SAMPLE EDITION · REDACTED FOR PUBLICATION · EIGHT PAGES REPRODUCED FROM THE STANDARD 31-PAGE DELIVERABLE

ASSESS · THE DIAGNOSTIC

Security Program Maturity Assessment

Against NIST CSF 2.0 · Scored 0-5, CMMI-aligned · Mapped to ISO/IEC 27001:2022, SOC 2, and the Essential Eight

Prepared for [redacted]

Engagement reference [redacted] · Version 1.2 · [redacted] 2026

Lead author Principal Security Architect [redacted]

Technical review Subject-matter specialist, identity and security operations [redacted]

Quality review Practice lead [redacted]

Document control

CLASSIFICATION AND DISTRIBUTION

Confidential. Prepared solely for [redacted] under master services agreement [redacted] and the engagement's mutual non-disclosure terms. Distribution is limited to the named recipients below; further distribution requires the practice lead's written consent. This sample edition is approved for publication with client identifiers, personnel, dates, evidence titles, and commercial figures redacted.

RECIPIENT	ROLE
[redacted]	Chief Executive Officer
[redacted]	Chief Technology Officer (engagement sponsor)
[redacted]	Head of Platform Engineering

VERSION HISTORY

VER	DATE	AUTHOR	CHANGE
0.9	[redacted]	Principal Security Architect [redacted]	Draft for internal technical and quality review
1.0	[redacted]	Principal Security Architect [redacted]	Issued to the engagement sponsor
1.1	[redacted]	SME, identity and security operations [redacted]	Corrections following the findings walkthrough with [redacted]
1.2	[redacted]	Principal Security Architect [redacted]	Reissued with validated technical sampling results; final

CONTENTS OF THE FULL REPORT

§	SECTION	PAGE	IN THIS SAMPLE
1	Executive summary	03	Included · p.03
2	Maturity profile and category summaries, six functions	05	Govern included · p.04-05
3	Control-level assessments, 48 controls in scope	12	PR.AA-05 included · p.06
4	Gap register and recommendations, 27 rows	21	Rows 14-18 included · p.07
5	Prioritised remediation roadmap, sequenced and costed	26	Extract included · p.08
6	Risk and scoring methodology	28	Summarised in §1.4
A	Evidence register, 23 documents and 14 interviews	30	Not reproduced
B	Framework mappings: ISO/IEC 27001:2022, SOC 2, Essential Eight	31	Sampled throughout

1. Executive summary

2.1 / 5.0	3.4 / 5.0	Tier 2	27 gaps
CURRENT MATURITY	AGREED TARGET, 12 MONTHS	CSF IMPLEMENTATION TIER	8 HIGH · 13 MEDIUM · 6 LOW

1.1 POSITION

The program is technically strong and weakly governed. The engineering disciplines, identity, cloud configuration, and vulnerability management, operate at or above the sector norm, and they are the reason the organisation has absorbed two years of rapid growth without a material incident. The structures that would make that resilience durable have not kept pace: risk decisions are made sensibly but informally, recovery has never been exercised against defined objectives, and detection is concentrated at the perimeter while the production estate generates little usable signal.

The overall score of 2.1 reflects this shape rather than a uniform mediocrity. Identify scores 3.0 while Recover scores 1.0, and the spread between the strongest and weakest functions is itself a finding: programs with this profile pass technical scrutiny and struggle in governance-led reviews, a customer security questionnaire, a regulator conversation, or ISO 27001 certification, because the evidence of decision-making does not exist in writing. On current evidence, roughly half of the ISO 27001:2022 Annex A controls in scope would survive an external audit without rework; the distance is closable, and it is concentrated in Govern, Detect, and Recover.

The agreed target profile of 3.4 is reachable within four quarters. The roadmap in §5 sequences the work so that the first ninety days retire the highest-exposure items, decision rights and production privileged access, before any tooling is purchased.

1.2 WHAT IS WORKING

- Identity foundations are strong: single sign-on with phishing-resistant MFA covers all sampled workforce applications, with automated joiner-mover-leaver flows.
- The cloud estate is built as code: 94% of sampled production infrastructure is declared in version-controlled templates, which makes Protect unusually improvable for its score.
- Vulnerability management runs to a defined cadence with measured burn-down, scoring 3.0 against the SANS VMMM in the function-level review.

1.3 PRIORITY THEMES

- **Decide who decides.** Risk appetite, decision rights, and oversight are undocumented (GV.RM, GV.RR, GV.OV). Every other improvement inherits this gap, so it is sequenced first.
- **Make recovery real.** Recovery objectives for core services are undefined and untested (RC.RP), a position incompatible with the availability commitments in [redacted]'s customer contracts.
- **Close production privilege.** Privileged access to production carries no workflow, approval, or session evidence (PR.AA-05, assessed in full at §3). This is the highest-likelihood path to a material incident found in this assessment.

1.4 METHOD AND EVIDENCE BASIS

> Scored against all six functions and 22 categories of NIST CSF 2.0 on a 0–5 CMMI-aligned scale (0 not performed, 1 initial, 2 repeatable, 3 defined, 4 measured, 5 optimising); function scores are the mean of category scores, rounded to 0.5, and the profile maps to CSF Implementation Tier 2, risk informed. Evidence basis: 14 interviews across engineering, operations, and leadership [redacted], 23 documents, and technical sampling of six control families in production between [redacted] and [redacted]. Scores reflect evidence sighted, not practices described; where the two differed, the evidence prevailed. Full rubric, risk matrix, and evidence register: §6 and Appendix A.

2. Maturity profile

2.1 FUNCTION-LEVEL SCORES

GOVERN	2.0 → 4.0	Decisions are made sensibly but informally. No documented risk appetite, decision rights, or board reporting cadence.
IDENTIFY	3.0 → 4.0	Asset and software inventories are current and automated. The third-party inventory exists but is not risk-tiered.
PROTECT	2.0 → 4.0	Strong identity and platform baselines, undermined by ungoverned privileged access to production (GR-014, §3).
DETECT	1.0 → 3.0	Logging is perimeter-weighted; production workloads emit little usable signal and no detection content is maintained.
RESPOND	2.0 → 3.0	An IR plan exists and roles are understood, but it has never been exercised and contact trees are stale.
RECOVER	1.0 → 3.0	Backups run and restore individually, but no recovery objectives are defined and no service-level recovery has been tested.

2.2 HOW TO READ THE SCORES

A function score is earned, not averaged into existence: each of the function's categories is scored from the control-level assessments behind it (§3 of the full report), and a category cannot score above 2 unless its practices are documented, nor above 3 unless they are followed consistently and owned. The same rubric is applied to every organisation we assess, which is what makes the score comparable over time: when this assessment is repeated, movement in the number is movement in the program.

The agreed target profile is not uniform either, and deliberately so. Carrying Detect and Recover to 3.0 while Govern, Identify, and Protect reach 4.0 reflects where [redacted]'s obligations actually bite: contractual availability commitments and a first ISO 27001 certification within four quarters. Chasing 4.0 everywhere would cost roughly half as much again and return little against the stated obligations; that trade-off is the sponsor's recorded decision [redacted].

> Category summaries for the lowest-scoring function follow on the next page; the remaining five functions receive the same treatment in §2 of the full report. Each category summary is backed by control-level assessments in the format shown at §3.

2.3 Category summaries · Govern

Six categories, scored 1.5–2.5, function mean 2.0. Evidence references point to the register at Appendix A; gap references to the register at §4.

GV.OC Organisational context **2.5 / 5**

The mission, customer commitments, and growth plan are well understood and consistently described across leadership interviews. What is missing is the catalogue: legal, regulatory, and contractual security obligations have never been enumerated in one place, so commitments are discovered in contracts when a customer asks, not before.

EVIDENCE Corporate strategy [redacted], sampled customer MSAs [redacted], interviews [redacted]

GAPS GR-022 (obligations catalogue)

GV.RM Risk management strategy **1.5 / 5**

Risk is weighed carefully in individual decisions, then the decision evaporates: there is no appetite statement, no prioritisation method, and no record of what was accepted, by whom, or until when. Three material acceptances were reconstructed from memory during interviews; none had a review date.

EVIDENCE Interviews [redacted], board pack sample [redacted]

GAPS GR-018 (acceptance register), GR-021 (appetite and method)

GV.RR Roles, responsibilities, authorities **1.5 / 5**

Security authority concentrates in one individual, [redacted], with no documented delegation, no cover for leave, and no defined escalation path when they are unavailable. The team executes well under this arrangement; it fails the moment the individual is absent, and it cannot be evidenced to an auditor.

EVIDENCE Org chart [redacted], interviews [redacted]

GAPS GR-021 (decision rights)

GV.PO Policy **2.0 / 5**

The core policy set exists, is readable, and is genuinely read: new starters could describe its substance unprompted. Review cycles, exception handling, and version control are informal, so the policies drift from practice in places (the access-control policy predates the current production platform by two years).

EVIDENCE Policy set [redacted], onboarding records [redacted]

GAPS GR-023 (policy lifecycle)

GV.OV Oversight **1.5 / 5**

No standing forum reviews security posture or risk. Board reporting happens when something prompts it, in an ad hoc format each time, which leaves directors carrying accountability they cannot evidence they discharged. A monthly forum and a stable four-metric board view are recommended at §4 and sequenced first on the roadmap.

EVIDENCE Board minutes sample [redacted], interviews [redacted]

GAPS GR-021, GR-018

GV.SC Supply chain risk management **2.0 / 5**

A vendor inventory exists and the top 50 suppliers are tiered by spend. Tiering by access and data held, the dimension that matters for security, stops there, and nothing triggers reassessment when a contract or integration changes. Two of the five highest-access vendors sat outside the tiered set when sampled.

EVIDENCE Vendor register [redacted], procurement records [redacted]

GAPS GR-016 (risk tiering), GR-024 (reassessment triggers)

3. Control-level assessment (sample of 48)

PROTECT › IDENTITY MANAGEMENT, AUTHENTICATION AND ACCESS CONTROL

PR.AA-05 · Privileged access

1.0 / 5
INITIAL · AD HOC

"Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties." — NIST CSF 2.0

METHOD AND EVIDENCE EXAMINED

- IAM configuration export for the production cloud organisation [redacted]; access reviews and entitlement reports, where they existed.
- Session sampling across the six production services [redacted] over a two-week window [redacted].
- Interviews with the platform lead [redacted] and two on-call engineers [redacted]; the access-control policy [redacted].

OBSERVATIONS

O-1 Standing administrative access exists in all six sampled services; in two, it is exercised through shared credentials held in a team password vault.

O-2 No elevation workflow exists: access is granted permanently at onboarding to the platform team and is not re-approved, time-bound, or reviewed thereafter.

O-3 No session recording or command auditing operates on administrative sessions; the activity trail ends at login.

O-4 Two former contractors retained active production credentials 60 and 94 days after their engagements ended; both were revoked during the assessment window.

O-5 The access-control policy requires least privilege in general terms but defines no procedure for privileged access; practice has no document to comply with.

ASSESSMENT

Scored 1.0, initial. The capability exists only as the residue of individual diligence: engineers are careful, but nothing requires them to be, nothing records whether they were, and nothing removes access when the reason for it lapses (O-4). Likelihood is assessed as high because the conditions for misuse or compromise are standing rather than exceptional; impact is high because the access reaches every customer-facing service. Registered as **GR-014, HIGH**.

RECOMMENDATION

R-1 Define the privileged-access procedure in the access-control policy: who may hold elevation rights, for what, approved by whom, for how long.

R-2 Replace standing access with just-in-time elevation: time-bound, ticket-linked approval, automatic expiry, and a monitored break-glass path for emergencies.

R-3 Eliminate shared credentials; bind every administrative action to an individual identity, and enable session recording on production elevation.

R-4 Run a quarterly entitlement review owned by [redacted]; the first pass should also close O-4's leaver gap at its source in offboarding.

FRAMEWORK MAPPING

FRAMEWORK	REFERENCE	EFFECT OF CLOSING GR-014
NIST CSF 2.0	PR.AA-05	Category score floor rises to 2.5
ISO/IEC 27001:2022	A.8.2 Privileged access rights · A.5.18 Access rights	Two Annex A controls become evidence-ready
SOC 2 (TSC)	CC6.1 · CC6.3	Clears the highest-risk CC6 exception
Essential Eight	Restrict administrative privileges	Maturity Level 1 becomes claimable

One of 48 control assessments in §3 of the full report; every control in scope receives this treatment.

4. Gap register and recommendations (extract)

Rows 14–18 of 27, reproduced as scored. Risk rank is likelihood × impact on the engagement risk matrix (§6); ranks were reviewed with [redacted] on [redacted]. Owners, due dates, and costed estimates are carried per row in the full register and redacted here.

REF	FINDING AND RECOMMENDATION	REFERENCES	RISK	OWNER · DUE · COST
GR-014	**No privileged-access workflow for production.** Standing admin access, shared credentials in two of six services, no session evidence. Recommend: just-in-time elevation with approval, expiry, individual identity, and session recording (§3, R-1 to R-4).	PR.AA-05 · ISO A.8.2 · CC6.1 · E8 admin privileges	HIGH	[redacted]
GR-015	**Recovery objectives undefined for core services.** No RTO/RPO set or tested; restoration proven for data objects only, never a service. Recommend: set objectives for the four core services with the business, then prove one full service recovery per quarter.	RC.RP · ISO A.5.30 · SOC 2 A1.2	HIGH	[redacted]
GR-016	**Vendor estate untiered above 50 suppliers.** Tiering is by spend, not access and data; no reassessment trigger on contract change. Recommend: re-tier by access and data held, embed a reassessment trigger in procurement, review top tier annually.	GV.SC-04 · ISO A.5.19 · CC9.2	MEDIUM	[redacted]
GR-017	**Production telemetry below detectable baseline.** Workload and identity-plane logs are not centralised; no detection content for the five highest-likelihood techniques for this estate. Recommend: centralise production and identity telemetry, deploy an ATT&CK-mapped starter detection set, assign tuning ownership.	DE.CM-09 · ISO A.8.16 · CC7.2	HIGH	[redacted]
GR-018	**Risk acceptance is untracked.** Material risks accepted verbally; no register, owner, or review date for current acceptances. Recommend: stand up an acceptance register with owner and expiry per risk; reconstruct and ratify the three known acceptances first.	GV.RM-02 · ISO 27001 cl. 6.1 · CC3.1	MEDIUM	[redacted]

Every reference is given against NIST CSF 2.0, ISO/IEC 27001:2022 Annex A, the SOC 2 Trust Services Criteria, and the Essential Eight where it applies, so one remediation evidences every framework the organisation answers to. Close GR-014 once and it holds across all four.

5. Prioritised roadmap (extract)

Sequenced so governance decisions land before tooling is purchased, and every initiative closes named gap-register rows. The full roadmap carries owners, dependencies, and costed estimates per initiative.

HORIZON	INITIATIVE	CLOSES	COST
NOW · 0–90d	Stand up decision rights, risk appetite, and a monthly oversight forum; bring current risk acceptances into a register with owners and expiry dates.	GR-018, GR-021, GR-022	[redacted]
NOW · 0–90d	Production privileged-access workflow: just-in-time elevation, approval, expiry, individual identity, session recording (§3).	GR-014	[redacted]
NEXT · 90–180d	Define and test recovery objectives for the four core services; exercise the IR plan against the most likely scenario for this estate.	GR-015, GR-019	[redacted]
NEXT · 90–180d	Centralise production and identity-plane telemetry; deploy a starter detection set mapped to MITRE ATT&CK with named tuning ownership.	GR-017	[redacted]
LATER · 180–360d	Risk-tier the full vendor estate with procurement-embedded reassessment triggers; extend the unified control set across ISO 27001 and SOC 2 evidence.	GR-016, GR-024	[redacted]

ABOUT THIS SAMPLE

These eight pages are reproduced from the standard deliverable of the fixed-fee Security Program Assessment. The full 31-page report adds category summaries for all six functions, the complete set of 48 control-level assessments in the format shown at §3, the full 27-row gap register with owners and costed remediations, the sequenced and costed roadmap, the risk and scoring methodology, the evidence register, and the complete framework mappings. Names, dates, owners, evidence titles, and figures are redacted; the structure, method, and depth are exactly what you receive.

Every assessment is led by a principal security architect, reviewed by a function subject-matter specialist, and quality-reviewed by the practice lead before issue. Scope and price are agreed in writing before any work begins.

ALVOR ADVISORY · alvor.io/advisory · Book a consultation: alvor.io/advisory#assessment