

B2B Trust Readiness Navigator

50 buyer questions → spot uncertainty → choose 3 next steps

ORIENT • MARK • RED FLAGS • ACT

You do not need 50 perfect answers today.

You need visibility: what is defensible, what is only assumed, what is open—and which three actions reduce the largest buyer and trust risk?

20-minute quick scan plus validation

1 • Quick scan (20 min)

Mark all 50 questions only as B, P, O or N/A. Do not research yet; add notes only for red flags.

2 • Validation (60–120 min)

Review the three most important gaps with the responsible roles. Verify statements, contracts, settings and evidence at this stage.

3 • Act

Set exactly three next steps with owner, due date, completion criterion and expected evidence.

Not an audit, certification, legal advice or compliance guarantee. Answers must match your real product and contracts.

Your orientation logic

Status is not a grade

B — backed

Specific statement + current basis + owner.

P — partial

Some elements Release v1.0, but scope, evidence or approval is missing.

O — open

Do not guess. Track as uncertainty with a next step.

N/A

Add a short rationale; revisit when the product changes.

RED FLAG ≠ FAILURE. RED FLAG = NO EXTERNAL CLAIM UNTIL RESOLVED.

Prioritise now: unknown AI/data recipient; unrestricted support/admin access; deletion promise without backup/log exception; “compliant”, “secure” or “EU-only” without basis; critical provider without an outage route.

1. Data flows & processing

Why buyers ask	Data scope, purpose and routes drive risk, contracts and review effort.
Inputs needed	Product/data inventory, architecture, providers and environments.
Defensible answer	Purpose + data type + system/location + recipient + deletion; current and evidenced.
Dangerous shortcut	Name only the main database; omit support, logs, backups or AI routes.
Later use	Basis for a data-flow view, DPA, deletion and subprocessor statements.

Mark the questions

#	Buyer question	Status	Note
1	What customer data does your product actually process—and why?	☐ B ☐ P ☐ O ☐ N/A	_____
2	Which data is essential and which is optional?	☐ B ☐ P ☐ O ☐ N/A	_____
3	Where is personal data created, stored or changed?	☐ B ☐ P ☐ O ☐ N/A	_____
4	Which data leaves the EU or EEA?	☐ B ☐ P ☐ O ☐ N/A	_____
5	Can test, demo or support work access real customer data?	☐ B ☐ P ☐ O ☐ N/A	_____
6	How do you document key data flows for buyers, privacy and security review?	☐ B ☐ P ☐ O ☐ N/A	_____

2. AI/LLM use & transparency

Why buyers ask	AI changes data disclosure, failure modes and accountability.
Inputs needed	Feature list, model/provider, prompt context, training/retention and human gates.
Defensible answer	Per feature: input data, provider, output, control, boundary and fallback.
Dangerous shortcut	Say “we use AI safely” without provider terms or real control points.
Later use	Basis for an AI disclosure and defensible product/marketing claims.

Mark the questions

#	Buyer question	Status	Note
7	Which AI/LLM features are part of the product?	☐ B ☐ P ☐ O ☐ N/A	_____
8	Which customer data is sent to AI/LLM providers?	☐ B ☐ P ☐ O ☐ N/A	_____
9	Are prompts, files, outputs or usage data used for training?	☐ B ☐ P ☐ O ☐ N/A	_____
10	How do you distinguish AI, automation and human review for buyers?	☐ B ☐ P ☐ O ☐ N/A	_____
11	Which human approvals or control points cover high-impact AI outputs?	☐ B ☐ P ☐ O ☐ N/A	_____
12	How do you handle hallucinations, incorrect advice and uncertain outputs?	☐ B ☐ P ☐ O ☐ N/A	_____

3. Access, roles & permissions

Why buyers ask	Unclear rights and privileged access increase misuse and insider risk.
Inputs needed	Role model, IAM configuration, joiner/mover/leaver and support process.
Defensible answer	Roles, rights, approval, MFA, review, logging and removal align.
Dangerous shortcut	Use “only the core team has access” instead of technical restriction.
Later use	Basis for access matrix, support statement and buyer questionnaires.

Mark the questions

#	Buyer question	Status	Note
13	Which roles and permissions exist?	☐ B ☐ P ☐ O ☐ N/A	_____
14	Can customers understand who can access which data?	☐ B ☐ P ☐ O ☐ N/A	_____
15	How is privileged administrator access controlled?	☐ B ☐ P ☐ O ☐ N/A	_____
16	Is MFA available for admin and customer accounts?	☐ B ☐ P ☐ O ☐ N/A	_____
17	How are leavers and former contractors removed?	☐ B ☐ P ☐ O ☐ N/A	_____
18	How is support access restricted and logged?	☐ B ☐ P ☐ O ☐ N/A	_____

4. Logging, traceability & operations

Why buyers ask	Without logs and an operating route, incidents and promises are not traceable.
Inputs needed	Log sources, retention, alerting, incident route and status/SLA data.
Defensible answer	Event, source, access, period, alert and owner are named.
Dangerous shortcut	Promise more logging than you review or protect.
Later use	Basis for incident, monitoring and operational answers.

Mark the questions

#	Buyer question	Status	Note
19	Which security-relevant events are logged?	☐ B ☐ P ☐ O ☐ N/A	_____
20	How long are logs retained?	☐ B ☐ P ☐ O ☐ N/A	_____
21	Can customers trace their own activity or exports?	☐ B ☐ P ☐ O ☐ N/A	_____
22	How do you detect abuse, unusual usage or data leakage?	☐ B ☐ P ☐ O ☐ N/A	_____
23	How are incidents documented and prioritised?	☐ B ☐ P ☐ O ☐ N/A	_____
24	Which operational metrics or status information can buyers expect?	☐ B ☐ P ☐ O ☐ N/A	_____

5. Subprocessors, hosting & supply chain

Why buyers ask	Third parties determine location, availability, privacy and concentration risk.
Inputs needed	Current provider list, purposes, regions, contracts, evidence and change route.
Defensible answer	Each provider has purpose, data, location, criticality, evidence and change route.
Dangerous shortcut	Name cloud hosting only; forget AI, email, analytics and support tools.
Later use	Basis for subprocessor list, diligence and exit priorities.

Mark the questions

#	Buyer question	Status	Note
25	Which subprocessors do you use?	☐ B ☐ P ☐ O ☐ N/A	_____
26	What purpose does each subprocessor serve?	☐ B ☐ P ☐ O ☐ N/A	_____
27	Where are hosting, backups, logging and AI processing located?	☐ B ☐ P ☐ O ☐ N/A	_____
28	Which DPAs or security evidence are available from key providers?	☐ B ☐ P ☐ O ☐ N/A	_____
29	How are customers informed about new or changed subprocessors?	☐ B ☐ P ☐ O ☐ N/A	_____
30	Which providers would be critical if unavailable or compromised?	☐ B ☐ P ☐ O ☐ N/A	_____

6. Deletion, retention & portability

Why buyers ask	Customers need to know what is exported, deleted or lawfully retained.
Inputs needed	Data classes, systems, periods, backup cycles and export/deletion tests.
Defensible answer	Period and exception per data class; owner, process and evidence are testable.
Dangerous shortcut	Say “everything is deleted immediately” despite backups, logs or duties.
Later use	Basis for offboarding, retention schedule and defensible DPA answers.

Mark the questions

#	Buyer question	Status	Note
31	How can customers export their data?	☐ B ☐ P ☐ O ☐ N/A	_____
32	How does deletion work after contract end?	☐ B ☐ P ☐ O ☐ N/A	_____
33	Which data remains in backups, logs or billing systems?	☐ B ☐ P ☐ O ☐ N/A	_____
34	Which retention periods apply to product data, support data, logs and AI context?	☐ B ☐ P ☐ O ☐ N/A	_____
35	How is deletion evidenced technically and organisationally?	☐ B ☐ P ☐ O ☐ N/A	_____
36	Are owners clear for deletion requests?	☐ B ☐ P ☐ O ☐ N/A	_____

7. Security baseline & technical measures

Why buyers ask	Buyers want a credible baseline, not certification rhetoric.
Inputs needed	Configuration, backup/restore test, secrets, patch and vulnerability process.
Defensible answer	Implemented + owner + frequency + latest evidence + known boundary.
Dangerous shortcut	Present tool names or planned measures as effective controls.
Later use	Basis for security overview and prioritised technical improvements.

Mark the questions

#	Buyer question	Status	Note
37	How is data protected in transit and at rest?	☐ B ☐ P ☐ O ☐ N/A	_____
38	Which backup and restore procedures exist?	☐ B ☐ P ☐ O ☐ N/A	_____
39	How are secrets, API keys and credentials managed?	☐ B ☐ P ☐ O ☐ N/A	_____
40	How are dependencies, libraries and vulnerabilities monitored?	☐ B ☐ P ☐ O ☐ N/A	_____
41	Is there a process for security updates and critical patches?	☐ B ☐ P ☐ O ☐ N/A	_____
42	Which minimum measures can you credibly describe today without overclaiming?	☐ B ☐ P ☐ O ☐ N/A	_____

8. Buyer questions, claims & next steps

Why buyers ask

Inputs needed

Defensible answer

Dangerous shortcut

Later use

Conflicting claims slow sales and create liability and trust risk.

Current answers, claims, documents, deal dates and owners.

Openness is prioritised; every external statement has basis, owner and approval.

Hide gaps or cover them with “compliant/secure”.

Basis for three next steps, safe sales answers and upgrade decision.

Mark the questions

#	Buyer question	Status	Note
43	Which B2B buyer security questions can you answer safely today?	☐ B ☐ P ☐ O ☐ N/A	_____
44	Which questions must honestly remain open?	☐ B ☐ P ☐ O ☐ N/A	_____
45	Which marketing claims may go too far?	☐ B ☐ P ☐ O ☐ N/A	_____
46	Which materials are missing for a first procurement or privacy review?	☐ B ☐ P ☐ O ☐ N/A	_____
47	Which three gaps should be closed or covered by a clear interim answer before the next buyer conversation?	☐ B ☐ P ☐ O ☐ N/A	_____
48	Which next trust step creates the strongest sales benefit at lowest risk?	☐ B ☐ P ☐ O ☐ N/A	_____
49	Which statement would you give an enterprise buyer in writing—and which would you avoid?	☐ B ☐ P ☐ O ☐ N/A	_____
50	Which trust materials must be ready before the next major sales conversation?	☐ B ☐ P ☐ O ☐ N/A	_____

Action Sheet — next steps

From open questions to three feasible steps in 15 minutes	
Trigger / next buyer conversation	
Count B / P / O / N/A	
Most important scan pattern	
Biggest uncertainty	
Claim we will not use until verified	

Top three next steps

NEXT STEP 1	
Uncertainty / red flag	
Why it matters	
Next action	
Owner	
Due date	
Completion criterion	
Evidence location / record	

NEXT STEP 2

Uncertainty / red flag

Why it matters

Next action

Owner

Due date

Completion criterion

Evidence location / record

NEXT STEP 3

Uncertainty / red flag

Why it matters

Next action

Owner

Due date

Completion criterion

Evidence location / record

Decision rule

STOP: pause external claims when a data route, provider term or control evidence is unknown. CAUTION: label the gap and set owner/date. GO: answer only when specific, current and evidenced.

Review date: _____ Approver: _____ Buyer answer updated: _____

Completed fictional example — CloudKite AI

FICTIONAL — not a real company	
Trigger / next buyer conversation	Vendor review with MedicoWorks, 30 July 2026
Count B / P / O / N/A	18 / 17 / 13 / 2
Most important scan pattern	LLM-provider and support-access data flows are not consolidated.
Biggest uncertainty	Whether prompt/output retention is disabled under the current provider terms.
Claim we will not use until verified	"EU-only processing"

Top three next steps

NEXT STEP 1	
Uncertainty / red flag	AI retention under the current provider terms is unclear
Why it matters	An incorrect statement about prompt use could stop the vendor review.
Next action	Review the DPA and admin setting together; draft an approvable statement.
Owner	Mira / CTO
Due date	17 Jul 2026
Completion criterion	CTO reviewed the statement and the buyer-answer set was updated.
Evidence location / record	DPA v3.2 + dated screenshot of the admin setting.

NEXT STEP 2	
Uncertainty / red flag	Support access is not consistently logged
Why it matters	Unevidenced privileged access is a concrete buyer and incident risk.
Next action	Test JIT access with a ticket ID in staging and update the procedure.
Owner	Jonas / Engineering
Due date	22 Jul 2026
Completion criterion	Test passed; ticket, approval and log chain are traceable.
Evidence location / record	TEST-LOG-014 + procedure SUP-02 v0.3.

NEXT STEP 3	
Uncertainty / red flag	Backup deletion is not explained
Why it matters	A blanket deletion promise is not defensible without a backup exception.
Next action	Document backup cycles and exceptions; bound the buyer answer.
Owner	Mira / CTO
Due date	24 Jul 2026
Completion criterion	Retention answer approved and added to the DPA FAQ.
Evidence location / record	Retention table v0.1 + review note dated 24 Jul 2026.

Decision rule

STOP: pause external claims when a data route, provider term or control evidence is unknown. CAUTION: label the gap and set owner/date. GO: answer only when specific, current and evidenced.

30-day result: AI disclosure v0.1, logged support access and a defensible retention answer; no compliance claim.

If you want to go further

Optional orientation: if your three actions mainly concern scope, responsibilities and defensible working structures, the ISMS Scope & Governance Starter Kit, with an intended price of EUR 199, may be a suitable self-service step. This VERSION 1.0 Release v1.0 does not claim that the kit is currently available. It structures the start but does not replace case-specific review or advice.

Before sharing

- Use only confirmed statements externally.
- Keep open items visible; do not close them cosmetically.
- Redact confidential architecture, customer and access data.
- Add owner and last-updated date.

A-R-C Andreas Rühl Consulting · SaaS Enablement Consulting · a.ruehl@a-r-c.me · www.a-r-c.me