VENDOR SECURITY ASSESSMENT

FRAMEWORK · QUESTIONNAIRE · SCORING · RISK TIERIN

By Dr. Erdal Ozkaya — CISO, NATO Cybersecurity Advisor, 17-time M

Author of 26 cybersecurity books · erdalozkaya.com

WHEN TO USE THIS QUESTIONNAIRE

- New vendor onboarding (pre-contract)
- Annual reassessment of existing vendors that handle sensitive data or are operationally
- Material change (vendor M&A, breach disclosure, change of subprocessors, AI feature
- Pre-renewal — use the result to anchor commercial terms

TIER → DEPTH OF ASSESSMENT

Tier 1 — Critical	Vendor handles regulated/sensitive data, is integral to core operatio environment. Full questionnaire + evidence + on-site/virtual review + clauses.
Tier 2 — Important	Material data access but not regulated, or operationally important bu review + biennial reassessment.
Tier 3 — Standard	Limited data access, low operational dependency. Short-form quest

HOW TO USE

1. Send the Questionnaire tab to the vendor. They populate the 'Vendor Answer' and 'Evi
2. Your team scores each answer (0–4) using the rubric on the Scoring Rubric tab. Don't
3. Risk Tiering tab auto-calculates overall risk score, domain breakdown, and tier recomr

4. Six Red Lines tab lists deal-breakers — any 'NO' here means escalate to CISO before

5. Use Decision Memo tab as the template for the documented risk-acceptance memo to

NG

Microsoft MVP

/ critical

launch)

ns, or has elevated privileges in your
+ annual reassessment + SLA breach

ut recoverable. Full questionnaire + evidence

ionnaire only. Reassess on material change.

idence Reference' columns.

accept marketing prose as evidence.

nendation.

- proceeding.
- procurement / legal.

v1.0

Vendor Security Asse

Vendor populates columns D–E.

#	Domain
1	Governance
2	Governance
3	Governance
4	Governance
5	Governance
6	Data Handling
7	Data Handling
8	Data Handling
9	Data Handling
10	Data Handling

11	Data Handling
12	Data Handling
13	IAM
14	IAM
15	IAM
16	IAM
17	IAM
18	Product Security
19	Product Security
20	Product Security
21	Product Security
22	Product Security

23	Infrastructure
24	Infrastructure
25	Infrastructure
26	Infrastructure
27	SecOps
28	SecOps
29	SecOps
30	Incident Response
31	Incident Response
32	Incident Response
33	Incident Response
34	BCM/DR

35	BCM/DR
36	BCM/DR
37	Personnel
38	Personnel
39	Personnel
40	AI / ML
41	AI / ML
42	AI / ML
43	AI / ML
44	Contractual
45	Contractual
46	Contractual

47	Contractual
48	Contractual

TOTALS

ssment Questionnaire — Dr. Erdal Ozkaya

CISO/Security team scores column F (0=No/Failed, 1=Partial, 2=Acceptable

Question
Is your information security programme certified to ISO/IEC 27001? Provide certification body, scope statement, and certificate ID. If SOC 2 Type II is held in lieu, provide the most recent report.
List all material compliance attestations (PCI DSS, HIPAA, FedRAMP, ISO 27017/27018, etc.) and the entities/services in scope.
Provide your published Information Security Policy and confirm board-level oversight of the security programme.
Name your CISO (or equivalent accountable executive) and provide their direct contact details.
Confirm you carry cyber liability insurance. Provide carrier, limit, and self-insured retention.
What classes of our data will you process (customer, employee, payment, health, intellectual property, regulated)?
Where is data stored, processed, and backed up (geographic regions, jurisdictions)? Confirm compliance with our data residency requirements.
List all subprocessors with name, function, jurisdiction. Confirm flow-down of security obligations to subprocessors.
Confirm encryption at rest (algorithm, key management) and in transit (TLS version, cipher suites) for our data.
Describe data segregation controls — how is our data isolated from other tenants and from your internal use?

Confirm support for customer-managed encryption keys (BYOK / HYOK) if applicable.
Describe data deletion process at contract termination: timelines, certification of destruction, retention exceptions.
Is MFA enforced for all administrative access to systems handling our data? Specify factor types — confirm phishing-resistant factors for privileged access.
Describe privileged access management: just-in-time elevation, session recording, vault, break-glass procedure.
How are joiner-mover-leaver events handled? Confirm SLA for revocation of access on termination.
Can you federate identity with our IdP (SAML/OIDC)? Confirm support for SCIM provisioning.
Describe access logging and retention. Confirm we can request export of access logs related to our tenant.
Describe your secure SDLC: threat modelling, secure coding training, SAST/DAST/SCA in CI, code review requirements.
Confirm vulnerability management SLAs: Critical (CVSS 9.0+), High (CVSS 7.0–8.9), Medium. Provide your historical adherence in the last 12 months.
Confirm penetration testing cadence (at minimum annual) and provide the most recent executive summary report.
Confirm a public vulnerability disclosure policy / bug bounty programme and provide the URL.
Describe dependency management: SBOM generation, software supply chain integrity, signed artefacts.

Describe network segmentation between production, non-production, and corporate environments.
List the security controls protecting customer-facing endpoints (WAF, DDoS, bot management, rate limiting).
Describe patch management cadence for OS, runtimes, container images. Provide last 12 months' compliance metrics.
Confirm endpoint protection deployed on all production and developer endpoints (EDR/XDR vendor + version).
Describe your security monitoring stack (SIEM, XDR) and 24/7 detection coverage.
Confirm log retention for our tenant access logs (minimum 12 months) and audit trail immutability.
Describe threat intelligence integration and proactive threat hunting activities.
Describe your incident response plan: detection, containment, eradication, recovery, post-incident. Confirm 24/7 IR coverage.
Confirm contractual breach notification SLA (e.g., 24/48/72 hours) and the trigger criteria. Provide the named IR contact details.
List material security incidents in the last 36 months affecting customer data. For each: nature, root cause, customers affected, remediation.
Confirm IR retainer or in-house DFIR capability. Provide annual tabletop exercise evidence.
State your contractual RTO and RPO for our services. Confirm last test date and results.

Describe backup architecture, encryption, immutability (object lock, etc.), and geographic separation from primary.
Confirm BCM exercise cadence (minimum annual) and provide most recent executive summary.
Confirm pre-employment background checks for all staff with access to customer data, including subcontractors.
Confirm mandatory security awareness training cadence and phishing simulation programme metrics.
Describe controls for offshore/contractor access — equivalent to employee controls?
Will any of our data be used to train, fine-tune, or improve AI/ML models (yours or third-party)? Describe consent and contractual basis.
If AI/LLM features are part of the product, describe data flow, prompt logging, output review, and protections against prompt injection and data leakage.
Confirm support for AI feature disable / opt-out at our tenant level.
Describe your AI governance programme. Confirm alignment with NIST AI RMF, ISO/IEC 42001, or EU AI Act risk classification where applicable.
Confirm right-to-audit clause acceptance: customer or independent auditor, with reasonable notice.
Confirm sub-processor change notice period (minimum 30 days) with right-to-object.
Confirm acceptable use of standard contractual clauses (SCCs) and / or Data Processing Agreement (DPA) execution.

Confirm cap on liability for security breach is uncapped or at least equal to a meaningful multiple of annual fees.
Confirm contract termination rights for material security incidents, regulatory orders, or repeated SLA breaches.

e, 3=Strong, 4=Best-in-class). Weight reflects domain importance for the deal context.

Vendor Answer	Evidence Reference	Score (0-4)	Weight
		0	3
		0	2
		0	2
		0	2
		0	2
		0	3
		0	3
		0	3
		0	3
		0	3

		0	1
		0	2
		0	3
		0	3
		0	2
		0	2
		0	2
		0	2
		0	3
		0	2
		0	1
		0	2

		0	2
		0	2
		0	2
		0	2
		0	3
		0	2
		0	1
		0	3
		0	3
		0	3
		0	2
		0	2

		0	2
		0	1
		0	2
		0	1
		0	2
		0	3
		0	3
		0	2
		0	2
		0	2
		0	2
		0	2

		0	3
		0	2
		0.00	**107.00**

Weighted	Reviewer Notes
0	
0	
0	
0	
0	
0	
0	
0	
0	
0	

0	
0	
0	
0	
0	
0	
0	
0	
0	
0	
0	
0	
0	

0	
0	
0	
0	
0	
0	
0	
0	
0	
0	
0	
0	
0	

0	
0	
0	
0	
0	
0	
0	
0	
0	
0	
0	
0	
0	

0	
0	

0.00 *Avg Score · Total Weight · Weighted Sum*

Scoring Rubric — What 0/1/2/3/4 Means

#	Score	Label	Definition
1	**0**	**No / Failed**	The control does not exist, or vendor cannot provide evidence. Treat marketing language without artefacts as 0.
2	**1**	**Partial**	Control exists but is informal, undocumented, or applied inconsistently. Evidence is verbal or sales-deck only.
3	**2**	**Acceptable**	Control is documented, implemented, and operating. Evidence is the actual artefact, not a description of the artefact.
4	**3**	**Strong**	Control is documented, implemented, regularly tested, with metrics reported to leadership. Evidence shows year-over-year improvement.
5	**4**	**Best-in-class**	Control is automated where possible, continuously monitored, externally validated, and integrated with broader risk management.

DISCIPLINE: An artefact is the document, the report, the screenshot, the saying 'we do that' is not an artefact. If the vendor cannot produce the art response window, score lower.

Examples of evidence at this level
No policy. No artefacts. 'We are working on it.' 'It's on our roadmap.'
Untested DR plan. SOC 2 in progress. Ad-hoc IR with no playbook.
ISO 27001 certificate (current). SOC 2 Type II report (last 12 months). Pen test executive summary.
Quarterly access reviews. Annual tabletop with results. Vulnerability SLA metrics for last 12 months.
Real-time SIEM-fed access reviews. Continuous control monitoring with auto-remediation. Independent audit certification.

certificate. A sales engineer tefact within a reasonable

Risk Tiering & Domain Roll-up

OVERALL SCORE

Weighted Sum	**0.0**
Total Weight	107.0
Max Possible (4 × Total We	428.0
Achieved %	**0.0%**
Tier Recommendation	**APPROVE — Mate**

DOMAIN BREAKDOWN

#	Domain	Questions	Avg Score	% of Max
1	Governance	5	0.00	0.0%
2	Data Handling	7	0.00	0.0%
3	IAM	5	0.00	0.0%
4	Product Security	5	0.00	0.0%
5	Infrastructure	4	0.00	0.0%
6	SecOps	3	0.00	0.0%
7	Incident Response	4	0.00	0.0%
8	BCM/DR	3	0.00	0.0%
9	Personnel	3	0.00	0.0%
10	AI / ML	4	0.00	0.0%
11	Contractual	5	0.00	0.0%

Status
Critical Gap
Critical Gap
Critical Gap
Critical Gap
Critical Gap
Critical Gap
Critical Gap
Critical Gap
Critical Gap
Critical Gap

The Six Red Lines — Deal-Breakers

Any 'NO' answer below is an automatic escalation to the CISO. The deal does not progres

#	Red Line	What we require
1	**Independent attestation**	ISO/IEC 27001 (current) OR SOC 2 Type II (last 12 months). Self-attestations do not count.
2	**Breach notification SLA**	Contractual SLA ≤ 72 hours from confirmed incident, with named 24/7 contact.
3	**Encryption in transit & at rest**	TLS 1.2+ in transit; AES-256 or equivalent at rest. Customer-managed keys available for regulated data.
4	**MFA on privileged access**	All vendor admin access to systems handling our data uses MFA. Phishing-resistant factors for tier-0 access.
5	**Right to audit**	Right-to-audit clause OR equivalent through an independent third-party attestation reviewable on request.
6	**AI training opt-out**	If AI/ML features process our data, explicit contractual confirmation that our data will not train shared models without explicit opt-in. Tenant-level disable available.

s without an explicit, documented exception.

Vendor (Y/N)	Notes / Exception Rationale

Vendor Risk Decision Memo

Use this memo to document the vendor risk decision. Save as PDF and attach to procurement record. Rec

Vendor name	
Vendor service / product	
Business sponsor	
Risk tier	Tier 1 / 2 / 3
Data classes processed	
Contract value (annual)	
Contract term	
Assessment date	
Overall achieved %	0.0%
Tier recommendation	DO NOT APPROVE — Material Risk
Red lines — any NO?	
Top 3 identified risks	
Compensating controls / risk mitigations	
Reassessment date	
Decision	APPROVE / APPROVE WITH CONDITIONS / REJECT
Conditions (if applicable)	
Approver (CISO or delegate)	
Approval date	

quired for Tier 1 & Tier 2 vendors.