CERTPILOT · GOVERNANCE EVIDENCE PACK

Governance Evidence Pack

Cross-module operational control posture

Prepared for: Example Ltd (Demo Workspace)

Generated date: 26 September 2026

SAMPLE REPORT — ALL DATA IS FICTIONAL DEMO DATA

This sample shows the on-demand Governance Evidence Pack: a high-level summary across public-signal checks (domains, SSL, DNS, RDAP, email authentication), customer-maintained registers (renewals, people & accounts, assets, access reviews), and vendor dependencies. People, accounts, assets, access reviews, and vendor status appear as counts only — no names, emails, serial numbers, or license keys. Every domain, count, and date below is fictional demo data.

Executive Verdict

1 domain needs immediate review and 1 renewal is overdue; 2 access reviews are overdue. Resolve the items in Recommended Actions before sharing this pack with leadership or clients.

Executive Summary

Monitored domains	Renewal records	Watched vendors	Access records
8	7	6	14

Module Coverage Snapshot

High-level counts across every live module. People, accounts, assets, access reviews, and vendor status are counts only.

External Footprint

Monitored domains	Critical	Warnings	Email-auth checks
8	1	2	3

Renewals

Renewal records	Overdue	Due in 30 days	Missing owner/date
7	1	2	2

Access Reviews

Systems	Access records	Action required	Overdue reviews
6	14	2	2

People, Accounts & Assets

People	Account records	Hardware assets	Software assets
9	14	12	7

Vendor Status Watch

Watched vendors	Operational	Active incidents	Upcoming maintenance
6	5	1	1

Recommended Actions

Generated from the current workspace data only. Capped at the highest-priority items.

1. Review 1 critical domain: SSL, DNS, or registration needs immediate action. See the Domain Health Report.
2. Confirm 1 overdue renewal with the responsible owner. See the Renewal Risk Report.
3. Complete 2 overdue access reviews before the next governance review.
4. Disable active accounts for 1 offboarding/left person in the People & Accounts register.
5. Resolve 2 access entries marked action required.
6. Confirm 2 renewals due within 30 days with the responsible owner.
7. Review email authentication (SPF, DMARC, MTA-STS) for 1 domain flagged for attention.
8. Review 1 watched vendor reporting an incident on its official public status feed.

External Footprint

Domain, SSL, DNS, and RDAP status from the latest public check per domain. Summary only — full per-domain detail lives in the Domain Health Report.

Total domains	Critical	Warnings	Healthy
8	1	2	5

All 8 monitored domains have a recent check.

Email Authentication

Domains checked	Healthy	Needs attention	Critical
3	2	1	0

Email authentication posture is based on public DNS records (SPF, DMARC, MTA-STS). It reports configuration state — not deliverability and not a compliance certification.

Renewals & Vendor Register

Counts of non-cancelled renewal records. Summary only — the full list lives in the Renewal Risk Report.

Renewal records	Overdue	Due in 30 days	Missing owner/date
7	1	2	2

Access Reviews

Counts only, from customer-entered access review records. Individual names and emails appear only in the dedicated Access Review Register report.

Systems	Access records	Action required	Overdue reviews
6	14	2	2

Latest completed review

Completed: 23 Sept 2026 · Period: Q3 2026 · Cadence: Quarterly · Next review due: 22 Dec 2026.
Snapshot: 8 people · 6 systems · 14 access records · 2 action required · 2 overdue.

People & Accounts

Counts only, from the People & Accounts register. Names, emails, and individual records never appear in this report.

People	Active people	Account records	Active accounts
9	8	14	12

1 person marked offboarding or left still holds at least one active account. Review and disable these accounts as an offboarding control.

Assets Register

Customer-entered hardware and software records. Counts only — no serial numbers, asset tags, license references, or owner-level detail appear here.

Hardware assets	Active hardware	Repair / retired / lost	Software records
12	10	2	7

Evidence gaps

Hardware — missing owner: 1 · missing location: 2 · missing desk/area: 3 · missing serial: 1 · missing purchase date: 2 · missing invoice/reference: 2.
Software — missing owner: 1 · missing license reference: 1 · missing renewal date: 1 · expired/replaced/cancelled: 1.
Evidence gaps are blank fields in customer-entered records, not security findings. Completing them strengthens ownership and review evidence.

Vendor Status Watch

Summary of the workspace vendor watchlist, based on cached official public vendor status feeds.

Watched vendors	Operational	Active incidents	Upcoming maintenance
6	5	1	1

All 6 watched vendor feeds were read at the last refresh. Based on cached official public vendor status feeds — this does not confirm whether your specific tenant or account is affected.

Evidence Readiness

Dedicated reports you can generate on demand from this workspace's data.

— Domain Health Report — SSL, DNS, domain expiry, and DNS changes.
— Renewal Risk Report — overdue, upcoming, and incomplete renewal records.
— Monthly Proof Report — domains, email auth, renewals, and register counts for the month.
— Weekly Governance Report — on-demand weekly-format cross-module summary.
— Access Review Register — full access matrix with the latest completed review.

People & Accounts and the Assets Register are live registers and appear in this pack as counts only. Dedicated People and Assets PDFs are not built yet, and there is no dedicated Vendor Status PDF — vendor status appears here as a summary.

Methodology

— Public technical checks (domain, SSL, DNS, RDAP, email authentication) use public DNS, TLS, and RDAP metadata only. They report configuration and status, not internal security posture.
— Registers (renewals, people & accounts, assets, access reviews) are customer-entered records. CertPilot does not connect to Google Workspace, Microsoft 365, or any directory in this version.
— Vendor Status figures are based on cached official public vendor status feeds. CertPilot uses no customer credentials for vendor status and makes no tenant-specific impact claims.
— People, accounts, assets, and access review figures in this pack are counts only. Names, emails, serial numbers, license keys, and individual records never appear here — they live in their dedicated registers.
— This is operational governance evidence for management, client, MSP, or internal IT review. It is not a compliance certification, not an audit guarantee, not legal advice, not a vulnerability scan, not an SLA or uptime validation, and not tenant-specific impact proof.
— CertPilot is not employee monitoring. It does not read or inspect email, document, chat, or AI prompt/response content.
— This is a static sample document. Every domain, count, date, and figure is fictional demo data.