Vendor Risk Memo: example.com

Generated 2026-08-11 16:42 UTC - Decision support only, not a certification.

INSUFFICIENT DATA | Score 20/100 (F) | Documentation/Placeholder Domain

Executive summary

Example.com is a placeholder domain intended for documentation purposes and lacks any operational security controls or business infrastructure. The top strength is the presence of basic email authentication records (SPF/DMARC), while the top gap is the complete absence of security headers and organizational security documentation.

Collection was partial - this vendor's site uses bot protection that limits public evidence. Obtain vendor documentation (SOC 2, security whitepaper) directly for a complete assessment.

Key findings

[HIGH] Placeholder Domain Status

The domain is explicitly designated for documentation examples, indicating it is not a functional business entity or service provider.

[MEDIUM] Missing Security Headers

The site lacks critical browser security headers (HSTS, CSP, X-Frame-Options), increasing susceptibility to XSS and clickjacking if used in a production context.

[HIGH] Lack of Security Documentation

No evidence of SOC 2, ISO 27001, or data protection policies exists, preventing any formal risk validation.

Risk by domain

Compliance	**0/100**	gaps: 6
Data Security	**22/100**	gaps: 4
Operational	**0/100**	gaps: 2

Contract recommendations

- Do not enter into a contract; this entity is not a service provider.
- If this is a placeholder for a different vendor, request the actual vendor's legal entity name and security documentation.

Documents to request from example.com

Based on 19 unverified controls, prioritized by risk impact:

1. **SOC 2 Type II report**
   Please provide your most recent SOC 2 Type II report, including the bridge letter if the audit period ended more than 3 months ago.
2. **Encryption architecture summary**
   Please confirm encryption at rest (algorithm, key management, e.g. AES-256, KMS/HSM).
3. **Access control / SSO documentation**
   Please describe your RBAC model and confirm SSO/SAML support for enterprise accounts.
4. **AI/ML data use policy or DPA with AI clause**
   Please confirm in writing whether customer data is used to train AI/ML models, and if so, whether an opt-out mechanism exists.
5. **ISO 27001 certificate**
   Please provide your current ISO 27001 certificate and the Statement of Applicability.
6. **MFA policy**
   Please confirm MFA is enforced for all employee access to production systems.
7. **Data retention and deletion policy**
   Please provide your data retention schedule and confirm deletion timelines after contract termination.

8. Subprocessor list

Please provide your current list of subprocessors and commit to 30-day advance notice of changes.

9. Incident response plan summary

Please provide your incident response plan summary and confirm breach notification timelines (we require 72 hours or less).

10. Latest penetration test attestation

Please provide an attestation letter or executive summary from your most recent penetration test (full report not required).

Detailed control assessment

Control	Answer	Citation / verify note	Weight
SOC 2 Type II report	UNKNOWN	Request SOC 2 Type II report and bridge letter from the actual service provider.	15
Data encrypted at rest	UNKNOWN	Request architecture documentation confirming AES-256 encryption at rest.	10
Data encrypted in transit (TLS)	YES	TLS handshake succeeded, cert expires Oct 27 22:17:21 2026 GMT	10
Access controls / RBAC / SSO	UNKNOWN	Request documentation on SSO integration and RBAC implementation.	10
Trains AI models on customer data	UNKNOWN	Request explicit confirmation that customer data is not used for model training.	10
ISO 27001 certification	UNKNOWN	Request current ISO 27001 certificate and scope statement.	10
MFA enforced internally	UNKNOWN	Request evidence of mandatory MFA for all administrative and user access.	5
Data retention/deletion policy	UNKNOWN	Request data retention and deletion policy documentation.	5
Subprocessors disclosed	UNKNOWN	Request a list of all third-party subprocessors.	5
Incident response / breach notification	UNKNOWN	Request incident response plan and breach notification SLA.	5
Penetration testing performed	UNKNOWN	Request executive summary of the most recent third-party penetration test.	5
Data Processing Agreement available	UNKNOWN	Request standard Data Processing Agreement (DPA).	5
GDPR compliance stated	UNKNOWN	Request GDPR compliance statement or privacy policy.	5
Vulnerability disclosure / bug bounty	UNKNOWN	Request details on vulnerability disclosure program or bug bounty policy.	3
Audit logging	UNKNOWN	Request documentation on audit logging capabilities and retention periods.	3
Uptime SLA published	UNKNOWN	Request published uptime SLA and historical availability reports.	3
Employee background checks	UNKNOWN	Request confirmation of background check policy for employees with data access.	2
Backups / disaster recovery	UNKNOWN	Request disaster recovery plan and backup frequency documentation.	2
Vendor's own third-party risk program	UNKNOWN	Request overview of the vendor's third-party risk management program.	2
Data residency / region hosting	UNKNOWN	Request confirmation of primary data hosting regions.	2

Verification checklist for example.com

Items to verify directly with the vendor before signing:

[ ] Request SOC 2 Type II report and bridge letter from the actual service provider.

[ ] Request architecture documentation confirming AES-256 encryption at rest.

[ ] Request documentation on SSO integration and RBAC implementation.

[ ] Request explicit confirmation that customer data is not used for model training.

[ ] Request current ISO 27001 certificate and scope statement.

[ ] Request evidence of mandatory MFA for all administrative and user access.

[ ] Request data retention and deletion policy documentation.

[ ] Request a list of all third-party subprocessors.

[ ] Request incident response plan and breach notification SLA.

[ ] Request executive summary of the most recent third-party penetration test.

[ ] Request standard Data Processing Agreement (DPA).

[ ] Request GDPR compliance statement or privacy policy.

[ ] Request details on vulnerability disclosure program or bug bounty policy.

[ ] Request documentation on audit logging capabilities and retention periods.

[ ] Request published uptime SLA and historical availability reports.

[ ] Request confirmation of background check policy for employees with data access.

[ ] Request disaster recovery plan and backup frequency documentation.

[ ] Request overview of the vendor's third-party risk management program.

[ ] Request confirmation of primary data hosting regions.