Buyer-Ready Security Evidence Review

Eight representative fictional questions showing supported, partial, contradictory, stale, assertion-only and unsupported outcomes.

FICTIONAL DEMONSTRATION. No real company, person or customer data. This sample supports buyer-readiness evidence preparation only; it is not certification, compliance attestation, legal advice, independent assurance or an audit opinion.

BR-001 **Supported**

Define the product, services and production-system boundary included in this review.

The review covers one fictional AI-enabled SaaS service, AWS London hosting, Azure OpenAI processing in Sweden Central, Cloudflare edge services, workforce access and the named buyer response. Corporate finance, payroll, the marketing site, source-code review, penetration testing, legal opinions and formal assurance are excluded.

Sanitised references: Source 1 (22 Jul 2026)

BR-003 **Contradictory**

In which countries and cloud regions is customer data processed or stored, including model processing?

Primary storage is in AWS London. Selected proposal excerpts and prompts are processed by Azure OpenAI in Sweden Central; two other suppliers process limited data in the EU. An older document incorrectly states that all processing is UK-only.

Sanitised references: Sources 1–3 (Dec 2024–Jul 2026)

BR-006 **Supported**

Is customer data encrypted in transit and what configuration is evidenced?

The supplied configuration summary records TLS 1.2 as the minimum, TLS 1.3 enabled and HTTP-to-HTTPS redirection.

Sanitised references: Source 1 (19 Jul 2026)

BR-011 **Partially supported**

How is privileged access approved, reviewed and time-bounded?

Privileged access requires approved roles, is limited to a named platform group and has an emergency-account alert. A quarterly review is described, but one review record was not retained and ordinary privileged access is not shown to be time-bounded.

Sanitised references: Sources 1–2 (Mar–Jul 2026)

Response register — continued

BR-017 **Stale evidence**

Is there a current incident-response process covering customer notification and external AI providers?

An incident-response plan exists and covers severity, containment, evidence preservation and customer communications. It is overdue, has not been exercised since November 2024 and omits the current external model provider.

Sanitised references: Source 1 (14 Nov 2024)

BR-021 **Contradictory**

Is the subprocessor register complete, current and consistent with customer terms?

The current register names four production suppliers. The older customer data-processing agreement names only two, is overdue and therefore is not consistent with the production vendor set.

Sanitised references: Sources 1–2 (Jan 2025–Jul 2026)

BR-023 **Customer assertion only**

Is customer data used to train first-party or third-party models?

The fictional company's named owner states that customer data is not used to train or fine-tune models and that the commercial provider setting prevents foundation-model training. The service configuration and processing region were not independently evidenced in this intake.

Sanitised references: Source 1 (17 Jul 2026)

BR-028 **Unsupported**

Are security and AI risks recorded, and are customer-facing claims supported by current evidence?

The security risk register contains several current risks, but the external-AI risk is overdue and has no owner or approved treatment. Several customer-facing claims are unsupported, contradictory or broader than the available evidence. A positive answer is not supportable.

Sanitised references: Sources 1–2 (20 Jul 2026)

Integrity note: archive checks can detect a file change after release. They do not establish that a source is truthful, that a control operated effectively or that the company is compliant.