Millwater Consulting

CLASSIFICATION

SAMPLE · ILLUSTRATIVE · V1.0

SECURITY & ARCHITECTURE HEALTH CHECK · 2026

Security & Architecture Health Check

An 80-point review across identity, data protection, logging, SIEM, identity-aware access and governance — benchmarked to ISO/IEC 27001, ISO/IEC 42001 and the NIST AI RMF. A sample report, shared to illustrate the deliverable.

29/80

EXPOSED

A capable environment with real foundations, but enterprise controls and assurance have not kept pace with scale.

CLIENT

SampleCo Holdings — mid-market, ~140 staff, multi-cloud

ENGAGEMENT

Security & Architecture Health Check — 80-point review

CONTROLS ASSESSED

80 · across 10 domains

FRAMEWORKS

ISO/IEC 27001 · ISO/IEC 42001 · NIST AI RMF (Responsible AI)

PREPARED

June 2026 · valid 90 days

SIGNED OFF BY

Patrick Sullivan, Managing Director

Reliance & scope — This is an illustrative sample using fictional data, shared to demonstrate the deliverable. It is not advice and may not be relied upon for any decision.

millwater.consulting

United States · Australia · New Zealand

SECTION 01

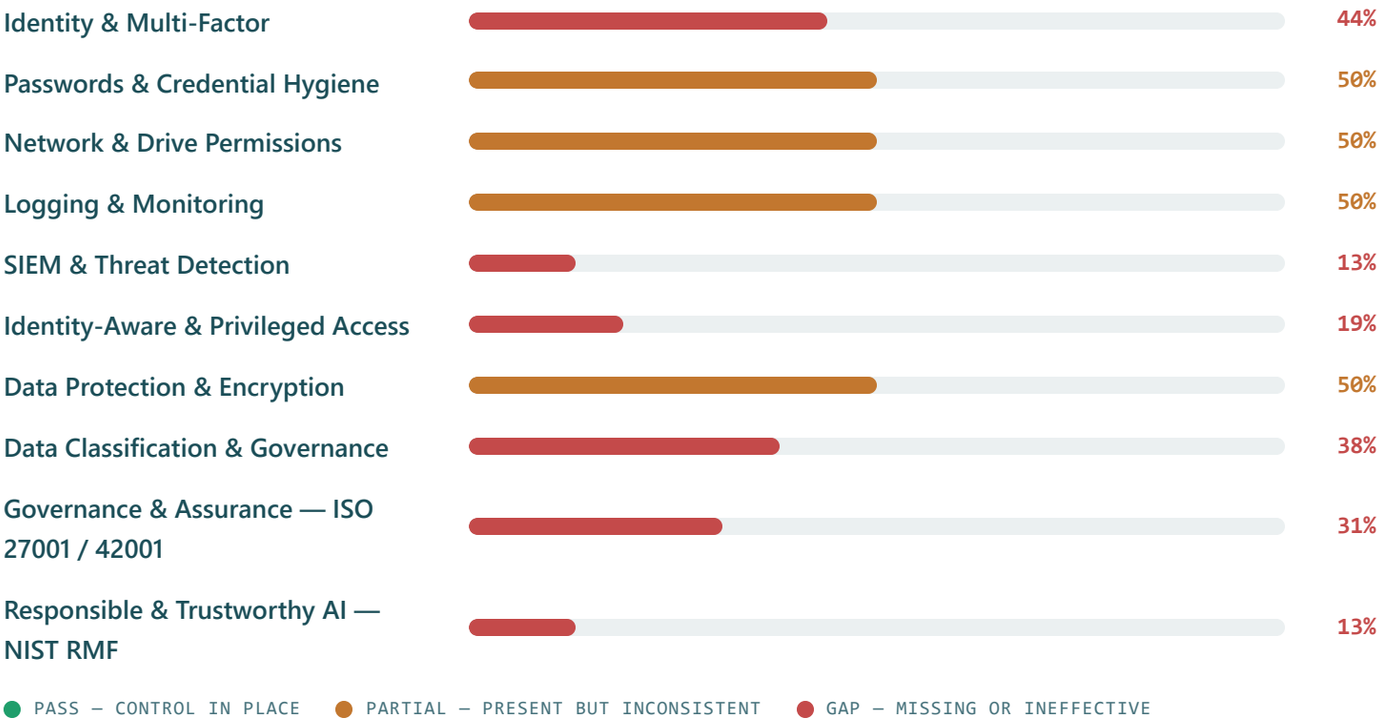
Executive summary

Solid foundations, enterprise controls lagging the scale

SampleCo Holdings has the building blocks of a secure environment, but as headcount and cloud footprint have grown the enterprise controls — SIEM, identity-aware access, data classification and an assurance baseline — have not kept pace. The findings below are grouped by domain and mapped to ISO/IEC 27001, ISO/IEC 42001 and the NIST AI RMF so remediation maps cleanly to certification.

29/80	10	37	33
OVERALL SCORE	PASS	PARTIAL	GAPS

Result by domain



SECTION 02 — Control findings

The 80-point review

PASS — CONTROL IN PLACE · PARTIAL — PRESENT BUT INCONSISTENT · GAP — MISSING OR INEFFECTIVE

Identity & Multi-Factor

2 / 8 PASS

MFA enforced on all accounts Tenant-wide conditional access requires MFA.	PASS
Phishing-resistant MFA for privileged roles OTP only; no FIDO2/passkeys for admins.	GAP
Legacy / basic auth disabled Blocked tenant-wide.	PASS
Privileged Identity Management / JIT admin Standing global-admin rights on 6 accounts.	GAP
Conditional access / risk-based policies Basic location policy; no risk scoring.	PARTIAL
Dormant & ex-staff accounts disabled promptly Joiner-mover-leaver partly manual.	PARTIAL
Service / non-human identities inventoried No inventory of service principals.	GAP
Break-glass accounts defined & monitored Exist but not alerted on.	PARTIAL

Passwords & Credential Hygiene

2 / 8 PASS

Length / complexity policy enforced 14-char minimum, passphrase guidance.	PASS
Breached-password screening On for email, not for the IdP.	PARTIAL
Enterprise password manager / vault Vault deployed for shared secrets.	PASS
Secrets out of code & config Some keys still in CI variables.	PARTIAL
Key / secret rotation policy No rotation schedule.	GAP
No shared / generic privileged logins One shared DBA login remains.	PARTIAL
Certificate lifecycle managed Manual renewals; one near-miss expiry.	PARTIAL

SECTION 03 — Control findings

Control findings (cont.)

SIEM & Threat Detection

0 / 8 PASS

- SIEM platform deployed — GAP
  No SIEM; manual log review only.
- Detection rules / use-cases defined — GAP
  No detection content.
- 24/7 monitoring or MDR coverage — GAP
  Business-hours only, ad-hoc.
- Incident-response runbook & owner — PARTIAL
  Draft runbook; untested.
- Threat intelligence feeds integrated — GAP
  None.
- Vulnerability scanning & patch SLAs — PARTIAL
  Scanning yes; no patch SLA.
- Tabletop / IR exercises run — GAP
  Never exercised.
- Mean-time-to-detect measured — GAP
  Not measured.

Identity-Aware & Privileged Access

0 / 8 PASS

- Identity-aware proxy / per-app access — GAP
  Network-location trust, not identity.
- Least-privilege RBAC enforced — PARTIAL
  Roles broad; over-provisioned.
- Periodic access reviews / recertification — GAP
  No recertification cycle.
- Privileged access workstation / bastion — GAP
  Admin from normal laptops.
- Just-in-time elevation — GAP
  Standing privilege.
- Third-party / OAuth app governance — PARTIAL
  Some review; no allow-list.
- SSO across all business apps — PARTIAL
  ~80% of apps on SSO.
- Session monitoring for privileged sessions — GAP
  Not recorded.

SECTION 04 — Control findings

Control findings (cont.)

Governance & Assurance — ISO 27001 / 42001

0 / 8 PASS

- ISMS scope & policies documented (27001) — PARTIAL
  Some policies; no formal ISMS.
- Risk register & treatment plan — PARTIAL
  Spreadsheet; not maintained.
- Asset inventory & ownership — PARTIAL
  Partial CMDB.
- Supplier / third-party risk assessment — GAP
  Not performed.
- AI management system scope (42001) — GAP
  No AIMS.
- Internal audit / management review — GAP
  None.
- Security awareness training — PARTIAL
  Annual; no phishing simulation.
- Business continuity / DR plan tested — PARTIAL
  Plan exists; untested.

Responsible & Trustworthy AI — NIST RMF

0 / 8 PASS

- AI acceptable-use policy approved — GAP
  No policy.
- AI inventory of models / tools / pilots — GAP
  No inventory.
- Human-in-the-loop & escalation thresholds — PARTIAL
  Ad-hoc per team.
- Bias / fairness & evaluation process — GAP
  None.
- AI audit trail / decision logging — GAP
  Not captured.
- Vendor-model data-handling reviewed — PARTIAL
  Reviewed for one vendor only.
- Responsible-AI review in delivery process — GAP
  Not embedded.
- Incident path for AI failures / misuse — GAP
  None.

SECTION 06 — Recommendations

A prioritised path to a defensible, AI-ready posture

OPERATE

Stand up SIEM, alerting and an incident path

Centralised logging into a SIEM with real detections and a tested incident-response runbook — the difference between catching an issue as a signal vs. as a breach notification.

BUILD

Identity-aware access + data classification & protection

Move to identity-aware, least-privilege access and classify/label data so DLP and AI tooling both know what's sensitive before a copilot can surface it.

ADVISE

Formalise ISO 27001 / 42001 alignment & Responsible-AI governance

Close the governance and assurance gaps to a defensible, certifiable baseline — and embed a NIST-RMF-aligned Responsible-AI review in the delivery process.

NEXT STEP

Let's walk through this together.

This sample shows the deliverable. On a real engagement we walk you through every finding, prioritise the gaps by exposure, and agree where to begin — no obligation.

Book your check-up →

hello@millwater.consulting
millwater.consulting