and procedures.

Report detail	Record
Reference	CYV-CL-ILL-2026-01
Version and issue	2.0 / 14 October 2026; revised 21 October 2026
Fictional records period	1 July to 30 September 2026
Illustrative review window	1 to 5 October 2026
Prepared for	Fictional executive sponsor and technology leadership
Classification	Public illustrative fictional sample

Sample status Illustrative fictional sample - not a client engagement. No assurance opinion or certification is provided.

Document control and contents

Control	Record
Version	2.0
Issue date	14 October 2026
Owner	Cyvelle Consulting sample production
Change record	21 October 2026: expanded original fictional technical exhibits, all 20 NIST family workpapers and a 12 month programme; 16 findings and 16 actions unchanged
Distribution	Public demonstration; no confidential client information
Data source	report_data.json version 2.0 with family_workpapers.json and technical_exhibits.json; separate domain and family views

Component	Pages
Executive Security & Risk Summary	3 to 5
IT Security & Governance Assessment	6 to 11
Detailed Security Findings	12 to 46
Compliance & Control Gap Matrix	47 to 91
Governance Debt Register	92 to 94
Evidence & Control Review Register	95 to 106
Prioritized Remediation Roadmap	107 to 116
Executive Recommendations & Next Steps	117 to 121

Use the linked component names to navigate the editable document and exported PDF. Each finding links to its evidence, selected check, action and closure requirements through stable identifiers.

Executive Security & Risk Summary

The fictional business has functioning safeguards and a traceable service environment. Material weaknesses remain in operation, review and decision authority. Sixteen findings require treatment: eight High, seven Medium and one Low. No Critical finding or observed breach is asserted.

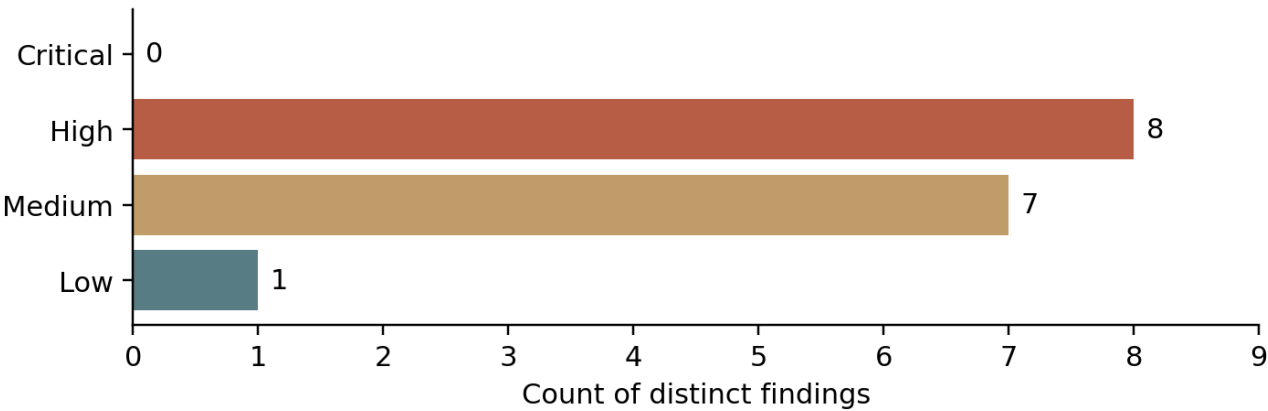


Figure 1. Counts of distinct findings at issue. One finding involves several controls or records; counts do not describe event probabilities or expected losses.

Decision priority	Required management action
First 14 days	Resolve unsupported privileged and departure access; keep the AI pilot within its synthetic-only boundary until an accountable risk decision exists. F03, F04, F15.
First 30 days	Restore collection and scan evidence; enforce release and change risk decisions. F06, F07, F09, F10.
By 45 to 60 days	Demonstrate portal business recovery, complete supplier and retention decisions, and establish repeatable AI draft evaluation. F11 to F14 and F16.

Approval of this roadmap does not mean work is complete. The sponsor assigns capacity, owners approve safe changes and closure follows the evidence and verification criteria for each finding.

Business context and supported strengths

Cedarline is an invented growing technology business providing a customer document-workflow portal and an internal service queue. The portal, identity service and queue are its three declared critical business services. An internal AI pilot summarizes synthetic support tickets for human review. It has no customer-send, autonomous decision or system-write permission.

Business reliance	Supported safeguard	Remaining issue
Workforce access	Eight of 11 departures met the internal removal target; ordinary requests retain independent approval.	Three departure exceptions and four unsupported MFA exclusions. F03, F04.
Customer service delivery	All six pipelines retain source, build and artifact references.	Release gates and independent change decisions remain incomplete. F09, F10.
Recovery	All eight protected workloads have recent successful copy records.	Portal business acceptance and queue retention require decisions. F11, F12.
Provider assurance	All five critical provider files retain signed agreements.	Two reviews omit customer responsibilities. F13.
AI pilot use	All 20 synthetic drafts had human review; tool permissions preserve draft-only behavior.	Risk approval and repeatable evaluation remain incomplete. F15, F16.

These strengths are fictional supported observations within the selected checks. They do not offset unrelated deficiencies or establish comprehensive compliance. Current settings, record samples and benign fixtures answer different questions and retain separate limits.

Buyer and leadership implications

Customer diligence would expose missing risk decisions and incomplete responsibility evidence. A release deadline should not silently replace approval, and provider assurance should not be presented as proof of customer configuration. Leadership should request owned decisions and operational evidence for its next assurance response.

Risk priorities and assessment boundaries

Plausible exposure path	Supporting condition	Business consequence
Obsolete access to service records	Late departure removal plus unsupported MFA exclusions. F03, F04.	Unnecessary access persists if credentials are obtained; no historical misuse is established.
Unreviewed change into production	Independent approval and exception gates incomplete. F09, F10.	Incorrect or inappropriate changes reach customer workflows without the intended challenge.
Incomplete investigation and recovery	Central delivery gap and missing portal acceptance. F07, F11.	Responders rely on manual evidence; infrastructure startup does not establish restored business operations.
Uncontrolled AI expansion	No accountable release risk decision or repeatable evaluation. F15, F16.	A later expansion into customer records lacks a defined approval basis. Current synthetic-only controls remain important.

What the conclusion supports

The report supports 16 findings through the original 48 domain checks, supplemented by 60 family workpaper tests and eight technical exhibits. The two test views deliberately reuse evidence and are not 108 independent observations. No breach probability, loss estimate or enterprise security percentage is asserted.

Decisions outside the assessment

Legal duties, contract acceptance and final residual-risk decisions require the appropriate business and legal authorities. A framework mapping identifies related context and does not prove equivalent compliance, examination readiness or certification. The sample is not a catalog of procedures promised by every Governance Blueprint tier.

IT Security & Governance Assessment

The fictional boundary includes corporate identity, workforce laptops, four cloud accounts, two applications, selected release and change evidence, critical suppliers and one internal AI pilot. Selected criteria address operation and ownership inside this boundary.

Population	Declared count and interpretation
People and identities	184 workforce people and 184 person-linked enabled members are separate snapshots, not a one-to-one authorization assertion. The account snapshot includes one departed identity still enabled. Twelve dedicated admin identities bring the member total to 196; 22 guests are separate.
Managed estate	184 workforce laptops and 24 cloud compute nodes; laptop and node populations are not combined into a protection rate.
Cloud and applications	Four cloud accounts, one corporate collaboration tenant, two applications and three declared critical services.
Engineering	Eight repositories, six pipelines and 18 quarter production changes; change sample 10 and release sample eight.
Suppliers	Nine total suppliers, of which five are critical. The five critical files form the selected review population.
Recovery	Eight protected workloads. Three business services selected for restore and acceptance evidence.
AI	One AssistNotes pilot, 12 authorized users and 20 synthetic drafts. No model weights, training data or external decisions assessed.

All counts and parameters on this page are invented for one coherent scenario. People, accounts, devices, services and workloads are different populations. Counts must not be added as if they were unique systems or incidents.

Extended workpaper boundary and populations

This expanded fictional scope adds selected office, personnel learning, maintenance and media-handling records to the original cloud, workforce, applications and supplier boundary. These are invented extensions for the reporting example, not evidence collected in a real engagement. The three critical services remain portal, identity service and internal queue. New subsets do not change the original 184 workforce people, 196 member identities, 184 active laptops, 24 compute nodes or four cloud accounts.

Selected population	Declared count and boundary
Office physical controls	1 office and 1 network room; 12 selected badges and 4 visitors; 1 UPS and 1 fire zone
Learning and access acknowledgments	184 people reconciled; 6 fictional custodians mapped to 12 dedicated admin identities; 2 training corrections
Maintenance	6 laptop repairs; 3 remote sessions; 4 authorized technicians and 2 external visits
Media lifecycle	4 retired drives outside the active laptop inventory; 2 shipments; 2 synthetic USB evaluations
People onboarding	8 selected starters already within the workforce population; 6 custodian screening indicators
Selected supporting governance records	4 monitoring schedules; 3 prior reviews; 3 risk scenarios; 4 budget decisions; 2 architecture changes; 2 privacy notice changes
Additional synthetic technical fixtures	2 application tenant-boundary pairs; 4 service credentials; network and TLS path examples; 2 cloud datastore/key examples; optional marketing preference pair

Distinct populations and evidence views

The 184-person workforce roster and 184 person-linked enabled-member snapshot are different populations. Equal counts do not prove a one-to-one authorization relationship: F03 retains one departed identity enabled at cut-off. Twelve dedicated administrative identities bring enabled members to 196; 22 guests remain separate. Training completion and access acknowledgments do not resolve that open departure finding.

The additional fixtures are selected examples, not an expansion into a complete physical-security audit, personnel assurance opinion or full enterprise technical test. Family workpapers specify the relevant subset and method. The 48 original domain checks and 60 family tests intentionally overlap and must not be added as independent evidence.

Environment and trust responsibilities

Layer	Declared responsibility	Evidence and boundary
People and devices	IT operations and identity leads govern joiner, mover, departure and device settings.	E03 to E06; workforce and admin identities have separate counts.
Customer-service cloud	Cloud operations maintains four accounts, node settings, logging and copies.	E06, E07, E12; provider physical infrastructure excluded.
Delivery chain	Engineering and the release manager govern changes, repository rules and security exceptions.	E09, E10; no malicious payload or production exploitation.
Incident and recovery	Incident and resilience leads coordinate decisions, evidence and business acceptance.	E08, E11; full business failover excluded.
Suppliers and data	Procurement, privacy and data owners approve provider responsibilities and retention.	E13, E14; no legal opinion or production deletion.
AI pilot	Product operations maintains synthetic-only use and human draft review.	E15, E16; no autonomous decisions or direct customer output.

Shared responsibility

Provider assurance contributes evidence about the stated provider boundary. Cedarline still owns access policy, data decisions, collection, configured recovery and its use of AI outputs. The assessment records F02 and F13 where these assignments are incomplete. A third-party report does not turn provider-operated functions into customer-operated passes.

Change triggers

New services, provider transfers, privilege changes, data flows and AI model or use changes should trigger a refreshed boundary and criteria selection. A point-in-time snapshot has no lasting assurance after the relevant configuration changes.

Methods and result interpretation

Method	Use and limitation
Examine	Describe corroboration among configuration, inventory, tickets and owner decisions within the invented population.
Interview	Record fictional role statements separately; corroborate rather than treat statements as independent operation evidence.
Benign fixture illustration	Document invented authorized and denied outcomes using synthetic identities and data; no real tests were executed.
Judgmental sampling	Select relevant records for the fictional sample; do not project sample exception rates to a whole enterprise.

Result	Meaning in this sample
PASS	Selected evidence supports the stated criterion or bounded fixture outcome. It does not establish every related control.
PARTIAL	A mechanism exists but sampled coverage, operation, review or evidence is deficient.
NOT IMPLEMENTED	A required mechanism is absent. The AI release risk approver and signed decision are absent in F15.
NOT APPLICABLE	The declared activity does not apply; a reason and boundary record exist. This is excluded from passes.
NOT ASSESSED	No determination was made because the procedure or evidence was unavailable or outside scope. This is excluded from passes.

In the original 48-check domain view, 28 pass, 15 are partial and one mechanism is absent; two are not applicable and two not assessed. The 44 applicable assessed checks are not a full-framework denominator. The separate 60-test family view is summarized in the expanded matrix; no compliance percentage is reported.

Positive and negative fixture checks illustrate authorized and denied decisions. Every outcome is invented. These checks demonstrate reporting design; no actual application, workflow or cloud account was accessed or tested.

Selected criteria and sample design

The CL criteria are authored fictional internal thresholds. NIST SP 800-53 Revision 5 with Release 5.2.0 supplies selected control context, NIST CSF 2.0 supplies outcome context and NIST AI RMF 1.0 supplies selected AI category context. They are not combined into a universal compliance baseline.

Domain	Selected check population	Mapping context
Governance	12 open security exceptions in the quarter-end register; all 12 examined	PM-09; CA-05 / PM-01; PL-02
Identity and access	11 workforce departures from 1 July to 30 September 2026; all 11 examined	AC-02; PS-04 / IA-02; AC-06
Assets and vulnerability	184 workforce laptops; risk-based sample of 30 laptops; full owner inventory examined	CM-08; CM-06 / RA-05; SI-02
Logging and response	Four cloud accounts and seven declared priority log sources; all configurations examined; 10 working days of review records	AU-02; AU-06; AU-12 / IR-04; IR-08
Change and delivery	18 production changes in the quarter; judgmental sample of 10 changes	CM-03; CM-04 / SA-11; SI-02
Resilience	Three declared critical business services; one isolated restore record per service examined	CP-04; CP-10 / CP-09
Suppliers and data	Nine suppliers including five critical providers; all five critical provider files examined	SR-03; SA-09 / SI-12; PT-03
AI oversight	One AssistNotes internal pilot with 12 authorized users; pilot approval and use boundary examined	AI RMF GOVERN 1; MANAGE 1 / AI RMF MEASURE 2; MANAGE 2

Sampling limits

All 11 departures, four cloud accounts, five critical-provider files, six data flows and 20 AI drafts were examined within their declared fictional populations. Laptop settings, production changes, releases and service-node patch decisions use judgmental samples. Their exceptions are not statistically representative and must not be projected to unexamined records.

Version 2.0 includes selected objectives in all 20 NIST SP 800-53 families, not every control or enhancement, every CSF outcome or every AI RMF category. Procedures are original tailored illustrations, informed by SP 800-53A assessment-method concepts rather than verbatim procedures. NIST source identity and release were rechecked on 21 October 2026.

Domain results and priority interpretation

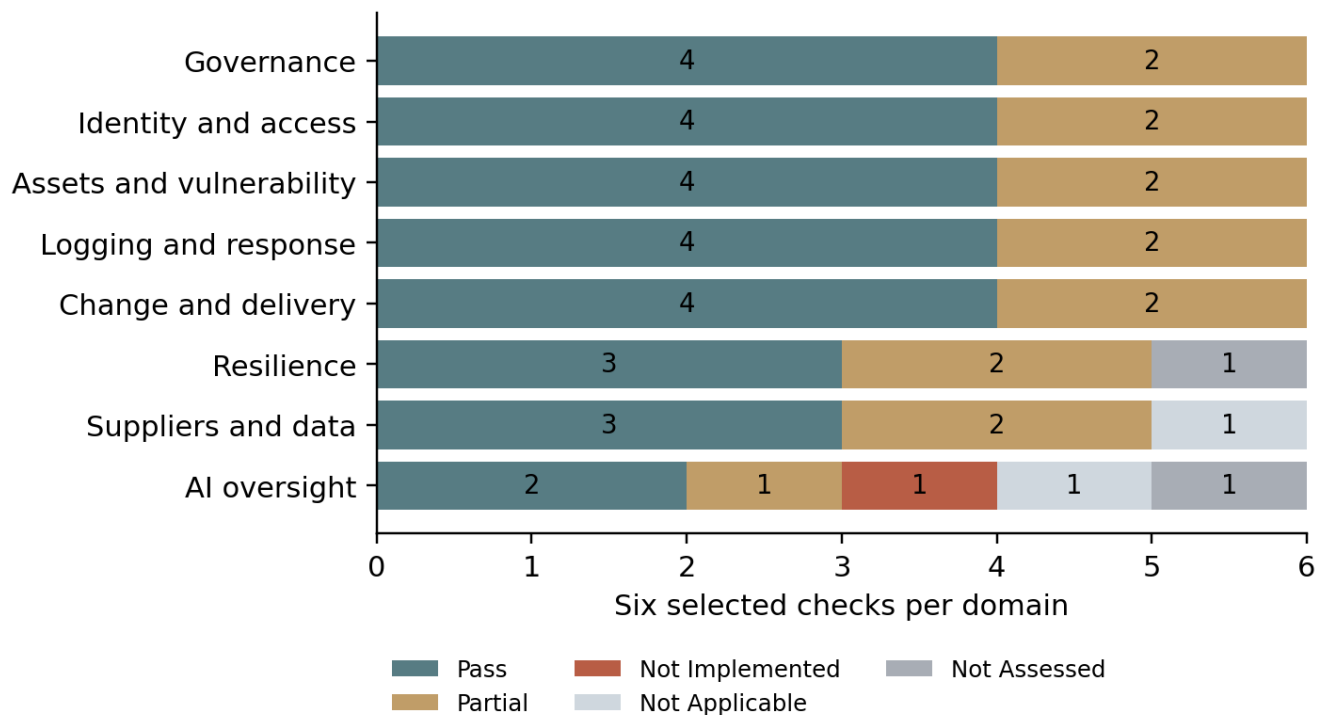


Figure 2. Original domain view only: six selected checks in each of eight domains, 48 total. Segment labels are counts. Not applicable and not assessed remain distinct and are excluded from passes. The domains are a report organization, not formal framework maturity levels.

Each domain has two findings. Several positive or denied fixture outcomes remain alongside those findings because a supported safeguard does not remove an unrelated gap. The chart is generated from the same test records shown in the matrix and stored in report_data.json.

Severity definitions

High indicates material service, privilege or expansion-control exposure requiring priority treatment within the declared boundary. Medium indicates a significant bounded control or evidence gap requiring scheduled correction. Low indicates a limited ownership weakness. Critical would require an immediate broad-consequence condition; none is represented here. These are qualitative scenario judgments, not CVSS scores or event probabilities.

Detailed Security Findings

F01 Risk exceptions lack expiry and sponsor decisions

Severity and rationale Medium. A significant bounded control or evidence gap requires scheduled correction and verification.

Accountable owner Security lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-01: Every retained risk exception requires owner, sponsor, safeguard and review expiry. Context mapping: PM-09; CA-05.

Population and method 12 open security exceptions in the quarter-end register; all 12 examined. Fictional examination of the declared records; no production execution.

Observed condition Five of 12 exceptions lack an expiry; three of those five also lack a sponsor decision. This is five unique deficient exception records, not eight incidents.

Evidence and workpaper E01; T01-01. The records and outcomes are fictional.

Risk and business consequence Four overdue access and change exceptions remain subject to informal team-level decisions. A customer diligence response would lack a current accountable treatment decision.

Root cause in the scenario The exception form permits blank review and sponsor fields; no recurring escalation owner is assigned.

Existing safeguards Seven records retain current approvals and expiries. The service desk sends monthly reminders, which do not enforce escalation.

Recommended action A01. Require owner, reason, safeguard, sponsor decision and expiry for each retained exception; reconcile the five records and route overdue items to the sponsor.

Dependency and target Management risk appetite and named decision authority. Days 1 to 30 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Updated register, five dated decisions, approval history and one subsequent monthly escalation record.

Verification Reconcile all 12 records and inspect a fresh exception submitted after the form change.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F02 Shared cloud responsibilities lack an assigned control owner

Severity and rationale Low. A limited ownership weakness requires correction; no broad authority path is established.

Accountable owner Technology director. Status: OPEN at issue; remediation not performed.

Selected criterion CL-02: Each selected shared responsibility requires an accountable owner and deputy. Context mapping: PM-01; PL-02.

Population and method Eight selected shared-control responsibility records; all eight examined. Fictional examination of the declared records; no production execution.

Observed condition Two responsibility records name a team but no accountable individual: cloud evidence retention and supplier-assisted recovery. Six records identify an individual and backup.

Evidence and workpaper E02; T01-02. The records and outcomes are fictional.

Risk and business consequence Collection and recovery tasks would stall during absence or a provider handoff. The bounded gap is an ownership weakness without a demonstrated failed security event.

Root cause in the scenario The ownership register predates the provider support change and has no update trigger.

Existing safeguards The technology director owns the enterprise charter; six responsibilities have working escalation routes.

Recommended action A02. Name accountable owners and deputies for both gaps; add a provider-change trigger and confirm each role accepts the assignment.

Dependency and target Provider support scope and sponsor approval. Days 1 to 45 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Accepted responsibility matrix, escalation contacts and a simulated absence handoff record.

Verification Trace a sample provider-support change to the revised assignment and confirm the deputy route.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F03 Departure accounts remain enabled beyond the internal target

Severity and rationale High. Material service or privileged-access exposure warrants priority treatment within the stated boundary.

Accountable owner Identity lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-03: Workforce departure access must be removed within 24 hours of the authoritative event. Context mapping: AC-02; PS-04.

Population and method 11 workforce departures from 1 July to 30 September 2026; all 11 examined. Fictional examination of the declared records; no production execution.

Observed condition Three of 11 workforce accounts did not meet the internal 24-hour removal target. Two were disabled after 41 and 63 hours; one account remained enabled at the 30 September cut-off. No use after departure is asserted.

Evidence and workpaper E03; T02-01. The records and outcomes are fictional.

Risk and business consequence An unnecessary account retains a route to customer workflow records if its credentials are obtained. Current session evidence does not establish historical misuse or its absence.

Root cause in the scenario HR and the service desk reconcile weekly rather than through a same-day departure trigger.

Existing safeguards Eight departures met the internal target. Approved role assignments and daily sign-in review were present for the sample.

Recommended action A03. Resolve the remaining account with the business owner, revoke sessions where required and implement a same-day HR trigger with an independent reconciliation.

Dependency and target Authoritative HR timestamps and safe access removal. Days 1 to 14 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Current account and session export, authorized tickets for three exceptions, HR trigger evidence and next departure timing.

Verification Reconcile all 11 records; trace the next departure from HR event to effective access removal.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F04 MFA policy exclusions include unsupported privileged access

Severity and rationale High. Material service or privileged-access exposure warrants priority treatment within the stated boundary.

Accountable owner Identity lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-04: All intended member accounts require enforced MFA or an approved monitored emergency design. Context mapping: IA-02; AC-06.

Population and method 196 enabled member accounts including 12 dedicated administrative identities; policy scope examined in full. Fictional examination of the declared records; no production execution.

Observed condition Four member accounts are excluded from the intended MFA policy without a current exception. Two are dedicated administrative identities. The two monitored emergency identities are separately approved and are not part of these four exceptions.

Evidence and workpaper E04; T02-02. The records and outcomes are fictional. See the E04 record exhibit on the following page.

Risk and business consequence A password-only route to administrative functions increases exposure to stolen credentials. Method registration is not proof of policy enforcement.

Root cause in the scenario A temporary migration group remained excluded after migration; its membership review was not scheduled.

Existing safeguards The remaining 192 accounts fall within the intended MFA policy or the two documented emergency-access designs. Sample policy evaluation records support those assignments.

Recommended action A04. Remove unsupported exclusions after validating access impact; document intended emergency design and test both authorized access and disallowed password-only access in a sandbox.

Dependency and target Monitored emergency route and user communication. Days 1 to 14 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Approved policy diff, membership reconciliation and positive and denial evaluation records.

Verification Re-evaluate the four affected identities and selected ordinary, privileged and emergency test identities.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

E04 MFA exclusion evidence exhibit

Fictional record-level illustration for F04

Trace: E04 to T02-02 to F04 to A04. These four invented aliases expand the existing four unsupported exclusions; they add no findings, checks or evidence bundles. No account was accessed, policy evaluated or test executed.

Scenario at the 30 September 2026 cut-off: the retained migration group excludes these accounts from the intended MFA policy. None has an approved emergency-access exception. The illustrative pre-change outcome below assumes valid credentials and the stated exclusion; it is not a measured sign-in result.

Fictional alias	Policy and emergency status	Illustrative pre-change outcome	Risk within scope	Planned verification and expected result
MFA-EX-01 Dedicated admin	Migration-group exclusion. No approved emergency status.	Invented fixture: password-only access allowed; no MFA challenge.	Stolen credentials could reach administrative functions.	After removal: DENY password-only access. ALLOW authorized admin access with valid MFA. Retain both results.
MFA-EX-02 Dedicated admin	Migration-group exclusion. No approved emergency status.	Invented fixture: password-only access allowed; no MFA challenge.	Stolen credentials could reach administrative functions.	After removal: DENY password-only access. ALLOW authorized admin access with valid MFA. Retain both results.
MFA-EX-03 Ordinary member	Migration-group exclusion. No approved emergency status.	Invented fixture: password-only access allowed; no MFA challenge.	Stolen credentials could reach ordinary member resources.	After removal: DENY password-only access. ALLOW authorized member access with valid MFA. Retain both results.
MFA-EX-04 Ordinary member	Migration-group exclusion. No approved emergency status.	Invented fixture: password-only access allowed; no MFA challenge.	Stolen credentials could reach ordinary member resources.	After removal: DENY password-only access. ALLOW authorized member access with valid MFA. Retain both results.

Count reconciliation

Four unsupported exclusions = two dedicated administrative identities + two ordinary member identities. The other 192 of 196 member accounts retain the existing intended-policy or approved-emergency classification. The two approved, monitored emergency identities are within those 192 and outside this table.

Closure under A04

Retain the approved policy diff, migration-group membership reconciliation and allowed/denied evaluation records for all four aliases. Also evaluate representative ordinary, privileged and both approved emergency identities against their intended designs. This planned verification does not claim remediation or closure.

F05 Asset owners and protection exceptions do not reconcile

Severity and rationale Medium. A significant bounded control or evidence gap requires scheduled correction and verification.

Accountable owner IT operations lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-05: Active laptops require an owner and current approved protection settings. Context mapping: CM-08; CM-06.

Population and method 184 workforce laptops; risk-based sample of 30 laptops; full owner inventory examined. Fictional examination of the declared records; no production execution.

Observed condition Six of 184 laptops lack a current business owner. In the 30-laptop sample, four reported encryption-profile exceptions and three protection-policy exceptions overlap on two laptops: five unique sample devices have at least one setting exception.

Evidence and workpaper E05; T03-01. The records and outcomes are fictional.

Risk and business consequence Unowned devices fall outside dependable patch and incident routing. Reported configuration gaps increase exposure if a device is lost or accessed without authorization.

Root cause in the scenario Device discovery and assignment records use different identifiers; exceptions are tracked as support tasks without expiry.

Existing safeguards All 30 sampled laptops report a managed endpoint agent. Twenty-five meet both examined settings; inventory and telemetry are present.

Recommended action A05. Reconcile six owner records and five unique sample devices; record current policy outcomes and approved time-limited exceptions where treatment is deferred.

Dependency and target Stable device identifiers and business-owner confirmation. Days 1 to 45 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Reconciled inventory, current five-device exports, approved exceptions and new onboarding record.

Verification Re-examine the five devices and a fresh onboarding sample; retain the overlap calculation.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F06 Authenticated scan coverage and flaw treatment lack full evidence

Severity and rationale High. Material service or privileged-access exposure warrants priority treatment within the stated boundary.

Accountable owner Cloud operations lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-06: Cloud nodes require monthly authenticated coverage; internal high flaws require treatment within 21 days or an approved exception. Context mapping: RA-05; SI-02.

Population and method 24 cloud compute nodes; latest monthly scan cycle examined; 10 customer-service nodes sampled for patch decisions. Fictional examination of the declared records; no production execution.

Observed condition 19 of 24 nodes report authenticated scanning; three report authentication failure and two lack a scheduled record. Three of the 10 sampled service nodes have internally rated high flaws older than the fictional 21-day treatment target without a current exception.

Evidence and workpaper E06; T03-02. The records and outcomes are fictional.

Risk and business consequence Coverage gaps obscure the current condition of service dependencies. A reported flaw requires applicability and exposure validation before its priority is finalized.

Root cause in the scenario Scanner credential rotation was not reconciled to new nodes; patch exceptions do not require expiry.

Existing safeguards Nineteen authenticated records and seven timely sample treatments exist. Network rules restrict service administration to the controlled support path.

Recommended action A06. Restore authenticated coverage for five exceptions; validate the three overdue flaw records and approve safe treatment or documented compensating safeguards.

Dependency and target Maintenance approval, applicability review and rollback. Days 1 to 30 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Fresh 24-node scan reconciliation, authentication outcomes, three treatment records and authorized exceptions.

Verification Inspect one fresh authenticated cycle and verify applicability and treatment on the three sampled nodes.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F07 Central event delivery omits one cloud account and feed health

Severity and rationale High. Material service or privileged-access exposure warrants priority treatment within the stated boundary.

Accountable owner Security operations lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-07: Every declared account delivers priority events centrally and required feeds have tested health alerts. Context mapping: AU-02; AU-06; AU-12.

Population and method Four cloud accounts and seven declared priority log sources; all configurations examined; 10 working days of review records. Fictional examination of the declared records; no production execution.

Observed condition Three of four cloud accounts have central management-event delivery. The development account retains native events but lacks central delivery. Two of seven priority feeds lack a tested stale-feed alert; one is the development account, so the sets overlap.

Evidence and workpaper E07; T04-01. The records and outcomes are fictional.

Risk and business consequence An investigation crosses incomplete central records and depends on manual recovery of native events. Missing central collection is not proof of missing native logging.

Root cause in the scenario The new-account checklist omits delivery verification and feed-health ownership.

Existing safeguards All four accounts have native management-event logging. Eight of 10 working days retain a documented central review and escalation record.

Recommended action A07. Add central delivery for the development account and test controlled stale-feed alerts for both affected sources; reconcile account onboarding and daily review records.

Dependency and target Native retention, collection permissions and test window. Days 1 to 30 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Delivery configuration, benign event trace, two stale-feed alert records and review history.

Verification Trace a benign event from each account and simulate a feed delay in an isolated test source.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F08 Incident decision authority is absent for supplier data exposure

Severity and rationale Medium. A significant bounded control or evidence gap requires scheduled correction and verification.

Accountable owner Incident lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-08: Incident decisions require named primary and deputy authority appropriate to supplier exposure. Context mapping: IR-04; IR-08.

Population and method One incident plan and six fictional supplier-exposure exercise decisions; all decisions examined. Fictional examination of the declared records; no production execution.

Observed condition Two of six exercise decisions lack a named approver: temporary suspension of supplier data flow and customer notification authorization. Four decisions identify an accountable role and alternative contact.

Evidence and workpaper E08; T04-02. The records and outcomes are fictional.

Risk and business consequence Containment and communication would wait for unplanned executive availability. A tabletop decision gap is not proof of a missed real incident or a legal notification deadline.

Root cause in the scenario The plan lists technical responders but omits commercial and privacy authorization during supplier events.

Existing safeguards The reporting channel, triage owner and four other exercise decisions are documented. No actual supplier incident is asserted.

Recommended action A08. Name primary and deputy decision roles, validate contractual notice duties with counsel and repeat the two decision paths in a tabletop exercise.

Dependency and target Legal and contract review; executive availability. Days 15 to 45 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Approved plan, contact acceptance, exercise log for both decisions and follow-up action decisions.

Verification Repeat a supplier scenario with the primary approver unavailable and observe the deputy decision route.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F09 Production changes lack independent approval and rollback evidence

Severity and rationale High. Material service or privileged-access exposure warrants priority treatment within the stated boundary.

Accountable owner Engineering lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-09: Production changes require independent authorization and evidenced rollback preparation. Context mapping: CM-03; CM-04.

Population and method 18 production changes in the quarter; judgmental sample of 10 changes. Fictional examination of the declared records; no production execution.

Observed condition Three of 10 sampled changes lack independent approval before deployment. Two of those three also lack recorded rollback validation. These are three unique deficient changes, not five.

Evidence and workpaper E09; T05-01. The records and outcomes are fictional.

Risk and business consequence A configuration error or inappropriate change reaches customer workflows without the intended challenge or dependable reversal evidence.

Root cause in the scenario Emergency changes bypass the ordinary approval form and retrospective review is not enforced.

Existing safeguards Seven sample changes retain independent approvals. All 10 map to a named deployer and a change ticket.

Recommended action A09. Enforce ordinary independent approval; define emergency authorization and retrospective review; validate rollback for the two identified changes before the next related release.

Dependency and target Release calendar and emergency support process. Days 1 to 30 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Approved workflow, revised three-change decisions, rollback records and fresh emergency-change review.

Verification Inspect the next ordinary and emergency changes and verify approval timing and rollback evidence.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F10 Release decisions do not enforce security exception approval

Severity and rationale High. Material service or privileged-access exposure warrants priority treatment within the stated boundary.

Accountable owner Release manager. Status: OPEN at issue; remediation not performed.

Selected criterion CL-10: Release decisions require resolution or an approved expiring exception for internal high issues. Context mapping: SA-11; SI-02.

Population and method Eight repositories and six delivery pipelines; eight releases sampled from the quarter. Fictional examination of the declared records; no production execution.

Observed condition Six of eight repositories have the intended branch protection. Three of eight sampled releases contain unresolved internal high security findings without an authorized expiring exception. No exploitability or breach is inferred.

Evidence and workpaper E10; T05-02. The records and outcomes are fictional.

Risk and business consequence A known material issue passes into a customer release without an accountable risk decision, increasing rework and potential service exposure.

Root cause in the scenario Security jobs record findings but the release workflow treats their status as advisory.

Existing safeguards All six pipelines produce traceable build logs. Five sampled releases have either resolved high issues or an approved exception.

Recommended action A10. Protect the remaining two repositories and require a resolution or valid exception before release; preserve an approved emergency path with time-bounded review.

Dependency and target Reliable severity triage and release-owner acceptance. Days 1 to 30 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Repository rules, enforced gate record, three issue decisions and approved and rejected benign test releases.

Verification Use synthetic fixtures to demonstrate one authorized release and one release denied for an unapproved high finding.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F11 Critical service restore evidence lacks business acceptance

Severity and rationale High. Material service or privileged-access exposure warrants priority treatment within the stated boundary.

Accountable owner Resilience lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-11: Critical service recovery requires business acceptance against its approved service objective. Context mapping: CP-04; CP-10.

Population and method Three declared critical business services; one isolated restore record per service examined. Fictional examination of the declared records; no production execution.

Observed condition Two of three services retain a complete restore and business-acceptance record. The customer portal has infrastructure restore evidence but no reconciliation or business-owner sign-off against its fictional four-hour recovery objective.

Evidence and workpaper E11; T06-01. The records and outcomes are fictional.

Risk and business consequence A technically restored database would still leave customer work unusable or inconsistent. A backup success or infrastructure startup does not establish business recovery.

Root cause in the scenario Recovery exercises stop at platform startup; product acceptance criteria were not assigned.

Existing safeguards The other two critical services retain accepted exercises. Portal backup jobs and a documented recovery objective exist.

Recommended action A11. Agree portal transaction reconciliation and user acceptance, perform an isolated restore with synthetic data and record elapsed time and the business decision.

Dependency and target Synthetic test dataset, isolated environment and business-owner availability. Days 1 to 45 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Restore log, record-count reconciliation, transaction checks, elapsed times and signed business acceptance.

Verification Reperform the portal scenario in isolation; compare outcome to the approved objective without claiming enterprise recoverability.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F12 Independent backup copy retention lacks an accountable decision

Severity and rationale Medium. A significant bounded control or evidence gap requires scheduled correction and verification.

Accountable owner Cloud operations lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-12: Workload copy retention follows a documented business decision; the sample default is 30 days. Context mapping: CP-09.

Population and method Eight protected workloads; all backup policies and copy records examined. Fictional examination of the declared records; no production execution.

Observed condition Seven of eight workloads have an independent copy with the fictional 30-day retention setting. The internal queue has a 14-day copy retention setting without an approved business decision. Copy success exists for all eight workloads.

Evidence and workpaper E12; T06-02. The records and outcomes are fictional.

Risk and business consequence Recovery options for one service fall outside the declared retention requirement. The gap concerns retained coverage, not a failed current backup job.

Root cause in the scenario The service was added with a default retention template and not routed through the business retention review.

Existing safeguards All eight workloads show recent successful copy records; independent recovery permissions are separated in the collected configuration.

Recommended action A12. Obtain the business retention decision, update the queue policy if required and review the next retention cycle with the recovery owner.

Dependency and target Business retention requirement and recovery capacity. Days 15 to 60 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Dated retention decision, policy record, subsequent copy history and selected restoration proof.

Verification Check the approved retention horizon and sample a retained queue copy after the policy observation period.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F13 Critical provider assurance omits customer responsibilities

Severity and rationale Medium. A significant bounded control or evidence gap requires scheduled correction and verification.

Accountable owner Procurement lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-13: Critical provider reviews cover report scope, exceptions and relevant customer responsibilities. Context mapping: SR-03; SA-09.

Population and method Nine suppliers including five critical providers; all five critical provider files examined. Fictional examination of the declared records; no production execution.

Observed condition Two of five critical-provider files contain current assurance reports but no recorded review of customer responsibilities or relevant exceptions. The other three retain reviewer decisions.

Evidence and workpaper E13; T07-01. The records and outcomes are fictional.

Risk and business consequence A provider report would be cited as assurance while required customer actions remain unassigned. Provider controls do not establish Cedarline configuration.

Root cause in the scenario Procurement checks report date and availability but not control relevance or assigned customer actions.

Existing safeguards All five files retain signed agreements and a designated contract owner. Three include responsibility and exception review.

Recommended action A13. Review the two reports for scope, period, exceptions and customer responsibilities; assign relevant actions and confirm evidence for required Cedarline controls.

Dependency and target Access to complete provider reports and system-owner review. Days 15 to 60 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Two review records, responsibility matrix, owner decisions and applicable customer-control evidence.

Verification Trace each identified responsibility to the accountable owner and inspect the next provider renewal review.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F14 Customer export retention decisions do not cover all flows

Severity and rationale Medium. A significant bounded control or evidence gap requires scheduled correction and verification.

Accountable owner Privacy lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-14: Customer-data flows require approved purpose and retention decisions with evidenced configuration. Context mapping: SI-12; PT-03.

Population and method Six customer-data processing flows and 12 export storage locations; all declared flows examined. Fictional examination of the declared records; no production execution.

Observed condition Two of six flows lack an approved retention purpose and duration. Three of 12 storage locations carry those two flows. No lawful basis or legal retention conclusion is made from these records.

Evidence and workpaper E14; T07-02. The records and outcomes are fictional.

Risk and business consequence Unnecessary retention enlarges the information subject to exposure and complicates deletion requests. A policy statement without configuration evidence does not establish deletion.

Root cause in the scenario New support exports bypass the processing-register change review.

Existing safeguards Four flows have approved retention decisions. Access to all 12 locations is restricted to documented support roles.

Recommended action A14. Obtain purpose and retention decisions for both flows with counsel and business owners; validate lifecycle rules in isolation using synthetic objects and reconcile the processing register.

Dependency and target Legal holds, contract duties and data-owner approval. Days 15 to 60 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Two decisions, updated register, lifecycle rules, synthetic expiry results and documented hold behavior.

Verification Trace synthetic objects through expiry and hold paths; do not delete production records during assessment.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F15 Internal AI assistant lacks an accountable release risk decision

Severity and rationale High. Material service or privileged-access exposure warrants priority treatment within the stated boundary.

Accountable owner Product operations lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-15: AI expansion and material change require a named accountable risk approver and documented decision. Context mapping: AI RMF GOVERN 1; MANAGE 1.

Population and method One AssistNotes internal pilot with 12 authorized users; pilot approval and use boundary examined. Fictional examination of the declared records; no production execution.

Observed condition The pilot charter identifies a technical owner but contains no accountable approver for residual AI risk or material model changes. No signed release risk decision exists. The pilot is limited to synthetic ticket data and draft notes.

Evidence and workpaper E15; T08-01. The records and outcomes are fictional.

Risk and business consequence The pilot would expand into customer records without a clear decision on privacy, errors and provider terms. The high rating reflects the missing expansion control, not demonstrated current customer harm.

Root cause in the scenario A tool trial was approved as a technical experiment without a business risk approval route.

Existing safeguards The pilot uses synthetic inputs, has no write or send permission and requires a human to review every draft. Current constraints reduce immediate exposure.

Recommended action A15. Keep the current synthetic-only boundary; assign the risk approver and stop expansion pending data, provider and impact review with an explicit release decision.

Dependency and target Privacy review, provider terms and named risk authority. Days 1 to 14 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Accepted responsibility, documented use boundary, impact review, change trigger and signed release or stop decision.

Verification Trace a fictional model-change request to the approver; demonstrate expansion remains blocked without the required decision.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

F16 AI draft evaluation lacks repeatable acceptance criteria

Severity and rationale Medium. A significant bounded control or evidence gap requires scheduled correction and verification.

Accountable owner Product operations lead. Status: OPEN at issue; remediation not performed.

Selected criterion CL-16: AI evaluation criteria, test cases and versioned results precede release approval. Context mapping: AI RMF MEASURE 2; MANAGE 2.

Population and method 20 synthetic ticket drafts in the internal AssistNotes pilot; all 20 review records examined. Fictional examination of the declared records; no production execution.

Observed condition Three of 20 drafts contain an unsupported operational detail requiring correction. Reviewers corrected all three before use, but no predeclared acceptance threshold, repeatable test set or model-change retest rule exists.

Evidence and workpaper E16; T08-02. The records and outcomes are fictional.

Risk and business consequence A successful human review in one small set does not establish reliable future outputs. Expansion would lack a consistent comparison for material error types.

Root cause in the scenario Pilot feedback records are informal and lack versioned evaluation criteria.

Existing safeguards Human review is mandatory; no draft is sent to customers or committed automatically. All 20 drafts retain reviewer notes.

Recommended action A16. Define unacceptable error categories and acceptance criteria before a new version; retain synthetic cases and repeat evaluation after material changes; route failures to the risk approver.

Dependency and target F15 risk approver and a versioned synthetic test corpus. Days 15 to 45 from the illustrative issue date, subject to safe approval and available owners.

Closure evidence Versioned criteria, test cases, reviewer calibration, results and approval for the evaluated model version.

Verification Repeat the fixed corpus and targeted negative cases using synthetic data; record any unresolved error rather than forecasting reliability.

No treatment or closure is asserted. A closed ticket, approved policy or purchased tool is insufficient without the required operational evidence.

Technical exhibit navigation

Eight original technical exhibits expand the existing findings into specific configuration, record-reconciliation and safe verification examples. They illustrate AWS, Microsoft 365, identity, release, recovery, data and bounded AI controls without adding new finding or action counts.

All exhibit records are original invented Cedarline fixtures. No real system was accessed or tested. Proposed verification cases and desired trust designs are not observed passes and do not enter the control-result denominator.

Exhibit	Technical subject	Existing findings	Pages
XE01	AWS central logging and feed health	F07	30 to 31
XE02	AWS authenticated scan and treatment reconciliation	F06	32 to 33
XE03	AWS independent backup copy and portal recovery	F11; F12	34 to 35
XE04	Microsoft 365 conditional access and administrative exceptions	F04	36 to 37
XE05	Microsoft 365 collaboration and customer export retention	F14	38 to 39
XE06	Application security gates and CI CD deployment trust	F10	40 to 42
XE07	Production change approval and rollback trace	F09	43 to 44
XE08	Bounded AI pilot release and repeatable evaluation	F15; F16	45 to 46

Reading the exhibits

Observed fictional conditions, successful or denied invented fixtures, desired designs and proposed closure tests are labeled separately. A desired policy or proposed retest is not an observed PASS. All identifiers are illustrative. No credentials, customer records or live infrastructure access are represented.

The report keeps the original 16 findings and their owners. The exhibit trace connects to those findings, existing evidence bundles and action acceptance requirements. Reuse of one export or control record does not create an independent observation.

XE01 AWS central logging and feed health

System and scope Four fictional AWS accounts and a central security collection service. Four accounts; seven declared priority feeds; ten working days of review records.

Selection All four account configurations and seven feed definitions; configuration excerpts below identify the one missing central route and the two overlapping feed-health exceptions.

Authored criterion CL logging criterion: retain native management events, deliver all four accounts centrally, and prove an alert when a priority feed becomes stale. A central route is not established by a trail definition alone.

Trace E07 to XE01 to F07 / A07. All records are invented.

Record	Native events	Central delivery	Stale alert evidence
aws-prod	Enabled; sample event P-0918-01	Delivered with matching event ID	HF01 retained
aws-shared	Enabled; sample event S-0918-01	Delivered with matching event ID	HF02 retained
aws-security	Enabled; sample event Q-0918-01	Delivered with matching event ID	HF03 retained
aws-development	Enabled; sample event D-0918-01	No destination configured	No stale test retained
feed-identity	Declared priority feed	Delivered	HF05 retained
feed-endpoint	Declared priority feed	Delivered	No stale test retained
feed-application	Declared priority feed	Delivered	HF07 retained

Configuration illustration

Purpose Contrast native logging with the missing central CloudWatch Logs destination for the fictional development account. The object joins selected fields from separate configuration/status views; it is not an AWS API response.

Status and boundary Invented observed-condition illustration for F07; no API called. Bucket name is fictional and no configuration should be deployed.

Representation Normalized JSON from trail configuration and status fields

```
{
  "accountAlias": "aws-development",
  "trail": {"Name": "cedarline-dev-management",
    "S3BucketName": "cedarline-example-dev-native-logs",
    "IsMultiRegionTrail": true,
    "CloudWatchLogsLogGroupArn": null},
  "trailStatus": {"IsLogging": true},
  "centralEventMatch": false,
  "staleFeedTestArtifact": null
}
```

XE01 Original technical procedure

1. Reconcile the four account IDs to the declared inventory before inspecting trail configuration; do not infer complete inventory from the console account list alone.
2. For each account, inspect event-selector scope, destination identifier, delivery status and destination read permissions. Match one synthetic native event ID and UTC timestamp to the central record.
3. Inspect the seven feed rules for owner, delay threshold and escalation route; reconcile test artifacts to feed IDs rather than counting rule definitions.
4. In an isolated collector test channel, suppress a synthetic heartbeat beyond the locally approved delay, observe the notification and restore the channel. Do not interrupt production logging.
5. Reconcile all ten review dates: the existing case contains eight documented reviews; missing review records are evidence gaps, not proof that no person reviewed events.

Allowed denied and proposed cases

Positive delivery A benign prod event is traceable end to end. Illustrated outcome: Fixture P-0918-01 appears in both native and central records.

Negative delivery An account without a destination cannot satisfy central collection. Illustrated outcome: Fixture D-0918-01 remains native only.

Proposed stale-feed retest Test heartbeat delay raises a dated alert with owner acknowledgment. Illustrated outcome: Future closure exercise; no successful retest is asserted.

Interpretation Three of four account routes are supported. Two of seven stale-feed tests are missing, and the development feed belongs to both sets. These are overlapping control weaknesses under F07, not three separate missing accounts.

Limitations No customer logs were accessed. Record identifiers and outcomes are invented. Native collection is distinct from central availability; configuration evidence alone cannot establish historical completeness or detection effectiveness.

Closure verification A07 closes only after four end-to-end event traces, both missing stale-feed tests and a subsequent review cycle are independently inspected.

XE02 AWS authenticated scan and treatment reconciliation

System and scope Fictional AWS compute inventory and scanner reporting. 24 compute nodes; latest monthly scan cycle; ten customer-service nodes selected for treatment decisions.

Selection Full 24-node coverage reconciliation, with five exception nodes and three overdue treatment records shown. Seven other sampled service nodes meet the fictional treatment requirement.

Authored criterion CL vulnerability criterion: every in-scope node has a current authenticated scan; confirmed applicable internally high flaws are treated within 21 days or carry a current approved exception. Scanner severity alone does not establish exploitability.

Trace E06 to XE02 to F06 / A06. All records are invented.

Record	Scope	Illustrated condition	Decision evidence
node-20	Coverage	Authentication failed	Credential reconciliation open
node-21	Coverage	Authentication failed	Credential reconciliation open
node-22	Coverage	Authentication failed	Credential reconciliation open
node-23	Coverage	No scheduled record	Schedule reconciliation open
node-24	Coverage	No scheduled record	Schedule reconciliation open
svc-03 / vf-03	Treatment sample	High; age 29 days	No current approved exception
svc-06 / vf-06	Treatment sample	High; age 34 days	No current approved exception
svc-09 / vf-09	Treatment sample	High; age 26 days	No current approved exception

XE02 Original technical procedure

1. Join authoritative inventory and scanner exports on immutable node identifiers; retain unmatched inventory nodes instead of dropping them from the denominator.
2. Distinguish a completed unauthenticated scan from authenticated coverage by inspecting credential success and authenticated-check indicators.
3. For the ten selected service nodes, trace first detection, applicability review, internal severity, treatment deadline, change ticket and exception expiry.
4. Corroborate the three overdue records with installed package or image evidence and exposure context before assigning remediation; do not run an exploit.
5. After authorized credential and schedule repairs, run a controlled fresh cycle during a maintenance window and record all 24 authentication outcomes.

Allowed denied and proposed cases

Positive coverage Current authenticated result supports covered status. Illustrated outcome: Nodes 01-19 have authenticated success in the invented cycle.

Negative coverage Authentication failure or absent schedule cannot count as covered. Illustrated outcome: Nodes 20-24 are retained as five coverage exceptions.

Negative treatment An expired or absent exception does not stop the 21-day clock. Illustrated outcome: All three illustrated overdue records lack current approval.

Interpretation Authenticated coverage is 19/24. Three of ten sampled treatment decisions are overdue without current exceptions. The sample does not justify a 30% enterprise vulnerability rate, and coverage exceptions are not added to treatment exceptions as unique assets.

Limitations Illustrated service identifiers are treatment-sample aliases and are not a second population of compute nodes. No CVE, exploitation, breach or universal patch compliance is asserted.

Closure verification A06 requires one fresh complete cycle plus independent reinspection of the three treatment decisions, rollback approval and any remaining time-limited safeguards.

XE03 AWS independent backup copy and portal recovery

System and scope Fictional AWS backup policies and isolated application recovery. Eight protected workloads and three critical services.

Selection All eight copy-policy and recent copy records; all three isolated service restoration records. The service and workload populations are different and are not summed.

Authored criterion CL recovery criterion: an independent copy retains 30 days unless the business approves another duration. The customer portal has a fictional four-hour recovery objective and requires transaction reconciliation and business acceptance, not merely infrastructure startup.

Trace E11; E12 to XE03 to F11; F12 / A11; A12. All records are invented.

Record	Copy retention	Copy result	Recovery acceptance
workload-01 to workload-07	30 days each	Seven successful copy records	Not a business acceptance conclusion
workload-08 internal queue	14 days	Successful copy record	No approved alternative retention decision
service-portal	Underlying copy present	Infrastructure restored in isolated fixture	Record reconciliation and owner acceptance absent
service-identity	Applicable copy present	Isolated restoration record	Business acceptance retained
service-internal-queue	Applicable copy present	Isolated restoration record	Business acceptance retained

XE03 Original technical procedure

1. Inspect source and destination administrative roles and recovery permissions separately; a second storage location alone is not evidence of an independent management boundary.
2. Reconcile eight workload IDs to copy policy, actual copy completion and expiry dates. Retain the queue discrepancy even though its latest copy succeeded.
3. For each service exercise, identify objective, scenario, start event, recovery point, technical availability and business-acceptance time. Do not substitute the technical-start timestamp for usable-service recovery.
4. For a future portal exercise, restore synthetic data to isolation, compare record counts and selected transaction totals, execute an approved user workflow, and capture the business owner decision.
5. Do not reconnect the test environment to production or remove backup records during the illustration.

Allowed denied and proposed cases

Positive retention A 30-day setting and retained-copy history support the selected criterion. Illustrated outcome: Seven policy records retain the intended horizon.

Negative retention A successful 14-day copy does not meet a 30-day requirement without approval. Illustrated outcome: Queue remains an open F12 exception.

Negative business recovery Infrastructure startup alone cannot satisfy business acceptance. Illustrated outcome: Portal remains an open F11 finding; no RTO success is asserted.

Interpretation Copy completion exists for eight of eight workloads; retention conforms for seven of eight. Two of three services have complete business-acceptance records. These are three separate measures and cannot be collapsed into a single recovery score.

Limitations No full failover or destructive restoration occurred. The sample does not establish recoverability of every dependency, an achieved RPO or a production RTO.

Closure verification A11 requires an accepted portal scenario with elapsed-time and reconciliation evidence. A12 requires an approved duration, subsequent retention history and selected restore proof after the observation period.

XE04 Microsoft 365 conditional access and administrative exceptions

System and scope Fictional Entra ID tenant supporting Microsoft 365. 196 enabled member identities including twelve dedicated administrative identities; 22 guests are a separate population.

Selection Full member-policy scope reconciliation; four unsupported exclusions; two separately approved monitored emergency identities; ordinary and privileged control fixtures.

Authored criterion CL identity criterion: every enabled member is covered by the intended MFA design or an approved monitored emergency design. Method registration is not evidence that conditional access requires MFA for the attempted access.

Trace E04 to XE04 to F04 / A04. All records are invented.

Identity fixture	Type	Policy evaluation	Exception decision
MFA-EX-03	Ordinary member	Migration exclusion; MFA requirement not applied	Unsupported
MFA-EX-04	Ordinary member	Migration exclusion; MFA requirement not applied	Unsupported
MFA-EX-01	Dedicated administrator	Migration exclusion; MFA requirement not applied	Unsupported
MFA-EX-02	Dedicated administrator	Migration exclusion; MFA requirement not applied	Unsupported
emg-01	Emergency design	Separate emergency access design	Approved and monitored; not one of four
emg-02	Emergency design	Separate emergency access design	Approved and monitored; not one of four
mem-control	Ordinary member fixture	Intended MFA policy applies	No exception required
adm-control	Administrator fixture	Intended MFA policy applies	No exception required

Configuration illustration

Purpose Show why an enabled MFA policy can exclude the migration group. Displayed JSON is a partial policy projection, not a complete Graph request; symbolic group identifiers replace GUIDs.

Status and boundary Invented pre-change illustration of F04. The expected denial is a future sandbox verification, not a measured result.

Representation Selected Microsoft Graph conditional access policy fields and explanatory fixture

```
{ "displayName": "Require MFA for members", "state": "enabled",
  "conditions": {
    "users": {"includeUsers": ["All"],
      "excludeGroups": ["<migration-group-id>", "<approved-emergency-group-id>"]},
    "applications": {"includeApplications": ["All"]}},
  "grantControls": {"operator": "OR", "builtInControls": ["mfa"]}
}
```

XE04 Configuration interpretation

Fixture: MFA-EX-01 is in migration-group; this policy does not apply.

Future negative case: remove unsupported exclusion; password-only context must not satisfy the required MFA grant. Preserve the approved emergency design.

XE04 Original technical procedure

1. Export the fictional member inventory and reconcile 184 workforce-linked accounts plus twelve dedicated administrator accounts to 196 members; do not add twelve administrators again.
2. Evaluate policy inclusion, exclusion-group membership, grant controls and policy state for the target cloud application and sign-in context. A report-only policy does not enforce denial.
3. Trace each of the four migration exclusions to approval and expiry records. Keep emergency identities in a distinct approved class rather than labeling them as unsupported gaps.
4. Use synthetic sandbox identities to compare ordinary, privileged, excluded and emergency evaluation paths; inspect both policy evaluation and the resulting authorized or denied access.
5. Before proposed exclusion removal, confirm emergency recovery and user communication; no production policy or credential is changed in this report.

Allowed denied and proposed cases

Positive ordinary access A valid MFA context permits the approved application path. Illustrated outcome: Control fixture meets the intended policy.

Negative password-only access A non-emergency member without required MFA should be denied. Illustrated outcome: Unsupported exclusion fixtures illustrate why that requirement is not enforced.

Emergency path Approved monitored recovery access follows its separate design. Illustrated outcome: Two emergency identities remain outside the four unsupported cases.

Interpretation Four of 196 members lack a supported policy decision; two of those four are administrators. The other 192 meet the intended MFA policy or the separately approved emergency design. Four exceptions plus two emergency accounts must not be presented as six unsupported exclusions.

Limitations The invented evaluations are explanatory fixtures, not live sign-in tests. No claim is made about every device condition, application, legacy authentication protocol or guest policy.

Closure verification A04 requires approved policy changes, four-identity reconciliation and positive and denial outcomes. An independent reviewer must inspect policy scope and outcomes, not rely on method-registration screenshots.

XE05 Microsoft 365 collaboration and customer export retention

System and scope Fictional Microsoft 365 collaboration destinations and customer export register. 22 guest identities; six customer export flows across twelve storage locations.

Selection Guest records are used only to illustrate the access boundary; retention decisions cover all six flows and twelve location mappings. Four supported flows occupy nine locations; two unsupported flows occupy three locations.

Authored criterion CL retention criterion: each export flow has a named purpose, accountable owner, approved duration and legal-hold decision before lifecycle automation. Guest invitation or successful access does not establish retention approval.

Trace E14 to XE05 to F14 / A14. All records are invented.

Record	Destination mapping	Purpose and duration decision	Illustrated access boundary
flow-01 to flow-04	loc-01 to loc-09	Four approved decisions	Owner-controlled collaboration scope
flow-05	loc-10 and loc-11	No approved purpose or duration	Guest-enabled collaboration does not cure gap
flow-06	loc-12	No approved purpose or duration	Internal access does not cure gap
guest-control	One synthetic guest from separate 22-guest inventory	Not a retention decision	Authorized only to designated test workspace
guest-negative	Same synthetic guest	Not a retention decision	Unrelated test workspace denies access

XE05 Original technical procedure

1. Reconcile processing-flow IDs to the twelve storage-location IDs; count flows and locations separately so two missing decisions are not reported as five separate gaps.
2. Inspect purpose, owner, duration, contractual requirements and hold authority for each flow. Route legal interpretation to counsel rather than infer a lawful basis from configuration.
3. Compare a Microsoft 365 site or library retention setting to the approved flow decision; preserve distinction between configured retention, deletion eligibility and legal hold.
4. For proposed closure, place synthetic objects into an isolated test workspace, exercise the configured expiry path and the hold-preservation path, and record event timestamps.
5. Use one synthetic guest fixture to demonstrate authorized workspace access and denied unrelated-workspace access; do not infer a complete guest-access review from this boundary illustration.

Allowed denied and proposed cases

Positive boundary A guest may access only the specifically authorized test workspace. Illustrated outcome: Access fixture permits the designated workspace and denies an unrelated workspace.

Negative approval A technically configured lifecycle rule without a business decision is insufficient. Illustrated outcome: Flows 05 and 06 remain open under F14.

Proposed hold retest A held synthetic object is preserved while an eligible unheld object follows approved expiry. Illustrated outcome: Future A14 verification; no production deletion or completed retest claimed.

Interpretation The observed retention gap remains two of six flows across three of twelve locations. The guest fixture adds technical explanation, not a new finding or a claim that all 22 guests have been certified.

Limitations The original case does not establish tenant-wide Exchange rules, consent grants, guest expiry or every Microsoft 365 workload. Those are explicit follow-on scoping considerations, not invented passed tests. Legal retention conclusions remain outside this readiness illustration.

Closure verification A14 closes only with the two approved decisions, aligned lifecycle records and isolated expiry-and-hold results reviewed by the privacy lead and an independent verifier.

XE06 Application security gates and CI CD deployment trust

System and scope Fictional source repositories, delivery pipelines and AWS deployment role. Eight repositories, six pipelines and eight sampled releases from the quarter; two applications.

Selection All repository protection settings and pipeline log availability; eight release decisions. A separate synthetic role-trust fixture explains the desired deployment boundary without asserting a new observed trust flaw.

Authored criterion CL release criterion: protected changes require independent review; internally high security findings must be resolved or carry an authorized expiring exception before release. The desired deployment role accepts only the approved repository, protected reference and audience.

Trace E10 to XE06 to F10 / A10. All records are invented.

Record	Security decision	Protection or gate result	Trace
repo-01 to repo-06	Required reviewer configured	Six protected repositories	Repository-rule fixture
repo-07 and repo-08	Required protection absent	Two unprotected repositories	F10 repository exceptions
release-02	Unresolved internal high issue; no current approval	Released with advisory security result	Pipeline log linked to release
release-05	Unresolved internal high issue; no current approval	Released with advisory security result	Pipeline log linked to release
release-07	Unresolved internal high issue; no current approval	Released with advisory security result	Pipeline log linked to release
Other five sampled releases	Issue resolved or approved exception	Supported risk decision	Five decision records
trust-design-01	Audience sts.amazonaws.com; subject repo:cedarline-sample/portal:ref:refs/heads/main	Desired scoped trust fixture only	No observed trust-pass claim

XE06 Configuration illustration

Purpose Demonstrate exact OIDC audience and subject constraints plus a fail-closed release decision. This is a proposed design fixture, not the observed historical configuration.

Status and boundary Desired future design only; excluded from observed PASS counts. The 111122223333 account ID is an illustrative placeholder, not a deployment target. The fictional repository predates July 2026 and has not opted into immutable subject claims; inspect the actual emitted subject before implementation. This reference-subject example assumes a protected main branch and no job environment subject; an environment-based job needs a different subject and environment branch restrictions. Do not deploy it.

Representation IAM trust policy JSON and non-executable release-gate pseudocode

```
{ "Version": "2012-10-17", "Statement": [{
  "Effect": "Allow",
  "Principal": {"Federated":
    "arn:aws:iam::111122223333:oidc-provider/token.actions.githubusercontent.com"},
  "Action": "sts:AssumeRoleWithWebIdentity",
  "Condition": {"StringEquals": {
    "token.actions.githubusercontent.com:aud": "sts.amazonaws.com",
    "token.actions.githubusercontent.com:sub":
      "repo:cedarline-sample/portal:ref:refs/heads/main"
  }}}] }
# Non-executable gate pseudocode; all conditions must hold
allow_release = scan_completed AND artifact_digest_matches
                AND independent_approval_valid
                AND (unresolved_high_count == 0 OR exception_current_and_authorized)
# Missing/failed scan, expired exception, wrong digest or absent approval => DENY
# Wrong OIDC audience/repository/reference => DENY role assumption
# Fork/pull-request validation never receives production deployment credentials
```

XE06 Original technical procedure

1. Join release ID to commit, repository, pipeline run, artifact digest and approval record; retain failed security-job output rather than treating a completed build as security acceptance.
2. For each sampled release, trace unresolved internally high findings to triage, disposition, approving authority and expiry at the release timestamp.
3. Inspect repository rules for required reviews, protected references and bypass permissions; reconcile two missing repository protections to the eight-repository denominator.
4. For a future sandbox gate test, submit a benign synthetic high-finding fixture without an exception; the release must stop. Repeat with the issue resolved or a current authorized exception and retain both outcomes.
5. Review the proposed deployment role trust for exact audience and repository/reference conditions, least-privilege permissions and separation of untrusted pull-request jobs from deployment credentials. Demonstrate deny for a wrong subject using a local policy fixture, never a stolen token.

Allowed denied and proposed cases

Negative release gate Unapproved internal high issue prevents release. Illustrated outcome: The existing three release fixtures show the intended gate was advisory; they do not demonstrate successful enforcement.

Positive closure fixture A resolved issue or approved unexpired exception permits an otherwise authorized release. Illustrated outcome: Proposed A10 retest, not completed remediation.

Negative trust design Wrong repository, branch or audience cannot obtain the deployment role. Illustrated outcome: Desired isolated policy-fixture result; not counted as an observed historical pass.

Interpretation Six of eight repositories have intended protection, and three of eight sampled releases lack an authorized decision for an unresolved high issue. All six pipelines produce traceable logs, but log existence does not establish gate enforcement. The trust example adds the technical design and verification boundary; it is not a seventeenth finding.

Limitations No exploitability, breached release, complete code review or universal software assurance is asserted. The AWS trust example is a proposed design fixture and must not enter the observed control-results denominator.

Closure verification A10 requires both protected-repository corrections, three issue decisions and approved and denied benign release demonstrations. Engineering and security reviewers verify digest traceability and bypass restrictions independently of the implementer.

XE07 Production change approval and rollback trace

System and scope Fictional application release and change-management records. 18 production changes in the quarter; ten judgmentally selected changes.

Selection Three selected changes without independent prior approval; two of those also lack rollback-validation evidence. Seven other selected changes retain independent approval.

Authored criterion CL change criterion: an approver independent of the deployer authorizes the change before production deployment; rollback is validated or a time-bounded exception is approved. Emergency processing needs explicit authorization and retrospective review.

Trace E09 to XE07 to F09 / A09. All records are invented.

Change	Prior independent approval	Rollback evidence	Unique exception status
chg-03	Absent	Absent	Approval and rollback gap
chg-06	Absent	Absent	Approval and rollback gap
chg-09	Absent	Retained	Approval gap only
Other seven selected changes	Retained before deployment	No additional deficiency asserted	Approval criterion supported

XE07 Original technical procedure

1. Reconcile 18 registered changes to the selection rationale and ten selected IDs; do not silently remove emergency changes from the sample.
2. Compare approver identity and timestamp to deployer identity and actual deployment timestamp; a ticket closed after deployment does not prove prior approval.
3. For chg-03 and chg-06, seek versioned rollback instructions, test environment, expected recovery result and recorded validation. Absence of the record is not proof that a rollback was attempted and failed.
4. Trace an emergency change through named authorization, reason, compensating safeguards and retrospective review due date.
5. For proposed closure, use a synthetic application version in isolation to apply and reverse a change, reconcile data and artifact version, and have a reviewer other than the implementer inspect the result.

Allowed denied and proposed cases

Positive sequence Independent approval timestamp precedes deployment. Illustrated outcome: Seven sampled changes have the required sequence.

Negative sequence A later approval cannot retrospectively become prior authorization. Illustrated outcome: Three sampled changes remain exceptions.

Rollback closure The previous version and synthetic data reconcile after reversal. Illustrated outcome: Future verification for the two missing records; no successful rollback is invented.

Interpretation Three of ten sampled changes are uniquely deficient; the two rollback gaps are within those three. Adding three and two would double-count exceptions. This sample does not support a 30% exception estimate for all 18 changes.

Limitations A missing rollback record is an assurance gap rather than evidence of an actual failed recovery. No production application was changed or reversed.

Closure verification A09 requires corrected workflow and decision records, the two rollback validations and subsequent ordinary and emergency changes demonstrating approval timing and independent review.

XE08 Bounded AI pilot release and repeatable evaluation

System and scope Fictional internal drafting assistant using synthetic service tickets. One pilot, twelve users and twenty synthetic drafts.

Selection All twenty draft reviews and the pilot charter; three drafts with unsupported operational details. Human reviewers corrected all three before use.

Authored criterion CL AI criterion: keep the pilot synthetic-only until an accountable risk approver accepts the release boundary; define error categories and acceptance criteria before evaluation and repeat the versioned corpus after material changes.

Trace E15; E16 to XE08 to F15; F16 / A15; A16. All records are invented.

Record	Observed outcome	Review action	Decision gap
draft-04	Unsupported operational detail	Corrected before use	No predeclared acceptance rule
draft-11	Unsupported operational detail	Corrected before use	No predeclared acceptance rule
draft-17	Unsupported operational detail	Corrected before use	No predeclared acceptance rule
Other seventeen drafts	No unsupported operational detail recorded in selected review	Human review retained	Not proof of future reliability
pilot-charter	Technical owner named	Synthetic-only restriction stated	Residual-risk approver not assigned
model-change-request fixture	Proposed model change	Should trigger reevaluation and approval	Desired workflow, not completed decision

XE08 Original technical procedure

1. Record the pilot use, allowed synthetic inputs, excluded operational uses and named technical owner; confirm that expanded data or autonomous actions are not silently included.
2. Reconcile twenty draft IDs to source tickets, reviewer corrections and review timestamps. Count three affected drafts rather than every corrected word as a separate failure.
3. Define a versioned test corpus with expected facts, prohibited disclosures and unsupported-detail categories before the next run; set acceptance and escalation criteria with the risk approver.
4. For future evaluation, include ordinary cases and adversarially phrased synthetic tickets, record model version and configuration, and preserve failures rather than averaging away unacceptable errors.
5. Trace a hypothetical material model change to the approver and block expansion until data, provider, impact and evaluation decisions are complete.

Allowed denied and proposed cases

Observed safeguard Human review corrects identified unsupported details before use. Illustrated outcome: All three affected draft fixtures were corrected.

Negative governance Technical ownership alone is not residual-risk acceptance. Illustrated outcome: No signed release-risk decision exists under F15.

Proposed change gate Material model change cannot bypass versioned evaluation and approval. Illustrated outcome: Future A15/A16 verification; no reliability forecast or completed approval asserted.

Interpretation Three of twenty reviewed drafts required correction. That descriptive sample proportion is not a production error rate, model-accuracy estimate or safety certification. Human review operated in the limited case while repeatable acceptance criteria remained absent.

Limitations No real ticket data, automated operational decisions or provider model internals are assessed. This is bounded AI governance evidence, not a conformity assessment or technical model validation.

Closure verification A15 establishes authority and a signed release or stop decision. A16 then requires versioned criteria, corpus, reviewer calibration, repeatable results and explicit handling of unresolved errors.

Compliance & Control Gap Matrix

Selected context mappings are not equivalent controls or a compliance opinion. CL criteria and fixtures are authored for this fictional boundary. The result, evidence and finding identifiers preserve traceability.

Check and context	Outcome and observed condition	Trace
T01-01 PM-09; CA-05	PARTIAL Five of 12 exceptions lack an expiry; three of those five also lack a sponsor decision. This is five unique deficient exception records, not eight incidents.	E01 F01
T01-02 PM-01; PL-02	PARTIAL Two responsibility records name a team but no accountable individual: cloud evidence retention and supplier-assisted recovery. Six records identify an individual and backup.	E02 F02
T01-03 PM-01	PASS The charter records the executive sponsor and quarterly review cadence.	E17 No finding
T01-04 PM-03	PASS Four of four selected security requests retain a dated sponsor decision.	E17 No finding
T01-05 CA-05	PASS A synthetic request with a past expiry is rejected in the sample workflow fixture.	E17 No finding
T01-06 CA-05	PASS A synthetic request with owner, sponsor and future expiry enters the approved state.	E17 No finding
T02-01 AC-02; PS-04	PARTIAL Three of 11 workforce accounts did not meet the internal 24-hour removal target. Two were disabled after 41 and 63 hours; one account remained enabled at the 30 September cut-off. No use after departure is asserted.	E03 F03
T02-02 IA-02; AC-06	PARTIAL Four member accounts are excluded from the intended MFA policy without a current exception. Two are dedicated administrative identities. The two monitored emergency identities are separately approved and are not part of these four exceptions.	E04 F04
T02-03 AC-05	PASS Six of six selected access requests retain an approver different from the requester.	E18 No finding
T02-04 IA-02	PASS Both emergency identities have monitored usage and current approved purpose.	E18 No finding
T02-05 AC-03	PASS A synthetic ordinary-user request for a restricted admin role is rejected by the fixture.	E18 No finding
T02-06 AC-03	PASS A synthetic approved role request enters the expected provision queue.	E18 No finding

All outcomes are fictional. PASS applies only to each selected check. The data source retains exact criteria and exclusions.

Selected control checks continued 2

Selected context mappings are not equivalent controls or a compliance opinion. CL criteria and fixtures are authored for this fictional boundary. The result, evidence and finding identifiers preserve traceability.

Check and context	Outcome and observed condition	Trace
T03-01 CM-08; CM-06	PARTIAL Six of 184 laptops lack a current business owner. In the 30-laptop sample, four reported encryption-profile exceptions and three protection-policy exceptions overlap on two laptops: five unique sample devices have at least one setting exception.	E05 F05
T03-02 RA-05; SI-02	PARTIAL 19 of 24 nodes report authenticated scanning; three report authentication failure and two lack a scheduled record. Three of the 10 sampled service nodes have internally rated high flaws older than the fictional 21-day treatment target without a current exception.	E06 F06
T03-03 SI-03	PASS All 30 selected laptops report the managed endpoint agent.	E19 No finding
T03-04 CM-08	PASS All 24 cloud compute nodes map to current service owners.	E19 No finding
T03-05 CM-06	PASS A synthetic device failing the approved posture rule is denied the test service route.	E19 No finding
T03-06 CM-06	PASS A synthetic compliant device receives the intended test route.	E19 No finding
T04-01 AU-02; AU-06; AU-12	PARTIAL Three of four cloud accounts have central management-event delivery. The development account retains native events but lacks central delivery. Two of seven priority feeds lack a tested stale-feed alert; one is the development account, so the sets overlap.	E07 F07
T04-02 IR-04; IR-08	PARTIAL Two of six exercise decisions lack a named approver: temporary suspension of supplier data flow and customer notification authorization. Four decisions identify an accountable role and alternative contact.	E08 F08
T04-03 AU-12	PASS All four account snapshots show native management-event logging.	E20 No finding
T04-04 IR-08	PASS Six of six fictional role interviews identify the incident channel; statements are corroborated by the distributed plan.	E20 No finding
T04-05 IR-04	PASS A synthetic incident case with no owner is held for triage instead of marked complete.	E20 No finding
T04-06 IR-04	PASS A synthetic case with the required triage owner follows the approved escalation route.	E20 No finding

All outcomes are fictional. PASS applies only to each selected check. The data source retains exact criteria and exclusions.

Selected control checks continued 3

Selected context mappings are not equivalent controls or a compliance opinion. CL criteria and fixtures are authored for this fictional boundary. The result, evidence and finding identifiers preserve traceability.

Check and context	Outcome and observed condition	Trace
T05-01 CM-03; CM-04	PARTIAL Three of 10 sampled changes lack independent approval before deployment. Two of those three also lack recorded rollback validation. These are three unique deficient changes, not five.	E09 F09
T05-02 SA-11; SI-02	PARTIAL Six of eight repositories have the intended branch protection. Three of eight sampled releases contain unresolved internal high security findings without an authorized expiring exception. No exploitability or breach is inferred.	E10 F10
T05-03 SA-11	PASS All six pipeline configurations retain source, job and artifact references.	E21 No finding
T05-04 CM-03	PASS All 10 sampled changes identify a deployer and ticket.	E21 No finding
T05-05 CM-03	PASS A benign synthetic deploy request lacking environment approval is rejected by the test fixture.	E21 No finding
T05-06 CM-03	PASS The same synthetic request with the expected approval follows the authorized path.	E21 No finding
T06-01 CP-04; CP-10	PARTIAL Two of three services retain a complete restore and business-acceptance record. The customer portal has infrastructure restore evidence but no reconciliation or business-owner sign-off against its fictional four-hour recovery objective.	E11 F11
T06-02 CP-09	PARTIAL Seven of eight workloads have an independent copy with the fictional 30-day retention setting. The internal queue has a 14-day copy retention setting without an approved business decision. Copy success exists for all eight workloads.	E12 F12
T06-03 CP-09	PASS All eight protected workloads retain a recent successful copy record.	E22 No finding
T06-04 CP-09	PASS A synthetic workload-admin delete request is denied in the recovery-permission fixture.	E22 No finding
T06-05 CP-10	PASS A synthetic recovery operator receives the intended read and restore permissions.	E22 No finding
T06-06 CP-04	NOT ASSESSED No end-to-end business failover evidence was created or assessed.	No evidence; outside assessment No finding

All outcomes are fictional. PASS applies only to each selected check. The data source retains exact criteria and exclusions.

Selected control checks continued 4

Selected context mappings are not equivalent controls or a compliance opinion. CL criteria and fixtures are authored for this fictional boundary. The result, evidence and finding identifiers preserve traceability.

Check and context	Outcome and observed condition	Trace
T07-01 SR-03; SA-09	PARTIAL Two of five critical-provider files contain current assurance reports but no recorded review of customer responsibilities or relevant exceptions. The other three retain reviewer decisions.	E13 F13
T07-02 SI-12; PT-03	PARTIAL Two of six flows lack an approved retention purpose and duration. Three of 12 storage locations carry those two flows. No lawful basis or legal retention conclusion is made from these records.	E14 F14
T07-03 SA-09	PASS All five critical providers retain signed agreements and a contract owner.	E23 No finding
T07-04 AC-03	PASS A synthetic request outside the approved support role is denied access to the test export.	E23 No finding
T07-05 AC-03	PASS A synthetic authorized support identity reads the intended test export.	E23 No finding
T07-06 PT-06	NOT APPLICABLE Not applicable to the declared private-company scenario; no federal system-of-records obligation is selected.	E23 No finding
T08-01 AI RMF GOVERN 1; MANAGE 1	NOT IMPLEMENTED The pilot charter identifies a technical owner but contains no accountable approver for residual AI risk or material model changes. No signed release risk decision exists. The pilot is limited to synthetic ticket data and draft notes.	E15 F15
T08-02 AI RMF MEASURE 2; MANAGE 2	PARTIAL Three of 20 drafts contain an unsupported operational detail requiring correction. Reviewers corrected all three before use, but no predeclared acceptance threshold, repeatable test set or model-change retest rule exists.	E16 F16
T08-03 AI RMF MANAGE 2	PASS A synthetic assistant action requesting customer-send permission is denied by the bounded pilot fixture.	E24 No finding
T08-04 AI RMF GOVERN 3	PASS A synthetic draft remains a draft and enters the human reviewer queue.	E24 No finding
T08-05 AI RMF MAP 1	NOT APPLICABLE Not applicable: the pilot performs no lending, eligibility or autonomous decision activity.	E24 No finding
T08-06 AI RMF MEASURE 2	NOT ASSESSED Training datasets and underlying model weights were not available or assessed.	No evidence; outside assessment No finding

All outcomes are fictional. PASS applies only to each selected check. The data source retains exact criteria and exclusions.

NIST family workpaper coverage

This family view covers selected objectives in all 20 NIST SP 800-53 control families. Each family contains three original tests with a stated criterion, population, procedure and invented result. This is broad family coverage, not examination of every control or enhancement.

The original 48 T-series domain checks remain intact. The 60 W-series tests deliberately revisit some of the same records from a family perspective and add bounded supporting illustrations. They must not be summed into 108 independent observations. Passing a fixture is not proof of live operation.

Family result counts PARTIAL: 21; PASS: 39. Counts describe selected tests only; there is no compliance percentage.

Family	Name	Workpaper tests	Pages
AC	Access Control	W-AC-01, W-AC-02, W-AC-03	52 to 53
AT	Awareness and Training	W-AT-01, W-AT-02, W-AT-03	54 to 55
AU	Audit and Accountability	W-AU-01, W-AU-02, W-AU-03	56 to 57
CA	Assessment Authorization and Monitoring	W-CA-01, W-CA-02, W-CA-03	58 to 59
CM	Configuration Management	W-CM-01, W-CM-02, W-CM-03	60 to 61
CP	Contingency Planning	W-CP-01, W-CP-02, W-CP-03	62 to 63
IA	Identification and Authentication	W-IA-01, W-IA-02, W-IA-03	64 to 65
IR	Incident Response	W-IR-01, W-IR-02, W-IR-03	66 to 67
MA	Maintenance	W-MA-01, W-MA-02, W-MA-03	68 to 69
MP	Media Protection	W-MP-01, W-MP-02, W-MP-03	70 to 71
PE	Physical and Environmental Protection	W-PE-01, W-PE-02, W-PE-03	72 to 73
PL	Planning	W-PL-01, W-PL-02, W-PL-03	74 to 75
PM	Program Management	W-PM-01, W-PM-02, W-PM-03	76 to 77
PS	Personnel Security	W-PS-01, W-PS-02, W-PS-03	78 to 79
PT	Personally Identifiable Information Processing and Transparency	W-PT-01, W-PT-02, W-PT-03	80 to 81
RA	Risk Assessment	W-RA-01, W-RA-02, W-RA-03	82 to 83
SA	System and Services Acquisition	W-SA-01, W-SA-02, W-SA-03	84 to 85
SC	System and Communications Protection	W-SC-01, W-SC-02, W-SC-03	86 to 87
SI	System and Information Integrity	W-SI-01, W-SI-02, W-SI-03	88 to 89
SR	Supply Chain Risk Management	W-SR-01, W-SR-02, W-SR-03	90 to 91

Each family workpaper retains its explicit limitation. Supporting evidence records are listed in the expanded Evidence and Control Review Register. Finding and action identifiers refer to the original 16 findings and 16 planned actions.

AC Access Control workpaper

Selection rationale Customer workflows and administrative routes require accountable least privilege; workforce and service identities have different purposes.

W-AC-01 Verify departure disablement

Control context AC-2. Result: PARTIAL.

Authored criterion CL-03 internal 24-hour departure target

Population and sample 11 quarter departures. Sample: All 11 HR events reconciled to effective access records

Original assessment procedure

1. Match immutable identity keys between HR and directory
2. Compute elapsed event-to-disable time using UTC
3. Inspect active sessions and owner decisions for each late record

Expected 11 of 11 removed within 24 hours or explicitly approved exception

Observed fictional result Eight timely; two disabled at 41 and 63 hours; one enabled at cut-off. No post-departure misuse asserted.

Evidence and finding trace E03; F03.

Gap Three of 11 workforce accounts did not meet the internal 24-hour removal target. Two were disabled after 41 and 63 hours; one account remained enabled at the 30 September cut-off. No use after departure is asserted.

Proposed treatment Resolve the remaining account with the business owner, revoke sessions where required and implement a same-day HR trigger with an independent reconciliation.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-AC-02 Check independent privilege approval

Control context AC-5; AC-6. Result: PASS.

Authored criterion CL-W-AC-02 requester cannot approve own privilege

Population and sample Six selected access requests from quarter log. Sample: Judgmental: two ordinary, two support and two administrative requests

Original assessment procedure

1. Compare requester and approver identifiers
2. Trace approved role to provisioned role export
3. Check grant timestamp follows approval

Expected All six requests have an approver different from the requester, and no grant exceeds the approved role.

Observed fictional result AR01-AR06 each have distinct approver and matching role; all six approvals precede grant.

Evidence and finding trace WE-AC-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-AC-03 Verify object-level customer separation

Control context AC-3. Result: PASS.

Authored criterion CL-W-AC-03 support scope cannot cross tenant boundary

Population and sample Two applications and two synthetic tenant identities. Sample: Both applications; four allowed/denied object requests

Original assessment procedure

1. Assign fixtures tenant A and B with separate records
2. Describe read of own record and another tenant record
3. Compare returned payload and denial log to expected scope

Expected Two own-tenant reads allowed; two cross-tenant reads denied without payload

Observed fictional result Portal and queue each allow own-tenant fixture and return access denied for the other tenant; four of four outcomes match.

Evidence and finding trace WE-AC-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

AT Awareness and Training workpaper

Selection rationale Personnel handle customer records and privileged staff need role-specific practices beyond an annual completion percentage.

W-AT-01 Reconcile security learning coverage

Control context AT-2. Result: PASS.

Authored criterion CL-W-AT-01 the declared 184-person learning roster has current annual core-course completion.

Population and sample The declared learning roster of 184 people: 168 employees and 16 contractors. This denominator is not a conclusion that every enabled account is currently authorized. Sample: Full roster join; identity counts exclude 12 separate admin accounts

Original assessment procedure

1. Join learning records to the 184-person roster, not the 196 enabled member identities.
2. Check completion date and current course version
3. Investigate unmatched or duplicate person keys

Expected 184 unique people have current completion

Observed fictional result 168 employee and 16 contractor records complete course SEC26 before 30 September; no duplicates in person-key join.

Evidence and finding trace WE-AT-01; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-AT-02 Check role-specific administrator learning

Control context AT-3. Result: PASS.

Authored criterion CL-W-AT-02 privileged custodians complete recovery and access modules

Population and sample 12 dedicated administrative identities. Sample: All 12 identity-to-custodian links; six fictional custodians each hold two identities

Original assessment procedure

1. Resolve each admin identity to accountable person
2. Check role module completion precedes privilege renewal
3. Inspect one knowledge-check response per custodian

Expected Six custodians current and all 12 identities attributable

Observed fictional result ADM01-ADM12 map two each to C01-C06; all six completed IAM26 and REC26 before renewal and retained passing knowledge checks.

Evidence and finding trace WE-AT-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-AT-03 Verify training-record integrity

Control context AT-4. Result: PASS.

Authored criterion CL-W-AT-03 completion corrections require traceable reason and approver

Population and sample Quarter training ledger and two corrections. Sample: Both correction entries, with original and revised states

Original assessment procedure

1. Locate original completion timestamp
2. Trace correction reason and independent approval
3. Confirm ledger retains old value rather than overwriting history

Expected Two corrections preserve original value and authorization

Observed fictional result TRC01 corrects person-key merge; TRC02 corrects course import date; both retain prior values and learning-owner approval.

Evidence and finding trace WE-AT-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

AU Audit and Accountability workpaper

Selection rationale Distributed cloud and application events must support incident reconstruction without confusing native retention with central collection.

W-AU-01 Reconcile central account event delivery

Control context AU-2; AU-12. Result: PARTIAL.

Authored criterion CL-07 every declared cloud account centrally delivers priority management events

Population and sample Four cloud accounts. Sample: All four account configurations and one event path per account

Original assessment procedure

1. Match account inventory to delivery configuration
2. Trace source event identifier into central destination
3. Record native retention separately from central availability

Expected Four central paths proven

Observed fictional result Three central paths present; development retains native events but no central delivery.

Evidence and finding trace E07; F07.

Gap Three of four cloud accounts have central management-event delivery. The development account retains native events but lacks central delivery. Two of seven priority feeds lack a tested stale-feed alert; one is the development account, so the sets overlap.

Proposed treatment Add central delivery for the development account and test controlled stale-feed alerts for both affected sources; reconcile account onboarding and daily review records.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-AU-02 Check scheduled event-review evidence

Control context AU-6. Result: PARTIAL.

Authored criterion CL-W-AU-02 daily priority review retains reviewer and disposition

Population and sample 10 working days of review records. Sample: All 10 days in defined review window

Original assessment procedure

1. Enumerate expected days using review calendar
2. Locate reviewer timestamp and disposition for each day
3. Reconcile missing days with approved exception record

Expected 10 dated reviews or approved exception

Observed fictional result Eight of 10 days retain review and escalation records; absence for two days remains an evidence gap, not proof that review never occurred.

Evidence and finding trace E07; F07.

Gap Three of four cloud accounts have central management-event delivery. The development account retains native events but lacks central delivery. Two of seven priority feeds lack a tested stale-feed alert; one is the development account, so the sets overlap.

Proposed treatment Add central delivery for the development account and test controlled stale-feed alerts for both affected sources; reconcile account onboarding and daily review records.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-AU-03 Verify log-store write and delete separation

Control context AU-9. Result: PASS.

Authored criterion CL-W-AU-03 workload roles cannot alter central retained logs

Population and sample Central log-store policy and two synthetic role requests. Sample: One authorized ingest and one unauthorized delete request

Original assessment procedure

1. Read allow and explicit-deny policy statements
2. Evaluate delivery-role write fixture
3. Evaluate workload-admin delete fixture and check denial record

Expected Delivery writes permitted; workload deletion denied

Observed fictional result ING-AU01 accepts signed delivery; DEL-AU01 denies workload administrator deletion; policy version LOG26 retained.

Evidence and finding trace WE-AU-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

CA Assessment Authorization and Monitoring workpaper

Selection rationale Management needs traceable treatment decisions and repeatable checks, not a compliance percentage detached from evidence.

W-CA-01 Check exception expiry and sponsorship

Control context CA-5. Result: PARTIAL.

Authored criterion CL-01 retained exception requires owner sponsor safeguard and expiry

Population and sample 12 open exceptions. Sample: All 12 register records

Original assessment procedure

1. Check required fields against approved template
2. Count unique deficient records rather than missing fields
3. Trace overdue records to sponsor review

Expected 12 complete current decisions

Observed fictional result Five missing expiry; three of those also missing sponsor decision: five unique deficient records.

Evidence and finding trace E01; F01.

Gap Five of 12 exceptions lack an expiry; three of those five also lack a sponsor decision. This is five unique deficient exception records, not eight incidents.

Proposed treatment Require owner, reason, safeguard, sponsor decision and expiry for each retained exception; reconcile the five records and route overdue items to the sponsor.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-CA-02 Verify monitoring responsibilities

Control context CA-7. Result: PASS.

Authored criterion CL-W-CA-02 selected recurring checks have owner cadence and evidence destination

Population and sample Four monitoring schedules for access scan logging and backup. Sample: All four schedule records; one completed occurrence each

Original assessment procedure

1. Match schedule to accountable owner
2. Check run date lies within specified cadence
3. Trace output reference to retained completion record

Expected Four schedules and occurrences traceable

Observed fictional result MON01 access monthly; MON02 scan monthly; MON03 logging daily; MON04 backup daily each retain owner and one occurrence. This proves scheduling not complete effective coverage.

Evidence and finding trace WE-CA-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-CA-03 Check independent assessment follow-through

Control context CA-2. Result: PASS.

Authored criterion CL-W-CA-03 scoped review workpapers record preparer reviewer and exceptions

Population and sample Three fictional completed prior review workpapers. Sample: Access approval, backup permissions and contract ownership reviews

Original assessment procedure

1. Inspect approved review scope and criteria
2. Compare preparer and reviewer identities
3. Trace review comments to documented resolution

Expected Three reviews independently signed and exceptions traceable

Observed fictional result REV01-REV03 show different preparer/reviewer roles and closed editorial comments; no claim that present open findings are closed.

Evidence and finding trace WE-CA-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

CM Configuration Management workpaper

Selection rationale Inventory accuracy and controlled change are prerequisites for operating customer workflows safely.

W-CM-01 Reconcile laptop ownership and protection

Control context CM-8; CM-6. Result: PARTIAL.

Authored criterion CL-05 current owner and approved device settings

Population and sample 184 laptops; 30 selected protection records. Sample: Full ownership inventory; 30 risk-based endpoints

Original assessment procedure

1. Join asset and directory identifiers
2. Compare protection status to approved baseline
3. Deduplicate overlapping exceptions by device key

Expected 184 owners; 30 devices meet both settings or current exception

Observed fictional result Six unowned; four encryption and three protection exceptions overlap on two: five unique deficient sample devices.

Evidence and finding trace E05; F05.

Gap Six of 184 laptops lack a current business owner. In the 30-laptop sample, four reported encryption-profile exceptions and three protection-policy exceptions overlap on two laptops: five unique sample devices have at least one setting exception.

Proposed treatment Reconcile six owner records and five unique sample devices; record current policy outcomes and approved time-limited exceptions where treatment is deferred.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-CM-02 Check production approval and rollback

Control context CM-3; CM-4. Result: PARTIAL.

Authored criterion CL-09 independent authorization and evidenced rollback

Population and sample 18 production changes; 10 selected. Sample: Judgmental ordinary and emergency changes across two applications

Original assessment procedure

1. Compare approval timestamp with deployment
2. Confirm approver differs from deployer
3. Inspect rollback validation and reconcile overlapping gaps

Expected 10 prior approvals and rollback records

Observed fictional result Three lack independent prior approval; two of those also lack rollback validation; three unique deficient changes.

Evidence and finding trace E09; F09.

Gap Three of 10 sampled changes lack independent approval before deployment. Two of those three also lack recorded rollback validation. These are three unique deficient changes, not five.

Proposed treatment Enforce ordinary independent approval; define emergency authorization and retrospective review; validate rollback for the two identified changes before the next related release.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-CM-03 Verify versioned configuration baselines

Control context CM-2. Result: PASS.

Authored criterion CL-W-CM-03 approved baseline version maps to each node role

Population and sample 24 cloud nodes and three node-role templates. Sample: All 24 node-to-role mappings; all three template approvals

Original assessment procedure

1. Join compute inventory to role template
2. Verify template version has approved change
3. Compare approved version to declared expected state not live conformity

Expected 24 nodes have an approved target baseline

Observed fictional result WEB26 covers 8 nodes; WORK26 covers 10; MGMT26 covers 6; all three templates approved. Baseline availability does not negate scan gaps.

Evidence and finding trace WE-CM-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

CP Contingency Planning workpaper

Selection rationale Recovery must demonstrate accepted business outcomes and retained copies rather than backup-job success alone.

W-CP-01 Check business restore acceptance

Control context CP-4; CP-10. Result: PARTIAL.

Authored criterion CL-11 critical service exercise includes business validation

Population and sample Three critical services. Sample: One isolated restore record for each service

Original assessment procedure

1. Read service recovery objective
2. Trace platform restore to transaction reconciliation
3. Check business-owner acceptance and elapsed time

Expected Three accepted service outcomes

Observed fictional result Two complete; portal lacks reconciliation and business sign-off against four-hour objective.

Evidence and finding trace E11; F11.

Gap Two of three services retain a complete restore and business-acceptance record. The customer portal has infrastructure restore evidence but no reconciliation or business-owner sign-off against its fictional four-hour recovery objective.

Proposed treatment Agree portal transaction reconciliation and user acceptance, perform an isolated restore with synthetic data and record elapsed time and the business decision.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-CP-02 Check independent copy retention

Control context CP-9. Result: PARTIAL.

Authored criterion CL-12 default 30 days unless documented business decision

Population and sample Eight protected workloads. Sample: All eight policies and copy histories

Original assessment procedure

1. Compare approved retention to policy
2. Identify isolated or independent-copy boundary
3. Inspect recent success separately from retention horizon

Expected Eight approved retention decisions reflected in policy

Observed fictional result Seven workloads retain 30-day copies; the internal queue retains 14-day copies without an approved decision. All eight recent copy jobs succeed.

Evidence and finding trace E12; F12.

Gap Seven of eight workloads have an independent copy with the fictional 30-day retention setting. The internal queue has a 14-day copy retention setting without an approved business decision. Copy success exists for all eight workloads.

Proposed treatment Obtain the business retention decision, update the queue policy if required and review the next retention cycle with the recovery owner.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-CP-03 Verify recovery contact usability

Control context CP-2. Result: PASS.

Authored criterion CL-W-CP-03 critical-service runbooks have primary deputy and offline contact route

Population and sample Three critical-service runbooks. Sample: All three contact sections; synthetic primary-unavailable call tree

Original assessment procedure

1. Check role-to-person contact mapping
2. Describe primary unavailable handoff
3. Confirm deputy can locate runbook through approved alternate route

Expected Three deputy routes resolve

Observed fictional result RC01 portal, RC02 identity service and RC03 internal queue each identify a primary, deputy and controlled offline contact copy; all three fictional handoffs resolve.

Evidence and finding trace WE-CP-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

IA Identification and Authentication workpaper

Selection rationale Separate identity registration, policy enforcement and emergency-access design to avoid misleading MFA coverage claims.

W-IA-01 Evaluate enforced MFA scope

Control context IA-2. Result: PARTIAL.

Authored criterion CL-04 intended users require MFA or approved monitored emergency design

Population and sample 196 members including 12 admin identities. Sample: Full policy membership and exclusion evaluation

Original assessment procedure

1. Join enabled accounts to include/exclude assignments
2. Separate registered methods from effective policy
3. Check unsupported exclusions independently of two approved emergency identities

Expected No unsupported exclusion

Observed fictional result Four unsupported exclusions include two admin identities; two separately approved emergency identities are not those four.

Evidence and finding trace E04; F04.

Gap Four member accounts are excluded from the intended MFA policy without a current exception. Two are dedicated administrative identities. The two monitored emergency identities are separately approved and are not part of these four exceptions.

Proposed treatment Remove unsupported exclusions after validating access impact; document intended emergency design and test both authorized access and disallowed password-only access in a sandbox.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-IA-02 Verify service-secret rotation evidence

Control context IA-5. Result: PASS.

Authored criterion CL-W-IA-02 selected application secrets rotate within fictional 90 day interval

Population and sample Four service credentials for two applications. Sample: All four declared credentials; metadata only not secret values

Original assessment procedure

1. Inspect credential owner and creation dates
2. Compute age at 30 September
3. Trace rotation ticket and revoked prior version metadata

Expected Four credentials current and prior versions disabled

Observed fictional result SCRED01-04 are aged 12, 21, 34 and 56 days. Each has a disabled prior version and retained rotation ticket. The scanner credential issue in F06 is outside these four application credentials.

Evidence and finding trace WE-IA-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-IA-03 Check identity uniqueness

Control context IA-4. Result: PASS.

Authored criterion CL-W-IA-03 each member identity has unique immutable identifier and accountable person

Population and sample 196 member identities and 22 guests. Sample: Full identifier duplicate scan; mapping types retained

Original assessment procedure

1. Compare immutable IDs rather than display names
2. Identify person accounts versus dedicated admin accounts
3. Check guest sponsor mapping independently

Expected No duplicate immutable IDs and attributable identities

Observed fictional result 184 person identities plus 12 admin identities produce 196 unique IDs; 22 separate guest IDs have sponsor fields. Enabled departure remains F03, not a uniqueness failure.

Evidence and finding trace WE-IA-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

IR Incident Response workpaper

Selection rationale Incident plans must route real decisions through authorized people, including supplier and communication decisions.

W-IR-01 Check supplier incident decision authority

Control context IR-4; IR-8. Result: PARTIAL.

Authored criterion CL-08 primary and deputy decision authority

Population and sample Six supplier-exposure exercise decisions. Sample: All six decision records

Original assessment procedure

1. Identify decision owner and alternate
2. Compare authority to plan delegation
3. Trace the two supplier decisions to exercise log

Expected Six authorized routes

Observed fictional result Four have roles; temporary data-flow suspension and customer notification authorization lack named approvers.

Evidence and finding trace E08; F08.

Gap Two of six exercise decisions lack a named approver: temporary suspension of supplier data flow and customer notification authorization. Four decisions identify an accountable role and alternative contact.

Proposed treatment Name primary and deputy decision roles, validate contractual notice duties with counsel and repeat the two decision paths in a tabletop exercise.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-IR-02 Check reporting-channel reachability

Control context IR-6. Result: PASS.

Authored criterion CL-W-IR-02 staff know a documented incident channel

Population and sample Six fictional role interviews. Sample: Support engineering IT procurement privacy and leadership roles

Original assessment procedure

1. Record each role statement separately
2. Compare stated route with distributed plan
3. Describe benign channel submission and ticket acknowledgment

Expected Six consistent routes and one acknowledged fixture

Observed fictional result Six of six identify the published channel; IR-TEST01 creates acknowledged triage ticket without sending real notification.

Evidence and finding trace WE-IR-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-IR-03 Verify incident-record completeness

Control context IR-5. Result: PASS.

Authored criterion CL-W-IR-03 triage records preserve timeline evidence pointers and accountable handler

Population and sample Four synthetic triage records. Sample: All four benign exercise records

Original assessment procedure

1. Check UTC event and triage timestamps
2. Trace evidence pointers to immutable exercise IDs
3. Check handler and disposition fields before completion

Expected Four complete records

Observed fictional result IR01-IR04 retain timestamps evidence pointers and handlers; incomplete owner fixture stays pending rather than closed.

Evidence and finding trace WE-IR-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

MA Maintenance workpaper

Selection rationale Remote and physical servicing must use authorized personnel and controlled access; cloud infrastructure operation is inherited, not inspected on site.

W-MA-01 Verify laptop servicing authorization

Control context MA-2. Result: PASS.

Authored criterion CL-W-MA-01 repair work requires ticket owner and return check

Population and sample Six quarter laptop repair tickets. Sample: All six declared servicing records; not the 30 device protection sample

Original assessment procedure

1. Match serial number to asset record
2. Inspect pre-work approval and authorized technician
3. Confirm return checklist and custody timestamps

Expected Six traceable approved repairs

Observed fictional result MA01-MA06 match serials to six managed laptops, retain approved scope and signed return checks; no protection status inferred for other devices.

Evidence and finding trace WE-MA-01; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-MA-02 Check remote maintenance session limits

Control context MA-4. Result: PASS.

Authored criterion CL-W-MA-02 vendor support session is approved time bounded and revoked

Population and sample Three scheduled application-vendor support sessions. Sample: All three records; session metadata only

Original assessment procedure

1. Compare approval scope with granted role
2. Check session start/end against allowed window
3. Inspect revocation and retained activity reference

Expected Three scoped sessions end and permissions revoke

Observed fictional result RMA01-03 each use named vendor identity; 60 minute window; actual durations 21, 34, 43 minutes; grants revoked after session.

Evidence and finding trace WE-MA-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-MA-03 Check maintenance personnel authorization

Control context MA-5. Result: PASS.

Authored criterion CL-W-MA-03 technician roster and escort route precede equipment access

Population and sample Four authorized repair technicians and two external visits. Sample: Full four-person roster and both visitor records

Original assessment procedure

1. Verify approved technician list and validity
2. Match visit identity to authorized individual
3. Check assigned escort and equipment-access record

Expected Both visits by current authorized personnel with escort

Observed fictional result TECH01-04 roster current; VISMA01 by TECH03 and VISMA02 by TECH04 each record IT escort and only approved asset access.

Evidence and finding trace WE-MA-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

MP Media Protection workpaper

Selection rationale Customer information can persist on removable media and retired devices; handling controls differ from online export-retention decisions.

W-MP-01 Check removable-media restriction

Control context MP-7. Result: PASS.

Authored criterion CL-W-MP-01 unapproved removable storage is blocked; approved encrypted media explicitly allowed

Population and sample Two synthetic device-policy evaluation cases. Sample: One unapproved USB and one approved encrypted recovery device

Original assessment procedure

1. Read device-control rule including exception selector
2. Evaluate unapproved media identity
3. Evaluate approved encrypted media and verify audit entry

Expected Unapproved blocked; approved bounded use logged

Observed fictional result USB-DENY01 is blocked and logged; USB-ALLOW01 permits approved encrypted recovery media only. This is not an endpoint encryption-coverage assertion.

Evidence and finding trace WE-MP-01; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-MP-02 Check retired media sanitization

Control context MP-6. Result: PASS.

Authored criterion CL-W-MP-02 retired data-bearing media has sanitization method verification and disposition

Population and sample Four retired drives in quarter disposal register. Sample: All four records; outside 184 active-laptop population

Original assessment procedure

1. Reconcile asset retirement with drive serial
2. Inspect authorized sanitization method and verifier
3. Trace certificate to final disposal or reuse decision

Expected Four unique serials with verified sanitization

Observed fictional result RET01-RET04 certificates name serial, approved method, verifier and disposal date; all four retired, not counted as active endpoints.

Evidence and finding trace WE-MP-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-MP-03 Check controlled physical media transport

Control context MP-5. Result: PASS.

Authored criterion CL-W-MP-03 data-bearing media transit uses sealed custody and approved recipient

Population and sample Two shipments of retired encrypted drives before destruction. Sample: Both custody chains

Original assessment procedure

1. Match serialized media to dispatch inventory
2. Trace seal number and courier custody
3. Match recipient acknowledgment to dispatch serials

Expected Two intact chains and no unaccounted serial

Observed fictional result SHIP01 carries RET01-02 under seal S001; SHIP02 carries RET03-04 under S002; both received with matching seal and serial count.

Evidence and finding trace WE-MP-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

PE Physical and Environmental Protection workpaper

Selection rationale Review Cedarline-controlled office safeguards and explicitly inherited cloud-provider assurance; no provider datacenter inspection is represented.

W-PE-01 Check office entry authorization

Control context PE-3. Result: PASS.

Authored criterion CL-W-PE-01 office badge access follows approved employee or visitor purpose

Population and sample One fictional office; 12 selected badge assignments and four visits. Sample: Risk-based 12 active badges and all four declared visitor records

Original assessment procedure

1. Compare badge holder to approved office-access list
2. Inspect visitor sponsor and check-in/out record
3. Trace one denied inactive-badge fixture to event record

Expected 12 current assignments; four sponsored visits; inactive fixture denied

Observed fictional result BAD01-12 have approved holders; VIS01-04 show sponsor and check out; BAD-INACTIVE fixture is denied. Physical badge results do not cure directory departure gap.

Evidence and finding trace WE-PE-01; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-PE-02 Check office equipment-room environment records

Control context PE-11; PE-13. Result: PASS.

Authored criterion CL-W-PE-02 selected room power and fire safeguards retain service records

Population and sample One office network room with one UPS and one fire-detection zone. Sample: Both quarterly maintenance records and two alarm-path fixtures

Original assessment procedure

1. Inspect dated UPS service and battery test result
2. Inspect fire detection service record
3. Describe alarm receipt by designated facilities contact

Expected Current service records and both alarm routes acknowledged

Observed fictional result UPS-01 quarterly record shows battery test accepted; FIRE-01 service current; two synthetic alarm routes acknowledge facilities contact. No live fire or power test performed.

Evidence and finding trace WE-PE-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-PE-03 Check inherited cloud physical safeguard coverage

Control context PE-2; SA-9. Result: PASS.

Authored criterion CL-W-PE-03 selected cloud service assurance identifies physical control coverage and relevant period

Population and sample One primary cloud-provider assurance package among five critical providers. Sample: Selected provider with completed responsibility review, not the two incomplete F13 files

Original assessment procedure

1. Match service and region to assurance scope
2. Read period bridge and physical access/environment sections
3. Record inherited boundary and required customer responsibilities

Expected Scoped period coverage and acknowledged inherited responsibilities

Observed fictional result SUP01 package covers selected hosted infrastructure period and physical access/environment sections; review records customer boundary. This is assurance review only, not onsite effectiveness testing.

Evidence and finding trace WE-PE-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

PL Planning workpaper

Selection rationale System plans must explain boundaries and responsibilities in a way operators can use when technology and providers change.

W-PL-01 Check shared-control owner assignments

Control context PL-2. Result: PARTIAL.

Authored criterion CL-02 each selected shared responsibility has accountable owner and deputy

Population and sample Eight shared-control responsibility records. Sample: All eight records

Original assessment procedure

1. Compare cloud service boundary to responsibility matrix
2. Inspect accountable individual and deputy fields
3. Confirm changed provider scope triggers review

Expected Eight accepted individual assignments

Observed fictional result Six complete; cloud evidence retention and supplier-assisted recovery name teams not accountable individuals.

Evidence and finding trace E02; F02.

Gap Two responsibility records name a team but no accountable individual: cloud evidence retention and supplier-assisted recovery. Six records identify an individual and backup.

Proposed treatment Name accountable owners and deputies for both gaps; add a provider-change trigger and confirm each role accepts the assignment.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-PL-02 Check rules-of-behavior acknowledgment

Control context PL-4. Result: PASS.

Authored criterion CL-W-PL-02 personnel accept current handling and acceptable-use rules

Population and sample The declared 184-person acknowledgment roster; completion is separate from current access authorization. Sample: Full 184-person acknowledgment join; separately exclude admin identities

Original assessment procedure

1. Match people roster to acknowledgment keys
2. Verify policy version current at cut-off
3. Check access onboarding checklist requires acceptance

Expected 184 current acknowledgments

Observed fictional result The roster contains 168 employee and 16 contractor acknowledgments of ROB26. Dedicated administrative accounts are not additional people. An acknowledgment does not justify the enabled departure account in F03.

Evidence and finding trace WE-PL-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-PL-03 Check application security boundary diagrams

Control context PL-8. Result: PASS.

Authored criterion CL-W-PL-03 diagrams identify identity data stores external services and trust crossings

Population and sample Two production applications. Sample: Both declared application architecture records

Original assessment procedure

1. Compare diagram version with current service inventory
2. Trace identity and customer-data ingress/egress
3. Check diagram owner and review after latest approved change

Expected Two versioned approved diagrams with explicit crossings

Observed fictional result ARCH-P01 portal and ARCH-Q01 queue show identity provider, customer stores and supplier interfaces; both reviewed after latest architecture change.

Evidence and finding trace WE-PL-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

PM Program Management workpaper

Selection rationale The programme must connect resources and decisions to enterprise risk; governance documents alone do not close operational findings.

W-PM-01 Verify programme accountability

Control context PM-1. Result: PASS.

Authored criterion CL-W-PM-01 charter names sponsor security lead and review cadence

Population and sample One security programme charter. Sample: Current approved version and one quarterly agenda

Original assessment procedure

1. Check approval and version owner
2. Trace named executive sponsor and security lead to role directory
3. Inspect recurring quarterly agenda for risk decisions

Expected Approved charter and accountable review forum

Observed fictional result CHAR26 names sponsor and security lead; Q3 agenda includes risk decisions and resource review. Individual shared-control gaps remain F02.

Evidence and finding trace WE-PM-01; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-PM-02 Verify resource decisions

Control context PM-3. Result: PASS.

Authored criterion CL-W-PM-02 security investment requests retain sponsor decision and priority rationale

Population and sample Four selected security budget requests. Sample: All four declared requests for fictional quarter

Original assessment procedure

1. Trace request to identified security need
2. Inspect sponsor decision and date
3. Check accepted/deferred decision retains rationale and accountable owner

Expected Four traceable decisions without implied funding promise

Observed fictional result BUD01-04 each retain sponsor decision; three accepted and one deferred with rationale. These are historical fictional decisions, not new remediation commitment.

Evidence and finding trace WE-PM-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-PM-03 Verify risk-acceptance expiry

Control context PM-9. Result: PARTIAL.

Authored criterion CL-01 sponsor decision and review expiry required

Population and sample 12 open exceptions. Sample: All 12 register records; same observation as CA workpaper not an independent sample

Original assessment procedure

1. Read documented risk-decision authority
2. Check sponsor decision for retained exceptions
3. Reconcile expiry and escalation route without double counting

Expected Current accountable treatment for each exception

Observed fictional result Five lack expiry; three of those lack sponsor decision. Same F01 population is cross-mapped, not three additional findings.

Evidence and finding trace E01; F01.

Gap Five of 12 exceptions lack an expiry; three of those five also lack a sponsor decision. This is five unique deficient exception records, not eight incidents.

Proposed treatment Require owner, reason, safeguard, sponsor decision and expiry for each retained exception; reconcile the five records and route overdue items to the sponsor.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

PS Personnel Security workpaper

Selection rationale People lifecycle records must align with system access and contractual obligations; screening conclusions remain bounded to evidence examined.

W-PS-01 Verify termination access coordination

Control context PS-4. Result: PARTIAL.

Authored criterion CL-03 access removed within 24 hours of HR event

Population and sample 11 workforce departures. Sample: Full quarter departure population shared with AC workpaper

Original assessment procedure

1. Read authoritative employment end timestamp
2. Match termination notice to service ticket
3. Reconcile effective directory state and elapsed removal time

Expected 11 timely removals

Observed fictional result Eight timely; two at 41/63 hours; one enabled at cut-off. This reuses F03 and is not a second departure population.

Evidence and finding trace E03; F03.

Gap Three of 11 workforce accounts did not meet the internal 24-hour removal target. Two were disabled after 41 and 63 hours; one account remained enabled at the 30 September cut-off. No use after departure is asserted.

Proposed treatment Resolve the remaining account with the business owner, revoke sessions where required and implement a same-day HR trigger with an independent reconciliation.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-PS-02 Check access agreements

Control context PS-6. Result: PASS.

Authored criterion CL-W-PS-02 selected starters sign confidentiality and access agreement before access

Population and sample Eight fictional quarter starters within 184-person workforce. Sample: Four employee and four contractor starters selected across quarter

Original assessment procedure

1. Match person identity and start date
2. Inspect signed agreement version and timestamp
3. Compare initial access grant timestamp

Expected Eight agreements signed before first access

Observed fictional result JOIN01-08 retain AGR26 acceptance one to five days before access; four employees and four contractors represented.

Evidence and finding trace WE-PS-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-PS-03 Verify role-based screening decisions

Control context PS-3. Result: PASS.

Authored criterion CL-W-PS-03 selected sensitive-role appointments have documented screening decision before assignment

Population and sample Six custodians of 12 dedicated admin identities. Sample: All six custodian appointment records; no background details disclosed

Original assessment procedure

1. Read role sensitivity and required screening decision
2. Check authorized HR completion indicator
3. Compare completion date to privilege assignment

Expected Six recorded decisions precede assignment

Observed fictional result C01-C06 retain HR-screening complete indicator and approval before privilege grant; no raw screening results or legal adequacy conclusion asserted.

Evidence and finding trace WE-PS-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

PT Personally Identifiable Information Processing and Transparency workpaper

Selection rationale Customer data flows need approved purpose and handling decisions; readiness evidence does not establish a legal basis or legal compliance.

W-PT-01 Verify processing-purpose decisions

Control context PT-3; SI-12. Result: PARTIAL.

Authored criterion CL-14 approved purpose and retention for declared flows

Population and sample Six customer-data flows and 12 export locations. Sample: All six flows with storage-location linkage

Original assessment procedure

1. Trace flow from source to recipient
2. Inspect approved purpose and retention decision
3. Map missing decisions to storage locations without multiplying flows

Expected Six approved purposes and durations

Observed fictional result Two flows lack approved retention purpose/duration; three of 12 locations carry those flows. Counsel retains legal interpretation.

Evidence and finding trace E14; F14.

Gap Two of six flows lack an approved retention purpose and duration. Three of 12 storage locations carry those two flows. No lawful basis or legal retention conclusion is made from these records.

Proposed treatment Obtain purpose and retention decisions for both flows with counsel and business owners; validate lifecycle rules in isolation using synthetic objects and reconcile the processing register.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-PT-02 Check transparency publication ownership

Control context PT-5. Result: PASS.

Authored criterion CL-W-PT-02 declared public notice has accountable owner version and review trigger

Population and sample One fictional customer privacy notice and two change requests. Sample: Current notice metadata and both workflow records; no legal opinion

Original assessment procedure

1. Compare published version with approved register
2. Inspect privacy-owner sign off and review trigger
3. Trace change requests to notice review outcome

Expected Version and change decisions traceable

Observed fictional result NOTICE26 matches register; PCH01 contact change updates notice; PCH02 internal routing change records no-public-text-change decision. Wording lawfulness not assessed.

Evidence and finding trace WE-PT-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-PT-03 Check consent withdrawal routing where selected

Control context PT-4. Result: PASS.

Authored criterion CL-W-PT-03 optional marketing preference can be withdrawn without affecting essential service

Population and sample Two synthetic optional-marketing preference records. Sample: One opt-in and one withdrawal fixture outside customer-service processing decisions

Original assessment procedure

1. Read selected marketing purpose and preference record
2. Describe withdrawal request through configured route
3. Verify suppression state while essential-service route remains separate

Expected Withdrawal suppresses optional marketing; no inference all processing uses consent

Observed fictional result MKT01 opt-in allows optional campaign; MKT02 withdrawal sets suppression and leaves service notifications separate. Fixtures demonstrate workflow only.

Evidence and finding trace WE-PT-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

RA Risk Assessment workpaper

Selection rationale Priority should reflect exposure and business context; scan output alone does not establish exploitability or enterprise risk.

W-RA-01 Reconcile authenticated scan coverage

Control context RA-5. Result: PARTIAL.

Authored criterion CL-06 monthly authenticated node coverage

Population and sample 24 compute nodes. Sample: Full node inventory against latest monthly scan

Original assessment procedure

1. Match scanner target IDs to compute inventory
2. Read authentication outcome not merely job completion
3. Reconcile missing schedules separately from failed credentials

Expected 24 authenticated outcomes

Observed fictional result Nineteen nodes have authenticated results; three show authentication failure and two have no scheduled record. These results do not establish that the 19 authenticated nodes are free of vulnerabilities.

Evidence and finding trace E06; F06.

Gap 19 of 24 nodes report authenticated scanning; three report authentication failure and two lack a scheduled record. Three of the 10 sampled service nodes have internally rated high flaws older than the fictional 21-day treatment target without a current exception.

Proposed treatment Restore authenticated coverage for five exceptions; validate the three overdue flaw records and approve safe treatment or documented compensating safeguards.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-RA-02 Check risk scenario evaluation

Control context RA-3. Result: PASS.

Authored criterion CL-W-RA-02 scenario assessment states asset threat impact safeguards and treatment owner

Population and sample Three selected business risk scenarios. Sample: Credential theft workflow outage and supplier exposure scenarios

Original assessment procedure

1. Trace scenario to affected service and data
2. Inspect likelihood/impact rationale and current safeguards
3. Check treatment owner and review trigger

Expected Three reasoned assessments with explicit assumptions

Observed fictional result RISK01-03 each state a scenario, service impact and owner; ratings remain qualitative sample judgments, not loss forecasts.

Evidence and finding trace WE-RA-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-RA-03 Check treatment decisions for overdue high flaws

Control context RA-7. Result: PARTIAL.

Authored criterion CL-06 internal high flaws treated within 21 days or current exception

Population and sample 10 selected customer-service nodes from 24. Sample: Same 10 node risk-based subset supporting F06

Original assessment procedure

1. Validate flaw applicability and affected service
2. Compute age against 21 day target
3. Inspect authorized treatment or expiring exception

Expected 10 timely treatments or approved exceptions

Observed fictional result Seven timely; three internally rated high flaws exceed 21 days without current exception. Applicability must be validated before final treatment.

Evidence and finding trace E06; F06.

Gap 19 of 24 nodes report authenticated scanning; three report authentication failure and two lack a scheduled record. Three of the 10 sampled service nodes have internally rated high flaws older than the fictional 21-day treatment target without a current exception.

Proposed treatment Restore authenticated coverage for five exceptions; validate the three overdue flaw records and approve safe treatment or documented compensating safeguards.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

SA System and Services Acquisition workpaper

Selection rationale Security obligations must be specified in supplier and development processes and supported by release decisions.

W-SA-01 Review critical supplier responsibility decisions

Control context SA-9. Result: PARTIAL.

Authored criterion CL-13 review assurance scope exceptions and customer responsibilities

Population and sample Five critical providers within nine suppliers. Sample: All five assurance files

Original assessment procedure

1. Match purchased service to report scope
2. Read exceptions and customer responsibility sections
3. Inspect reviewer decision and assigned follow-up

Expected Five completed relevant reviews

Observed fictional result Three completed; two have current reports but no recorded responsibility or exception review.

Evidence and finding trace E13; F13.

Gap Two of five critical-provider files contain current assurance reports but no recorded review of customer responsibilities or relevant exceptions. The other three retain reviewer decisions.

Proposed treatment Review the two reports for scope, period, exceptions and customer responsibilities; assign relevant actions and confirm evidence for required Cedarline controls.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-SA-02 Check release security decisions

Control context SA-11. Result: PARTIAL.

Authored criterion CL-10 unresolved internal high issues require resolution or approved expiry

Population and sample Eight sample releases; eight repositories; six pipelines. Sample: Eight quarter releases selected across declared applications

Original assessment procedure

1. Trace release artifact to security job outputs
2. Inspect triage and approved exception for unresolved high issues
3. Check gate outcome rather than job existence

Expected Eight justified security release decisions

Observed fictional result Three of eight releases lack authorized expiring exceptions; six of eight repositories have intended branch protection.

Evidence and finding trace E10; F10.

Gap Six of eight repositories have the intended branch protection. Three of eight sampled releases contain unresolved internal high security findings without an authorized expiring exception. No exploitability or breach is inferred.

Proposed treatment Protect the remaining two repositories and require a resolution or valid exception before release; preserve an approved emergency path with time-bounded review.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-SA-03 Check threat review before material design changes

Control context SA-3; SA-8. Result: PASS.

Authored criterion CL-W-SA-03 selected design changes document trust boundary review and requirements

Population and sample Two application design changes. Sample: Both declared material architecture changes

Original assessment procedure

1. Read change objectives and data flows
2. Inspect threat review for new trust crossings
3. Trace agreed security requirement into implementation ticket

Expected Two traceable design reviews

Observed fictional result DES01 tenant import and DES02 queue API change each identify trust boundary, abuse case and security acceptance ticket. This does not assert complete code review.

Evidence and finding trace WE-SA-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

SC System and Communications Protection workpaper

Selection rationale Validate selected transport and network-boundary mechanisms with allowed and denied paths; avoid treating configuration presence as universal enforcement.

W-SC-01 Check network administration boundaries

Control context SC-7. Result: PASS.

Authored criterion CL-W-SC-01 workload administration only through controlled support path

Population and sample Four cloud accounts and two synthetic network paths. Sample: All four account administrative rule snapshots; authorized and internet-origin fixtures

Original assessment procedure

1. Identify management ports and allowed source selectors
2. Trace approved support source through selected rule
3. Evaluate unapproved internet origin and retain denial

Expected Four snapshots restrict administration; approved path allowed and internet path denied

Observed fictional result NET01-04 restrict management source; PATH01 support origin allowed; PATH02 public origin denied. No port scan or penetration test performed.

Evidence and finding trace WE-SC-01; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-SC-02 Check application transport protection

Control context SC-8; SC-13. Result: PASS.

Authored criterion CL-W-SC-02 customer-facing endpoints enforce a fictional minimum of TLS 1.2 and a valid certificate hostname.

Population and sample Two production application endpoint configurations. Sample: Both declared endpoints; synthetic TLS negotiation matrices

Original assessment procedure

1. Inspect minimum protocol setting and certificate hostname
2. Describe current protocol connection and obsolete protocol attempt
3. Check HTTP redirect does not expose authenticated payload

Expected Both accept TLS 1.2 or higher and reject obsolete protocol

Observed fictional result TLS-P01 and TLS-Q01 accept TLS 1.2 and 1.3 and reject TLS 1.0 and 1.1. Both certificate hostnames match. The HTTP redirect contains a location header without customer payload.

Evidence and finding trace WE-SC-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-SC-03 Check selected cloud-store encryption and key scope

Control context SC-28. Result: PASS.

Authored criterion CL-W-SC-03 customer application stores encrypted with restricted key administration

Population and sample Two customer application data stores. Sample: Both declared stores; two authorized application reads and two unauthorized key-administration requests, one pair for each store.

Original assessment procedure

1. Match store identifier to encryption key reference
2. Inspect separation of application use and key administration
3. Describe denied key-policy change by application role

Expected Two stores encrypted; app can use storage but cannot administer key

Observed fictional result STORE-P01 and STORE-Q01 show encryption settings. KEY-DENY01 for KEY-P01 and KEY-DENY02 for KEY-Q01 deny policy changes by the respective application roles; APP-READ01 and APP-READ02 allow the intended store read. Active laptop encryption exceptions in F05 remain separate.

Evidence and finding trace WE-SC-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

SI System and Information Integrity workpaper

Selection rationale Coverage, treatment and data retention require operational evidence; working agents or successful jobs alone do not establish complete protection.

W-SI-01 Check high-flaw treatment

Control context SI-2. Result: PARTIAL.

Authored criterion CL-06 internal high flaws require 21 day treatment or authorized exception

Population and sample 10 sampled service nodes. Sample: Same 10 node treatment population as W-RA-03; not an independent sample

Original assessment procedure

1. Validate scanner observation against package or configuration record
2. Trace age and business owner
3. Inspect treatment or current exception

Expected All 10 meet declared treatment rule

Observed fictional result Three overdue without current exception; seven timely. Reuses F06, not an additional finding.

Evidence and finding trace E06; F06.

Gap 19 of 24 nodes report authenticated scanning; three report authentication failure and two lack a scheduled record. Three of the 10 sampled service nodes have internally rated high flaws older than the fictional 21-day treatment target without a current exception.

Proposed treatment Restore authenticated coverage for five exceptions; validate the three overdue flaw records and approve safe treatment or documented compensating safeguards.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-SI-02 Check managed endpoint agent reporting

Control context SI-3. Result: PASS.

Authored criterion CL-W-SI-02 selected laptops report a managed endpoint agent within the fictional 24-hour check-in interval.

Population and sample 30 selected laptops from the 184 active laptop records. Sample: The same 30-device protection sample supporting F05.

Original assessment procedure

1. Join device identifier to management console
2. Read agent version and last check-in timestamp
3. Separate agent presence from encryption and protection policy conformance

Expected 30 managed-agent records with check-in within 24 hours.

Observed fictional result All 30 report managed agent within 24 hours. Five unique protection-setting exceptions in F05 remain open; presence is not policy conformance.

Evidence and finding trace WE-SI-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-SI-03 Check export retention decisions

Control context SI-12. Result: PARTIAL.

Authored criterion CL-14 retention configuration follows approved purpose and duration

Population and sample Six customer-data flows and 12 export storage locations. Sample: All six flows; all 12 location links

Original assessment procedure

1. Read approved retention decision for each flow
2. Map location lifecycle configuration to decision
3. Distinguish missing decision from proven over-retention

Expected Six approved decisions implemented across 12 locations

Observed fictional result Two flows carried by three locations lack approved retention purpose/duration. No breach or legal retention conclusion asserted.

Evidence and finding trace E14; F14.

Gap Two of six flows lack an approved retention purpose and duration. Three of 12 storage locations carry those two flows. No lawful basis or legal retention conclusion is made from these records.

Proposed treatment Obtain purpose and retention decisions for both flows with counsel and business owners; validate lifecycle rules in isolation using synthetic objects and reconcile the processing register.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

SR Supply Chain Risk Management workpaper

Selection rationale Criticality, contractual accountability and provider-assurance decisions should remain linked throughout service changes.

W-SR-01 Check critical provider assurance review

Control context SR-3; SR-6. Result: PARTIAL.

Authored criterion CL-13 reviewer considers scope exceptions and customer responsibilities

Population and sample Five critical providers from nine total suppliers. Sample: All five critical files; cross-map existing F13 population

Original assessment procedure

1. Confirm provider criticality and service scope
2. Read assurance exceptions and customer responsibilities
3. Trace reviewer acceptance or remediation decision

Expected Five completed reviews

Observed fictional result Two incomplete reviews despite current reports; three retain reviewer decisions. This is the same F13 population as W-SA-01.

Evidence and finding trace E13; F13.

Gap Two of five critical-provider files contain current assurance reports but no recorded review of customer responsibilities or relevant exceptions. The other three retain reviewer decisions.

Proposed treatment Review the two reports for scope, period, exceptions and customer responsibilities; assign relevant actions and confirm evidence for required Cedarline controls.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-SR-02 Check supply-chain risk plan and tiering

Control context SR-2. Result: PASS.

Authored criterion CL-W-SR-02 inventory records criticality owner data access and review cadence

Population and sample Nine supplier inventory entries. Sample: Full nine entry review

Original assessment procedure

1. Match procurement list to supplier inventory
2. Inspect criticality rationale based on service/data dependence
3. Check owner and cadence for each supplier

Expected Nine complete records; five identified critical

Observed fictional result SUP01-05 critical with annual review; SUP06-09 standard with biennial review; all nine owners and service/data descriptions present. Completed reviews remain a separate test.

Evidence and finding trace WE-SR-02; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

W-SR-03 Check supplier notice and contract ownership

Control context SR-8; SA-9. Result: PASS.

Authored criterion CL-W-SR-03 critical contracts name owner and notification route

Population and sample Five critical provider agreements. Sample: All five signed agreements; one benign supplier notice fixture

Original assessment procedure

1. Locate executed agreement and contract owner
2. Inspect agreed incident/change communication route
3. Describe notice intake and owner acknowledgment without inventing legal time obligation

Expected Five owned agreements and traceable routing

Observed fictional result CON01-05 signed with owners; SUPNOTICE01 routes benign notice to procurement and incident triage. Authority to notify customers remains F08.

Evidence and finding trace WE-SR-03; no additional finding.

Gap No exception in this bounded fictional objective.

Proposed treatment Retain the stated operating cadence and reperform after relevant change; no new remediation finding.

Limit Invented records and procedures demonstrate reporting depth. No real assessment, interview, system query or execution occurred; selected objectives do not establish full family implementation.

Governance Debt Register

Governance Debt in this sample means unresolved ownership, exception, evidence or risk decisions accumulated over time. It is not a monetary valuation or a proprietary numerical security score. Six items link to existing findings and actions, so they do not add six new findings.

Debt	Owner and age	Required decision	Links
GD01	Security lead 98 days	Risk acceptance with expiry; reject unsupported ongoing deferral	F01 / A01
GD02	Technology director 65 days	Accept named owners and deputies	F02 / A02
GD03	Identity lead 55 days	Approve safe removal or documented emergency exception	F04 / A04
GD04	Resilience lead 106 days	Reserve isolated exercise and business-owner time	F11 / A11
GD05	Procurement lead 81 days	Assign system-owner review and responsibility decisions	F13 / A13
GD06	Product operations lead 43 days	Name the AI risk approver and retain current use boundary	F15 / A15

Age runs from the fictional opening date to 14 October 2026 and describes unresolved decision time, not exposure duration. All six items require review on 21 October 2026. Escalation depends on the consequence and any delay to safe treatment, rather than the oldest item alone.

Escalation rule

The Security lead collates owner decisions and raises overdue High finding dependencies to the sponsor. A retained exception requires a business reason, current safeguard, accountable acceptance, expiry and review trigger. The sponsor should not accept a delay by silence. Every acceptance remains separate from technical closure.

Governance Debt decisions 1

GD01 linked to F01

Decision owner and age Security lead; opened 2026-07-08; 98 days at issue.

Reason for deferral Sponsor decisions deferred during service migration.

Consequence Four overdue access and change exceptions remain subject to informal team-level decisions. A customer diligence response would lack a current accountable treatment decision.

Interim safeguard Seven records retain current approvals and expiries. The service desk sends monthly reminders, which do not enforce escalation.

Required decision and dependency Risk acceptance with expiry; reject unsupported ongoing deferral. Management risk appetite and named decision authority.

Review and action 21 October 2026; A01. UNRESOLVED at issue.

GD02 linked to F02

Decision owner and age Technology director; opened 2026-08-10; 65 days at issue.

Reason for deferral Provider support transfer completed without a responsibility refresh.

Consequence Collection and recovery tasks would stall during absence or a provider handoff. The bounded gap is an ownership weakness without a demonstrated failed security event.

Interim safeguard The technology director owns the enterprise charter; six responsibilities have working escalation routes.

Required decision and dependency Accept named owners and deputies. Provider support scope and sponsor approval.

Review and action 21 October 2026; A02. UNRESOLVED at issue.

GD03 linked to F04

Decision owner and age Identity lead; opened 2026-08-20; 55 days at issue.

Reason for deferral Migration exclusion retained pending user-impact review.

Consequence A password-only route to administrative functions increases exposure to stolen credentials. Method registration is not proof of policy enforcement.

Interim safeguard The remaining 192 accounts fall within the intended MFA policy or the two documented emergency-access designs. Sample policy evaluation records support those assignments.

Required decision and dependency Approve safe removal or documented emergency exception. Monitored emergency route and user communication.

Review and action 21 October 2026; A04. UNRESOLVED at issue.

Governance Debt decisions 2

GD04 linked to F11

Decision owner and age Resilience lead; opened 2026-06-30; 106 days at issue.

Reason for deferral Portal recovery acceptance deferred for product availability.

Consequence A technically restored database would still leave customer work unusable or inconsistent. A backup success or infrastructure startup does not establish business recovery.

Interim safeguard The other two critical services retain accepted exercises. Portal backup jobs and a documented recovery objective exist.

Required decision and dependency Reserve isolated exercise and business-owner time. Synthetic test dataset, isolated environment and business-owner availability.

Review and action 21 October 2026; A11. UNRESOLVED at issue.

GD05 linked to F13

Decision owner and age Procurement lead; opened 2026-07-25; 81 days at issue.

Reason for deferral Complete provider reports retained without assigned reviewer capacity.

Consequence A provider report would be cited as assurance while required customer actions remain unassigned. Provider controls do not establish Cedarline configuration.

Interim safeguard All five files retain signed agreements and a designated contract owner. Three include responsibility and exception review.

Required decision and dependency Assign system-owner review and responsibility decisions. Access to complete provider reports and system-owner review.

Review and action 21 October 2026; A13. UNRESOLVED at issue.

GD06 linked to F15

Decision owner and age Product operations lead; opened 2026-09-01; 43 days at issue.

Reason for deferral Pilot treated as a technical trial without expansion authority.

Consequence The pilot would expand into customer records without a clear decision on privacy, errors and provider terms. The high rating reflects the missing expansion control, not demonstrated current customer harm.

Interim safeguard The pilot uses synthetic inputs, has no write or send permission and requires a human to review every draft. Current constraints reduce immediate exposure.

Required decision and dependency Name the AI risk approver and retain current use boundary. Privacy review, provider terms and named risk authority.

Review and action 21 October 2026; A15. UNRESOLVED at issue.

Evidence & Control Review Register

Each record below is an invented evidence bundle. Dates are fictional record or workpaper dates. The period is the quarter unless a current snapshot is stated. A real engagement retains source identity, time zone, filters, pagination and integrity evidence in restricted workpapers.

Evidence and date	Declared scope and reliability	Links
E01 2026-10-02	12 open security exceptions in the quarter-end register; all 12 examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T01-01 F01
E02 2026-10-02	Eight selected shared-control responsibility records; all eight examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T01-02 F02
E03 2026-10-02	11 workforce departures from 1 July to 30 September 2026; all 11 examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T02-01 F03
E04 2026-10-02	196 enabled member accounts including 12 dedicated administrative identities; policy scope examined in full Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T02-02 F04
E05 2026-10-02	184 workforce laptops; risk-based sample of 30 laptops; full owner inventory examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T03-01 F05
E06 2026-10-02	24 cloud compute nodes; latest monthly scan cycle examined; 10 customer-service nodes sampled for patch decisions Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T03-02 F06
E07 2026-10-02	Four cloud accounts and seven declared priority log sources; all configurations examined; 10 working days of review records Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T04-01 F07
E08 2026-10-02	One incident plan and six fictional supplier-exposure exercise decisions; all decisions examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T04-02 F08

Records establish only the stated sample or snapshot. Interview intent requires corroboration. Configuration does not prove historical absence of misuse; a benign denied fixture does not substitute for penetration testing. No credentials, personal records or live infrastructure identifiers are included.

Evidence register continued 2

Each record below is an invented evidence bundle. Dates are fictional record or workpaper dates. The period is the quarter unless a current snapshot is stated. A real engagement retains source identity, time zone, filters, pagination and integrity evidence in restricted workpapers.

Evidence and date	Declared scope and reliability	Links
E09 2026-10-02	18 production changes in the quarter; judgmental sample of 10 changes Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T05-01 F09
E10 2026-10-02	Eight repositories and six delivery pipelines; eight releases sampled from the quarter Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T05-02 F10
E11 2026-10-02	Three declared critical business services; one isolated restore record per service examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T06-01 F11
E12 2026-10-02	Eight protected workloads; all backup policies and copy records examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T06-02 F12
E13 2026-10-02	Nine suppliers including five critical providers; all five critical provider files examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T07-01 F13
E14 2026-10-02	Six customer-data processing flows and 12 export storage locations; all declared flows examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T07-02 F14
E15 2026-10-02	One AssistNotes internal pilot with 12 authorized users; pilot approval and use boundary examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T08-01 F15
E16 2026-10-02	20 synthetic ticket drafts in the internal AssistNotes pilot; all 20 review records examined Synthetic illustration; corroborating export and ticket fields described, not independently collected.	T08-02 F16

Records establish only the stated sample or snapshot. Interview intent requires corroboration. Configuration does not prove historical absence of misuse; a benign denied fixture does not substitute for penetration testing. No credentials, personal records or live infrastructure identifiers are included.

Evidence register continued 3

Each record below is an invented evidence bundle. Dates are fictional record or workpaper dates. The period is the quarter unless a current snapshot is stated. A real engagement retains source identity, time zone, filters, pagination and integrity evidence in restricted workpapers.

Evidence and date	Declared scope and reliability	Links
E17 2026-10-05	Four supporting checks for this domain, with explicit exclusions where stated. Synthetic reporting demonstration; no real fixture or configuration was executed.	T01-03, T01-04, T01-05, T01-06 Supporting checks
E18 2026-10-05	Four supporting checks for this domain, with explicit exclusions where stated. Synthetic reporting demonstration; no real fixture or configuration was executed.	T02-03, T02-04, T02-05, T02-06 Supporting checks
E19 2026-10-05	Four supporting checks for this domain, with explicit exclusions where stated. Synthetic reporting demonstration; no real fixture or configuration was executed.	T03-03, T03-04, T03-05, T03-06 Supporting checks
E20 2026-10-05	Four supporting checks for this domain, with explicit exclusions where stated. Synthetic reporting demonstration; no real fixture or configuration was executed.	T04-03, T04-04, T04-05, T04-06 Supporting checks
E21 2026-10-05	Four supporting checks for this domain, with explicit exclusions where stated. Synthetic reporting demonstration; no real fixture or configuration was executed.	T05-03, T05-04, T05-05, T05-06 Supporting checks
E22 2026-10-05	Four supporting checks for this domain, with explicit exclusions where stated. Synthetic reporting demonstration; no real fixture or configuration was executed.	T06-03, T06-04, T06-05, T06-06 Supporting checks
E23 2026-10-05	Four supporting checks for this domain, with explicit exclusions where stated. Synthetic reporting demonstration; no real fixture or configuration was executed.	T07-03, T07-04, T07-05, T07-06 Supporting checks
E24 2026-10-05	Four supporting checks for this domain, with explicit exclusions where stated. Synthetic reporting demonstration; no real fixture or configuration was executed.	T08-03, T08-04, T08-05, T08-06 Supporting checks

Records establish only the stated sample or snapshot. Interview intent requires corroboration. Configuration does not prove historical absence of misuse; a benign denied fixture does not substitute for penetration testing. No credentials, personal records or live infrastructure identifiers are included.

The original 24 bundles support the 48 domain checks. Two unassessed checks explicitly lack supporting evidence, with reasons in the test records. The 16 finding bundles E01 to E16 and eight supporting workpapers E17 to E24 are not 24 independent observations of enterprise security.

Record level evidence and fixture register

The records that follow are original invented exhibits. They make sample selection, procedure and result traceable without claiming that a real system was inspected or a real fixture was executed. The original E01 to E24 bundles remain the domain-view evidence register; repeated use of a bundle is not independent corroboration.

The T-series supporting checks sometimes use a bounded fixture-only population rather than an operational sample. Their PASS labels apply only to the illustrated path; they are not elevated to live operating-effectiveness results by this expansion. W-series workpapers retain their own explicit population and selection fields.

Common record metadata All WE entries are dated 2026-10-05; period: 2026-07-01 to 2026-09-30 unless snapshot stated. Type: Original fictional record-level fixture.

Limit applying to every WE record Invented fixture, not collected evidence. Record labels are illustrative; no conclusion beyond stated sample. Blank table cells indicate a field not represented in that fixture, not an additional control failure.

WE-AC-02 Check independent privilege approval fictional fixture

Source and trace workpapers.cedarline.example/we-ac-02; W-AC-02.

Record	Request	Approver	Result
AR01-AR02	ordinary workflow role	business owner not requester	approved role only
AR03-AR04	support role	support owner not requester	approved role only
AR05-AR06	admin role	technology director not requester	approved role only

WE-AC-03 Verify object-level customer separation fictional fixture

Source and trace workpapers.cedarline.example/we-ac-03; W-AC-03.

Application	Own	Other	Log
portal	200 permitted	403 no payload	DENY-AC01
queue	200 permitted	403 no payload	DENY-AC02

WE-AT-01 Reconcile security learning coverage fictional fixture

Source and trace workpapers.cedarline.example/we-at-01; W-AT-01.

Roster	Count	Course	Current completions
EMP001-EMP168	168	SEC26	168
CTR001-CTR016	16	SEC26	16

WE-AT-02 Check role-specific administrator learning fictional fixture**Source and trace** workpapers.cedarline.example/we-at-02; W-AT-02.

Custodians	Identities	Modules	Completion	Renewal
C01-C06	ADM01-ADM12	IAM26; REC26	6 of 6	after completion

WE-AT-03 Verify training-record integrity fictional fixture**Source and trace** workpapers.cedarline.example/we-at-03; W-AT-03.

Id	Reason	Old retained	Approved by
TRC01	duplicate person-key merge	True	learning owner
TRC02	course import date correction	True	learning owner

WE-AU-03 Verify log-store write and delete separation fictional fixture**Source and trace** workpapers.cedarline.example/we-au-03; W-AU-03.

Id	Role	Action	Outcome
ING-AU01	log-delivery	write event	allow
DEL-AU01	workload-admin	delete retained event	deny

WE-CA-02 Verify monitoring responsibilities fictional fixture**Source and trace** workpapers.cedarline.example/we-ca-02; W-CA-02.

Id	Check	Cadence	Record
MON01	access	monthly	access-review-September
MON02	scan	monthly	scan-September
MON03	logging	daily	review-September30
MON04	backup	daily	copy-September30

WE-CA-03 Check independent assessment follow-through fictional fixture**Source and trace** workpapers.cedarline.example/we-ca-03; W-CA-03.

Ids	Preparer	Reviewer	Comment disposition
REV01-REV03	control analyst	security lead	3 of 3 documented

WE-CM-03 Verify versioned configuration baselines fictional fixture**Source and trace** workpapers.cedarline.example/we-cm-03; W-CM-03.

Template	Nodes	Approved
WEB26	8	CHG-B01
WORK26	10	CHG-B02
MGMT26	6	CHG-B03

WE-CP-03 Verify recovery contact usability fictional fixture**Source and trace** workpapers.cedarline.example/we-cp-03; W-CP-03.

Service id	Runbook	Deputy route
service-portal	RC01	resolved
service-identity	RC02	resolved
service-queue	RC03	resolved

WE-IA-02 Verify service-secret rotation evidence fictional fixture**Source and trace** workpapers.cedarline.example/we-ia-02; W-IA-02.

Id	Age days	Prior
SCRED01	12	disabled
SCRED02	21	disabled
SCRED03	34	disabled
SCRED04	56	disabled

WE-IA-03 Check identity uniqueness fictional fixture**Source and trace** workpapers.cedarline.example/we-ia-03; W-IA-03.

Type	Unique ids	Sponsors
person	184	
Dedicated admin	12	
guest	22	22

WE-IR-02 Check reporting-channel reachability fictional fixture

Source and trace <workpapers.cedarline.example/we-ir-02>; W-IR-02.

Roles	Consistent	Total	Id	Outcome
support; engineering; IT; procurement; privacy; leadership	6	6		
			IR-TEST01	triage acknowledged

WE-IR-03 Verify incident-record completeness fictional fixture

Source and trace <workpapers.cedarline.example/we-ir-03>; W-IR-03.

Record	Illustrated fields
IR01-IR04	Complete records: 4; Timestamps: UTC; Handler: assigned
IR-NOOWNER	State: pending triage

WE-MA-01 Verify laptop servicing authorization fictional fixture

Source and trace <workpapers.cedarline.example/we-ma-01>; W-MA-01.

Tickets	Approved	Serial matches	Return checks	Population
MA01-MA06	6	6	6	6

WE-MA-02 Check remote maintenance session limits fictional fixture

Source and trace <workpapers.cedarline.example/we-ma-02>; W-MA-02.

Id	Minutes	Allowed minutes	Grant after
RMA01	21	60	revoked
RMA02	34	60	revoked
RMA03	43	60	revoked

WE-MA-03 Check maintenance personnel authorization fictional fixture

Source and trace workpapers.cedarline.example/we-ma-03; W-MA-03.

Roster	Current	Visit	Technician	Escort
TECH01-TECH04	4			
		VISMA01	TECH03	IT01
		VISMA02	TECH04	IT02

WE-MP-01 Check removable-media restriction fictional fixture

Source and trace workpapers.cedarline.example/we-mp-01; W-MP-01.

Id	Media	Outcome
USB-DENY01	unapproved	blocked and logged
USB-ALLOW01	approved encrypted recovery device	allowed and logged

WE-MP-02 Check retired media sanitization fictional fixture

Source and trace workpapers.cedarline.example/we-mp-02; W-MP-02.

Ids	Count	Method	Certificate matches	Active inventory
RET01-RET04	4	approved cryptographic erase with verification	4	False

WE-MP-03 Check controlled physical media transport fictional fixture

Source and trace workpapers.cedarline.example/we-mp-03; W-MP-03.

Shipment	Serials	Seal	Received count
SHIP01	RET01; RET02	S001	2
SHIP02	RET03; RET04	S002	2

WE-PE-01 Check office entry authorization fictional fixture

Source and trace workpapers.cedarline.example/we-pe-01; W-PE-01.

Record	Illustrated fields
BAD01-BAD12	Approved: 12
VIS01-VIS04	Sponsored and closed: 4
BAD-INACTIVE	Outcome: denied

WE-PE-02 Check office equipment-room environment records fictional fixture

Source and trace <workpapers.cedarline.example/we-pe-02>; W-PE-02.

Device	Record	Outcome	Fixture	Acknowledged
UPS-01	Q3 service	accepted battery test		
FIRE-01	Q3 service	current		
			UPS and fire alarm routes	2

WE-PE-03 Check inherited cloud physical safeguard coverage fictional fixture

Source and trace <workpapers.cedarline.example/we-pe-03>; W-PE-03.

Supplier	Scope	Period	Review	Onsite inspection
SUP01	selected cloud infrastructure	covers declared quarter with bridge	completed	False

WE-PL-02 Check rules-of-behavior acknowledgment fictional fixture

Source and trace <workpapers.cedarline.example/we-pl-02>; W-PL-02.

Policy	Employees	Contractors	Total people	Current acknowledgments
ROB26	168	16	184	184

WE-PL-03 Check application security boundary diagrams fictional fixture

Source and trace <workpapers.cedarline.example/we-pl-03>; W-PL-03.

Id	System	Trust crossings	Review
ARCH-P01	portal	identity; customer upload; supplier API	approved
ARCH-Q01	queue	identity; workflow store; notification API	approved

WE-PM-01 Verify programme accountability fictional fixture

Source and trace <workpapers.cedarline.example/we-pm-01>; W-PM-01.

Id	Approved by	Operational owner	Cadence	Risk and resource items
CHAR26	executive sponsor	security lead	quarterly	
Q3AGENDA				True

WE-PM-02 Verify resource decisions fictional fixture**Source and trace** workpapers.cedarline.example/we-pm-02; W-PM-02.

Record	Illustrated fields
BUD01-BUD03	Decision: accepted; Count: 3
BUD04	Decision: deferred; Rationale: dependency sequencing; Owner: technology director

WE-PS-02 Check access agreements fictional fixture**Source and trace** workpapers.cedarline.example/we-ps-02; W-PS-02.

Ids	Type	Signed before grant
JOIN01-JOIN04	employee	4
JOIN05-JOIN08	contractor	4

WE-PS-03 Verify role-based screening decisions fictional fixture**Source and trace** workpapers.cedarline.example/we-ps-03; W-PS-03.

Custodians	Completion indicators	Prior to assignment	Sensitive details
C01-C06	6	6	not reproduced

WE-PT-02 Check transparency publication ownership fictional fixture**Source and trace** workpapers.cedarline.example/we-pt-02; W-PT-02.

Id	Owner	Version matches	Decision
NOTICE26	privacy lead	True	
PCH01			notice updated
PCH02			no public wording change; reason recorded

WE-PT-03 Check consent withdrawal routing where selected fictional fixture**Source and trace** workpapers.cedarline.example/we-pt-03; W-PT-03.

Id	Preference	Optional campaign	Essential service
MKT01	opted in	allowed	
MKT02	withdrawn	suppressed	separate route

WE-RA-02 Check risk scenario evaluation fictional fixture

Source and trace workpapers.cedarline.example/we-ra-02; W-RA-02.

Id	Scenario	Service	Owner
RISK01	credential theft	portal	identity lead
RISK02	workflow outage	identity service	resilience lead
RISK03	supplier exposure	queue	procurement lead

WE-SA-03 Check threat review before material design changes fictional fixture

Source and trace workpapers.cedarline.example/we-sa-03; W-SA-03.

Id	Boundary	Requirement	Ticket
DES01	tenant import	tenant-scoped authorization	SEC-D01
DES02	queue API	service identity scope	SEC-D02

WE-SC-01 Check network administration boundaries fictional fixture

Source and trace workpapers.cedarline.example/we-sc-01; W-SC-01.

Record	Illustrated fields
NET01-NET04	Management source: controlled support path; Count: 4
PATH01	Source: approved support; Outcome: allow
PATH02	Source: internet; Outcome: deny

WE-SC-02 Check application transport protection fictional fixture

Source and trace workpapers.cedarline.example/we-sc-02; W-SC-02.

Id	Endpoint	Accepted	Rejected
TLS-P01	portal.cedarline.example	TLS 1.2; TLS 1.3	TLS 1.0; TLS 1.1
TLS-Q01	queue.cedarline.example	TLS 1.2; TLS 1.3	TLS 1.0; TLS 1.1

WE-SC-03 Check selected cloud-store encryption and key scope fictional fixture

Source and trace workpapers.cedarline.example/we-sc-03; W-SC-03.

Store	Key	Encryption	Read fixture	Key change fixture
STORE-P01	KEY-P01	enabled	APP-READ01 allowed	KEY-DENY01 denied
STORE-Q01	KEY-Q01	enabled	APP-READ02 allowed	KEY-DENY02 denied

WE-SI-02 Check managed endpoint agent reporting fictional fixture**Source and trace** workpapers.cedarline.example/we-si-02; W-SI-02.

Devices	Agent present	Checkin within24h	Policy exceptions
LAP-S01-LAP-S30	30	30	F05 unchanged

WE-SR-02 Check supply-chain risk plan and tiering fictional fixture**Source and trace** workpapers.cedarline.example/we-sr-02; W-SR-02.

Suppliers	Tier	Count	Cadence
SUP01-SUP05	critical	5	annual
SUP06-SUP09	standard	4	biennial

WE-SR-03 Check supplier notice and contract ownership fictional fixture**Source and trace** workpapers.cedarline.example/we-sr-03; W-SR-03.

Record	Illustrated fields
CON01-CON05	Signed: 5; Owners: 5
SUPNOTICE01	Route: procurement and incident triage; Acknowledged: True

Prioritized Remediation Roadmap

The roadmap sequences planned work from the fictional issue date. It does not predict risk reduction or show completed remediation. Every action is linked to one finding and remains PLANNED. Internal effort, approval and observation time require management scheduling.

Window	Actions and owner	Required output
Days 1 to 14 by 28 October	A03, A04 - Identity lead A15 - Product operations lead	Reconcile access, approve safe MFA changes and name the AI risk approver. Keep synthetic-only pilot limits.
Days 1 to 30 by 13 November	A01 - Security lead A06, A07 - Cloud and Security operations A09, A10 - Engineering and Release	Risk decisions, fresh scan and delivery evidence, enforceable approvals and benign release tests.
Days 1 to 45 by 28 November	A02 - Technology director A05 - IT operations A11 - Resilience	Accepted responsibility matrix, device reconciliation and portal business recovery evidence.
Days 15 to 45 by 28 November	A08 - Incident lead A16 - Product operations	Deputy incident decision path and repeatable AI evaluation linked to A15.
Days 15 to 60 by 13 December	A12 - Cloud operations A13 - Procurement A14 - Privacy	Retention decisions, customer responsibilities and synthetic lifecycle verification.

Immediate sponsor response

Approve named owner capacity and safe test windows. Review any proposed delay to the High findings before its target expires. Keep the AI pilot within the current synthetic-only boundary. The roadmap does not authorize production deletion, unapproved access changes or customer communication.

Remediation dependencies and safe sequencing

Sequence	Dependency	Verification milestone
Access before routine review	HR event source, authorized removal and monitored emergency route before changing identity policy. A03, A04.	Fresh departure trace plus privileged and emergency policy evaluations.
Visibility before dependable monitoring	Collector permissions and retained native events before delivery changes; known node inventory before scan reconciliation. A06, A07.	All four account event traces; one fresh 24-node authenticated cycle.
Release control before continuous enforcement	Reliable triage, independent approval and a tested emergency path before the gate becomes blocking. A09, A10.	Authorized fixture passes and unapproved fixture fails; inspect a fresh release.
Business acceptance before recovery closure	Isolated dataset and agreed transaction checks before restore; approved retention decision before policy observation. A11, A12.	Portal acceptance and selected retained-copy recovery evidence.
AI authority before expansion	A15 risk approver and data/provider review before A16 acceptance and version decisions.	Unsigned expansion request is held; fixed synthetic corpus and targeted error cases reviewed.

Dependencies do not excuse silent delay. Owners record interim safeguards and bring resource conflicts to the sponsor. The same configuration export supports several decisions; repeated use does not create independent proof. Changes require a rollback route and checks for service impact.

Observation period

Some closure evidence follows the change, such as the next scan cycle, departure, release or retained-copy horizon. Record implementation and operational verification as separate milestones. A completed implementation task remains open for verification until its required subsequent evidence exists.

Action ownership and acceptance register

Action and finding	Accountable owner	Due date	Status
A01 / F01	Security lead	2026-11-13	PLANNED
A02 / F02	Technology director	2026-11-28	PLANNED
A03 / F03	Identity lead	2026-10-28	PLANNED
A04 / F04	Identity lead	2026-10-28	PLANNED
A05 / F05	IT operations lead	2026-11-28	PLANNED
A06 / F06	Cloud operations lead	2026-11-13	PLANNED
A07 / F07	Security operations lead	2026-11-13	PLANNED
A08 / F08	Incident lead	2026-11-28	PLANNED
A09 / F09	Engineering lead	2026-11-13	PLANNED
A10 / F10	Release manager	2026-11-13	PLANNED
A11 / F11	Resilience lead	2026-11-28	PLANNED
A12 / F12	Cloud operations lead	2026-12-13	PLANNED
A13 / F13	Procurement lead	2026-12-13	PLANNED
A14 / F14	Privacy lead	2026-12-13	PLANNED
A15 / F15	Product operations lead	2026-10-28	PLANNED
A16 / F16	Product operations lead	2026-11-28	PLANNED

Due dates are fictional planning targets derived from the issue date and stated window. They are not Cyvelle delivery promises or a price entitlement. Each action retains its exact output and closure requirement in the detailed finding and structured data.

Closure authority

The Security lead reviews technical and operational evidence. The appropriate business owner accepts service outcomes, and the executive sponsor accepts residual risk with an expiry when treatment remains incomplete. An owner attestation alone is insufficient where the finding requires a current export, test outcome or observed process record.

Reporting cadence

Owners report weekly through the first 30 days, then at the agreed governance review. Progress should show implementation, verification, unresolved dependency and residual decision separately. Closed-ticket counts must not be displayed as measured security improvement.

Verification measures and baseline records

Measure	Fictional baseline and period	Verification target
Departure removal	8 of 11 within 24 hours; quarter	Reconcile all 11 records and observe the next departure.
MFA coverage	Four unsupported exclusions in 196 enabled member accounts; cut-off snapshot	Remove or approve each exception and verify intended policy.
Authenticated scan	19 of 24 nodes; latest monthly cycle	Fresh authenticated reconciliation for all 24 declared nodes.
Central cloud delivery	Three of four accounts; snapshot	Benign trace from all four accounts and stale-feed alerts.
Change approval	Seven of 10 sampled changes approved independently; quarter sample	Next ordinary and emergency changes retain required authorization.
Release risk decision	Five of eight sampled releases resolved or excepted; quarter sample	Fresh release plus allowed and denied benign fixtures.
Business recovery	Two of three critical services with accepted restore evidence	Portal restore includes transaction checks and business acceptance.
AI evaluation	Three unsupported details corrected in 20 synthetic drafts; pilot sample	Versioned error criteria and repeatable corpus reviewed by approver.

Every measure retains numerator, denominator, population and period. These are counts, not a single security score. Sample measures must not be projected beyond the selected records; targets are planned, not measured post-remediation outcomes. Future comparison should preserve the population and collection procedure or explain any change.

Twelve month assurance programme

Illustrative programme measured from management authorization, not a claim of completed work. Existing A01-A16 target windows remain the initial remediation objectives; later phases demonstrate sustained operation and expanded assurance, not extensions that erase overdue dates.

P01 Days 0 to 14

Contain unsupported access and prevent unapproved AI expansion

Owner and action trace Identity lead and product operations lead. A03; A04; A15.

Dependencies Executive sponsor confirms decision authority; Identity owner validates emergency route before changing exclusions; HR timestamps and synthetic-only AI boundary are available.

Deliverables Departure-account reconciliation and session decisions; Approved MFA scope and positive/denial fixtures; Named AI risk approver and signed release or stop decision.

Independent verification Security lead rechecks the affected identities and the model-change approval path; implementers do not self-certify closure.

Exit gate No unsupported access exception remains untreated without explicit dated acceptance; AI expansion remains blocked absent approval.

P02 Days 15 to 30

Establish enforceable risk, scan, logging and release decisions

Owner and action trace Security lead with cloud operations, engineering and release owners. A01; A06; A07; A09; A10.

Dependencies P01 urgent controls stabilized; Approved maintenance and release windows; Reliable inventories and issue-severity triage.

Deliverables Exception register with expiry and sponsor decisions; 24-node authenticated scan reconciliation; Four-account central traces and two stale-feed tests; Independent change workflow and enforced security release gate.

Independent verification A reviewer not making the configuration changes examines full exception populations and selected fresh ordinary/emergency release records.

Exit gate Current evidence supports coverage and decision controls; remaining exceptions are owned, time-bounded and escalated rather than silently counted as passes.

Assurance programme days 31 to 90

P03 Days 31 to 60

Close ownership, recovery, supplier, retention and AI-evaluation gaps

Owner and action trace Technology director coordinating resilience, procurement, privacy and product operations leads. A02; A05; A08; A11; A12; A13; A14; A16.

Dependencies A15 precedes A16 approval; A02 ownership decisions enable provider-assisted recovery; Counsel and data owners determine retention and notice duties; Isolated recovery and lifecycle test environments exist.

Deliverables Accepted responsibility matrix and device reconciliation; Deputy incident-decision exercise; Portal business-accepted recovery and queue retention decision; Two critical-provider reviews; Two export-flow decisions with synthetic expiry/hold evidence; Versioned AI evaluation and approval record.

Independent verification Security assurance reviewer traces each original finding to closure evidence and observes targeted negative cases; counsel validates legal interpretations rather than the assessor issuing them.

Exit gate Every original finding is either evidence-closed, explicitly accepted with expiry, or overdue with sponsor escalation; no assumed improvement is reported.

P04 Days 61 to 90

Demonstrate operation beyond one-time fixes

Owner and action trace Security lead. A01; A03; A04; A06; A07; A09; A10; A11; A12; A13; A14; A16.

Dependencies Earlier changes have had an operating observation period; Evidence retention and reviewer access are established.

Deliverables Subsequent departure and exception review; Fresh scan and feed-health cycle; New release and emergency-change samples; Retention horizon observation and follow-on recovery proof; AI model-change or no-change review.

Independent verification Internal audit or a suitably independent assurance reviewer repeats a risk-based selection, includes prior exceptions, and records reopened findings separately.

Exit gate Design corrections and operating evidence are distinguished; ineffective controls are reopened with owners and dates.

Assurance programme months 4 to 12

P05 Months 4 to 6

Extend coverage and validate sustained governance

Owner and action trace Technology director and security lead. A01; A02; A07; A08; A10; A11; A13; A14; A15; A16.

Dependencies 90-day evidence review completed; Sponsor approves any additional scope and resources.

Deliverables Quarterly twenty-family coverage review and updated applicability decisions; Supplier renewal and customer-responsibility follow-through; Cross-team supplier incident and recovery exercise; Targeted cloud trust and Microsoft 365 workload review where scoped; AI use and material-change inventory review.

Independent verification An independent reviewer challenges omitted systems, provider-inherited controls, exceptions and evidence quality; additional tests are scoped explicitly rather than implied by this sample.

Exit gate Management approves residual risks and next-quarter priorities using demonstrated evidence, not a generic maturity percentage.

P06 Months 7 to 12

Institutionalize recurring assurance and refresh the assessment

Owner and action trace Executive sponsor with security lead. A01; A02; A03; A04; A05; A06; A07; A08; A09; A10; A11; A12; A13; A14; A15; A16.

Dependencies Midyear scope and resource decisions; Annual planning cycle and independent review availability.

Deliverables Recurring control-owner attestations with supporting records; Updated service inventory, threat assumptions and business recovery objectives; Annual reassessment across all twenty families with relevant selected tests; Year-end findings disposition, evidence-retention review and next-year programme.

Independent verification Independent reassessment tests operating evidence and changed scope; closure status is reset where conditions recur or evidence expires.

Exit gate Board or sponsor receives an evidence-supported year-end decision pack and approves the following year; this sample does not forecast that all gaps will be closed.

Programme resources and verification authority

The programme extends the initial remediation plan into repeatable assurance. The original action deadlines remain tied to the 14 October 2026 issue date. The 21 October revision does not restart the clock, close a finding or authorize a change.

Executive sponsor retains risk acceptance and priority authority; accountable business and technical owners remain responsible for implementation.

Named owners require protected capacity for evidence collection, authorized changes and retesting; no staffing level, fee, completion date or service entitlement is promised.

An independent verifier must be separate from the person implementing each material fix. Internal audit, a peer assurance team or a separately commissioned reviewer may fill the role.

Maintenance windows, vendor access, legal review and isolated synthetic test environments are prerequisites; unavailable prerequisites must be logged as blockers with owners rather than hidden by a green status.

Months 4-12 are a planning proposal requiring management scoping and resourcing decisions; they are not implied deliverables of every commercial Blueprint tier.

Decisions at each gate

An implementing owner proposes readiness with traceable records. A reviewer separate from that implementation checks the stated acceptance evidence. A business owner accepts service outcomes. Only the designated sponsor can approve residual risk, with a reason, safeguard, expiry and review trigger. Missing evidence or a failed retest remains visible.

Measurement discipline

Preserve the population, period, method and source for each future observation. When the estate changes, restate numerator and denominator together rather than comparing unlike populations. A higher count of closed tasks is not by itself a measured improvement in security. The following metrics are baselines and planned verification targets, not achieved outcomes.

Programme metrics 1

Authenticated scan coverage

Numerator Nodes with current authenticated success.

Denominator 24 in-scope nodes at the fictional baseline.

Baseline and planned target 19/24; target: 24/24 or explicit time-bounded risk decision.

Review cadence and owner Each cycle; Cloud operations lead.

Supported MFA decisions

Numerator Members covered by intended policy or approved emergency design.

Denominator 196 enabled members at baseline.

Baseline and planned target 192/196; target: 196/196 with policy evaluation evidence.

Review cadence and owner After changes and monthly; Identity lead.

Central account delivery

Numerator Accounts with matched end-to-end event trace.

Denominator 4 declared accounts.

Baseline and planned target 3/4; target: 4/4.

Review cadence and owner After onboarding and monthly; Security operations lead.

Independent prior change approval

Numerator Sampled changes with independent approval before deployment.

Denominator 10 selected changes at baseline.

Baseline and planned target 7/10; target: All subsequent selected changes meet approved ordinary or emergency rules.

Review cadence and owner Monthly sample; Engineering lead.

These are separate measures of selected populations. No weighted security score, forecast risk-reduction percentage or statistically projected exception rate is presented.

Programme metrics 2

Supported release decisions

Numerator Selected releases with resolved high issues or valid approval.

Denominator 8 selected releases at baseline.

Baseline and planned target 5/8; target: All selected releases have an enforceable authorized decision.

Review cadence and owner Each release and monthly review; Release manager.

Business accepted critical restoration

Numerator Critical services with complete accepted exercise records.

Denominator 3 declared critical services.

Baseline and planned target 2/3; target: 3/3 within agreed exercise scope.

Review cadence and owner Exercise cycle and material change; Resilience lead.

Retention decision coverage

Numerator Export flows with approved purpose and duration.

Denominator 6 export flows.

Baseline and planned target 4/6; target: 6/6 with lifecycle and hold alignment.

Review cadence and owner Quarterly and new-flow onboarding; Privacy lead.

AI draft corrections

Numerator Reviewed synthetic drafts requiring unsupported-detail correction.

Denominator 20 reviewed drafts in the original corpus.

Baseline and planned target 3/20 corrected before use; target: Future acceptance criteria set before evaluation; no retrospective reliability target.

Review cadence and owner Every material model change; Product operations lead.

These are separate measures of selected populations. No weighted security score, forecast risk-reduction percentage or statistically projected exception rate is presented.

Executive Recommendations & Next Steps

The sponsor should approve owner capacity for the High findings and require current evidence before closing them. The sample does not demand a wholesale tool replacement. Existing safeguards should be preserved while access, release authority, evidence completeness and business acceptance are corrected.

Management decision	Recommended disposition	Acceptance record
Risk exceptions	Treat unsupported ongoing decisions and formalize any residual acceptance. A01.	Owner, safeguard, sponsor, expiry and review trigger.
Identity controls	Prioritize safe removal and policy enforcement. A03, A04.	Current export and authorized and denied evaluations.
Release and recovery	Reserve Engineering and business-owner test capacity. A09 to A12.	Fresh change and release records plus accepted portal exercise.
Suppliers and data	Assign responsibility and retention reviews. A13, A14.	Scoped provider review and synthetic lifecycle results.
AI pilot expansion	Hold current boundary until the accountable release decision and evaluation exist. A15, A16.	Signed scope and risk decision; versioned evaluation with unresolved errors visible.

Residual risks

Unexamined changes, device settings, provider controls and model internals remain outside the conclusion. Successful retests would close the stated sample conditions only. Material changes should trigger reassessment. Management retains responsibility for availability, lawful processing, contractual commitments and risk acceptance.

Next governance review

At the 21 October 2026 fictional review, confirm owners, dependencies and any interim acceptance. Request supporting records for implementation and verification separately. The report remains an illustrative sample with no real management decisions or remediation asserted.

Criteria references and application limits

SRC01 NIST SP 800-53 Revision 5 and Release 5.2.0

Rev. 5; release 5.2.0 issued 27 August 2025. Accessed 14 October 2026.

<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

Selected context mappings; not a full control baseline or exact assessment entitlement.

SRC02 NIST Cybersecurity Framework 2.0

CSF 2.0; 26 February 2024. Accessed 14 October 2026.

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

Domain-level outcome context; no one-to-one compliance equivalence.

SRC03 NIST AI Risk Management Framework 1.0 Core

AI RMF 1.0; 26 January 2023. Accessed 14 October 2026.

<https://airc.nist.gov/airmf-resources/airmf/5-sec-core/>

Selected GOVERN, MAP, MEASURE and MANAGE category context; not a complete AI impact or legal assessment.

Version and mapping treatment

The NIST publication page identifies Release 5.2.0 issued on 27 August 2025. This report cites related control identifiers and uses authored CL criteria; it does not reproduce the catalog or claim complete baseline coverage. CSF 2.0 category labels organize outcome context. AI RMF 1.0 categories support the bounded pilot review, and NIST revision activity does not make a draft replacement an adopted criterion here.

Mappings are selected professional context for the fictional scenario, not assertions of equivalence across frameworks. The report does not constitute an ISO 27001 or ISO 42001 certification assessment, SOC examination, PCI validation, legal opinion or complete AI impact assessment. Any such engagement requires an agreed scope and appropriate assurance authority.

Source provenance

External sources establish framework identity and version only. All policy thresholds, populations, system records, outcomes, findings, owners, actions and dates describing Cedarline are invented. The fictional scenario and its records are original.

Assessment method reference and interpretation

SRC04 NIST SP 800 53A Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations. Revision 5 with Release 5.2.0 update. Source identity and release checked on 21 October 2026.

<https://csrc.nist.gov/pubs/sp/800/53/a/r5/final>

Used for assessment-method context: examining records, interviewing relevant roles and testing selected behavior. The procedures in this report are original, tailored fictional illustrations. They are not copied catalog assessment procedures and do not establish completion of the full SP 800-53A objectives for any baseline.

Assessment dimensions

A selected result needs a defined objective, applicable criterion, explicit population, method, evidence and bounded conclusion. A stated policy may support design; a configuration snapshot may support an instantaneous setting; an observed or fictional fixture result supports only the described path. They should not be silently substituted for one another.

Two views and one finding register

The 48 T-series domain checks remain the original reporting view. The 60 W-series family tests add traceable selected objectives across all 20 families. Both views intentionally share evidence and findings. Technical exhibits deepen the record trail but do not add independent test counts. The overall register remains 16 findings and 16 planned actions.

Original fictional status

No real client engagement, production execution, exploit, data deletion or corrective action occurred. All system and record examples, policy thresholds, management roles and outcomes describing Cedarline are invented. External references provide framework context only; they do not validate the fictional observations.

Technical implementation references

These primary product references identify field names and design context for the fictional configuration illustrations. They do not establish that Cedarline operated any setting or passed a technical test. Product-specific examples remain partial, non-deployable illustrations within their stated boundaries.

TSRC01 GitHub OIDC in AWS

<https://docs.github.com/en/actions/how-tos/secure-your-work/security-harden-deployments/oidc-in-aws>

Checked 2026-10-21.

TSRC02 AWS CloudTrail Trail fields

https://docs.aws.amazon.com/awscloudtrail/latest/APIReference/API_Trail.html

Checked 2026-10-21.

TSRC03 AWS CloudTrail GetTrailStatus

https://docs.aws.amazon.com/awscloudtrail/latest/APIReference/API_GetTrailStatus.html

Checked 2026-10-21.

TSRC04 Microsoft Graph conditional access policy creation

<https://learn.microsoft.com/en-us/graph/api/conditionalaccessroot-post-policies?view=graph-rest-1.0>

Checked 2026-10-21.

Real implementation requires confirming the current product behavior, emitted identity claims, permission boundaries, approved environment and safe rollback plan. Proposed trust and gate examples are excluded from observed result counts.

Assessment conclusion and limitations

The fictional dataset retains 16 open findings, 48 original domain checks, 24 original evidence bundles, 16 planned actions and six linked Governance Debt items. Version 2.0 adds 60 tests across all 20 NIST control families, eight technical exhibits, record-level supporting evidence and a 12 month programme. Deliberate overlap between the two test views must not be counted as independent observations.

Evidence conclusion

The declared results support the specific invented conditions and limits described in this report. They are not a security guarantee, probability forecast, comprehensive compliance determination or certification. A successful selected test does not cover all systems; missing evidence does not automatically prove a technical failure. Interview statements describe fictional role intent and require corroboration.

Technical and sampling limits

No real production access, exploit execution, destructive test, data deletion, credential use or remediation occurred. Benign fixtures and configuration exhibits are fictional illustrations. Judgmental samples are not statistically representative. Native logging, authenticated scanning, backups and human review each require evidence of their own outcome; their presence must not be averaged into a maturity score.

Closure and commercial limits

All findings are open and actions planned at issue. Closure requires current evidence and the stated verification method. A purchased tool, written policy or closed task does not satisfy the operational requirement by itself. This sample demonstrates reporting functions, not a universal list of procedures, fixed report length or tier entitlement. A real proposal defines scope, methods, commercial terms and exclusions.

Public fictional status

Cedarline Workflow Services Ltd and every related identity, system, record, observation and decision are invented. The .example identifiers avoid real infrastructure references. The report contains no real client results, credentials or confidential personal records. Its purpose is to show an original Governance Blueprint assessment format with evidence, ownership and action traceability.

End of report Illustrative fictional sample - not a client engagement.