Enterprise customer evidence checklist

Talsoft TS

Enterprise customer evidence checklist - Talsoft TS

Recommended use:
Use this checklist as a starting point to organize evidence before answering security questionnaires, vendor reviews or contract requests. It does not replace a GAP assessment, external audit or legal review.

1. Governance and ownership

- Internal security or risk owner defined.
- Owners by domain: access, infrastructure, product, vendors, incidents.
- Register of decisions or accepted risks.

2. Policies and procedures

- Information security policy.
- Access control policy.
- Incident response procedure.
- Change management procedure.
- Backup and recovery procedure.

3. Access and identity

- MFA enabled on critical systems.
- List of privileged users.
- Joiner, mover and leaver access process.
- Evidence of periodic access review.

4. Vulnerabilities and PenTest

- Relevant asset inventory.
- Evidence of vulnerability scans or reviews.
- Finding register with severity, owner and status.
- Evidence of remediation or risk acceptance.
- PenTest connected to roadmap when applicable.

5. Backups and continuity

- Backup scope.
- Backup frequency.
- Evidence of restore testing.
- Process owner.

6. Incidents

- Internal incident reporting channel.
- Basic playbook or procedure.
- Incident or tabletop register if available.
- Relevant internal and external contacts.

Enterprise customer evidence checklist

Talsoft TS

7. Vendors

- Critical vendor list.
- Vendor evaluation criteria.
- Available contractual or security evidence.
- Follow-up owner.

8. Awareness and people

- Evidence of training or communications.
- Participant register when applicable.
- Baseline rules for phishing, passwords, data and AI tools.

9. Reusable minimum evidence

- Folder by domain.
- Last update date.
- Owner for each evidence item.
- Notes about pending gaps.

10. What to avoid

- Do not invent controls.
- Do not promise certifications, approvals or absence of incidents.
- Do not share architecture, credentials, sensitive vendors or private data without criteria.
- Do not answer "yes" when the control only exists partially.

Suggested next step:

If evidence, owners or priorities are missing, consider an Initial GAP + Roadmap to organize gaps, risks and an action plan.