DILIGENCE RESCUE

Illustrative Mapped Evidence Response Pack

Fictional example: Northstar Metrics (B2B SaaS)

IMPORTANT: This is a fictional worked example created to show the Diligence Rescue method. It is not customer data, not independent assurance, and not evidence that Northstar Metrics exists or has any stated control.

What Diligence Rescue is for

- One live buyer security questionnaire or diligence request.
- Map each question to evidence the founder actually has.
- Separate supported claims from self-attestation, gaps, ambiguity, and hard independent-assurance requirements.
- Produce buyer-facing wording without hiding founder-only limitations.

Example engagement snapshot

Company	Northstar Metrics (fictional)
Team	7-person B2B SaaS team
Stack	GitHub, Vercel, Supabase, Google Workspace
Buyer request	Enterprise vendor-security questionnaire
Review scope	Illustrative subset of 8 questions

Method: understand the buyer's intent -> identify the relevant scope -> map available evidence -> expose gaps -> draft only what the evidence can support.

1. Evidence status model

The status is not a certification score. It describes what the current evidence supports for this specific question and scope.

EVIDENCE IDENTIFIED	Specific evidence has been identified and reviewed for consistency with the scoped statement. This is not independent verification of authenticity, completeness, currency, or operating effectiveness.
PARTIALLY SUPPORTED	Some of the claim is evidenced, but the buyer's full scope is not yet covered.
SELF-ATTESTED	The company reports the control/process as true, but supporting evidence has not been identified.
EVIDENCE MISSING	The requested control/evidence cannot currently be substantiated.
NEEDS CLARIFICATION	The buyer wording or company scope must be clarified before a defensible answer is possible.
NOT APPLICABLE	Based on the stated scope, the requirement does not appear applicable. The basis for that conclusion should be recorded.
INDEPENDENT ASSURANCE REQUIRED	The buyer is asking for an external artifact Vauntico cannot create or substitute.

Evidence recency: Each evidence item in this illustrative pack carries an observed or referenced date. The status applies only to the evidence reviewed as of that date; configurations and operating state can change afterward.

2. Buyer-facing security review summary

Illustrative wording suitable for the customer-facing response layer. Internal gaps and next actions are kept in the founder-only section that follows.

Buyer topic	Status	Buyer-facing summary
MFA for production access	PARTIALLY SUPPORTED	MFA evidence identified for GitHub organization access. Coverage of additional production-administration paths is still being confirmed.
Encryption at rest	EVIDENCE IDENTIFIED	Application data is hosted in Supabase/Postgres and provider-managed encryption at rest is documented for the service. Scope is limited to the systems described.
Backups and recovery	SELF-ATTESTED	Provider-managed backups are reported. Retention and restoration-test evidence has not yet been identified.
Incident response	EVIDENCE MISSING	No formal incident-response policy or dated exercise evidence has been identified.
Independent penetration test	INDEPENDENT ASSURANCE REQUIRED	No independent penetration-test report is available. Vauntico cannot substitute for a buyer requirement for an external test.
SOC 2	INDEPENDENT ASSURANCE REQUIRED	The company is not SOC 2 certified. This must be stated plainly if requested.
Subprocessors	PARTIALLY SUPPORTED	A current vendor inventory identifies third-party services in use. Which providers actually process customer data as subprocessors still needs to be confirmed before a buyer-facing subprocessor disclosure is finalized.

Buyer topic	Status	Buyer-facing summary
Production access review	NEEDS CLARIFICATION	Named administrators are known, but the buyer's requested review cadence and evidence format require clarification.

3. Mapped response examples

Each item shows the buyer question, what it is really asking, evidence available in this fictional scenario, safe buyer-facing wording, and the private founder note.

01	**Do you enforce multi-factor authentication for all production access?**

What the buyer is actually asking The buyer is asking whether every identity capable of reaching production systems is required to use MFA - not merely whether the founder personally uses MFA.

Evidence identified

- GitHub organization setting requiring 2FA for organization members (illustrative evidence date: 2 Sep 2026).
- Named production repository administrators confirmed as GitHub organization members subject to that requirement (illustrative evidence date: 2 Sep 2026).

PARTIALLY SUPPORTED	**Buyer-facing wording:** MFA is enforced for GitHub organization members with production repository access. Coverage of Supabase administrative access and any other direct production paths is currently being confirmed.

FOUNDER-ONLY NOTE Do not answer “Yes - all production access” until every administrative path is identified and MFA enforcement is evidenced. Obtain Supabase/admin access evidence before broadening the claim.

02	**Is customer data encrypted at rest?**

What the buyer is actually asking The buyer wants to know whether stored customer data is encrypted, where that control is provided, and which stores are in scope.

Evidence identified

- Supabase documentation describing encryption at rest for the referenced database service (illustrative reference date: 2 Sep 2026).
- Architecture note showing customer application data stored in Supabase/Postgres (illustrative evidence date: 2 Sep 2026).

EVIDENCE IDENTIFIED	**Buyer-facing wording:** According to the provider documentation referenced for the current service, customer application data stored in the Supabase-hosted PostgreSQL database is encrypted at rest using provider-managed controls. This statement applies only to the application data stores described in the current architecture.

FOUNDER-ONLY NOTE Keep the scope narrow. Do not imply every possible file, export, local developer copy, or third-party system is covered unless separately evidenced.

03	**Are backups performed and regularly tested for restoration?**

What the buyer is actually asking The buyer is asking two things: whether backups exist, and whether restoration is periodically proven to work.

Evidence identified

- Founder reports provider-managed backups are enabled (self-attestation recorded 2 Sep 2026).

SELF-ATTESTED	**Buyer-facing wording:** Provider-managed backup capability is used for the production database. Backup retention and restoration-test evidence are being confirmed; we do not currently claim a documented periodic restoration test.

FOUNDER-ONLY NOTE This is not fully supported. Gather provider backup configuration/retention evidence and perform/document a restoration test before answering “Yes” to both parts.

04	**Do you maintain and test an incident response plan?**

What the buyer is actually asking The buyer wants evidence that incident responsibilities, escalation, communication, and recovery steps are documented and exercised.

Evidence identified None identified for the requested artifact/control.

EVIDENCE MISSING	**Buyer-facing wording:** A formal, tested incident-response plan has not yet been evidenced. The company should not represent this control as fully implemented until a documented plan and testing record exist.

FOUNDER-ONLY NOTE Do not turn informal founder knowledge into a formal-control claim. This is a real gap, not a wording problem.

05	**Provide the executive summary of your most recent independent penetration test.**

What the buyer is actually asking This is a request for third-party assurance, not a request for a self-description of secure coding practices.

Evidence identified None identified for the requested artifact/control.

INDEPENDENT ASSURANCE REQUIRED	**Buyer-facing wording:** No independent penetration-test report is currently available. If an independent test is a condition of progression, this requirement must be addressed through an appropriate external security-testing provider.

FOUNDER-ONLY NOTE Vauntico cannot substitute for this artifact. Ask the buyer whether the report is mandatory for the current pilot/contract and what scope/recency they require.

06	**Are you SOC 2 Type II certified?**

What the buyer is actually asking The buyer is asking for formal independent assurance covering an operating period. A roadmap, policy set, or self-attestation is not the same thing.

Evidence identified None identified for the requested artifact/control.

INDEPENDENT ASSURANCE REQUIRED	**Buyer-facing wording:** No. Northstar Metrics is not SOC 2 Type II certified. If SOC 2 Type II is a mandatory condition of onboarding, an evidence pack cannot replace that requirement.

FOUNDER-ONLY NOTE Do not say “SOC 2 aligned” unless there is a precise, defensible basis and a reason to use that wording. Clarify whether the buyer permits alternatives for the current risk tier.

07	List the subprocessors that may process customer data.

What the buyer is actually asking The buyer needs to understand which third parties may handle customer data and for what purpose.

Evidence identified

- Current architecture/vendor inventory identifying Vercel, Supabase, GitHub, and Google Workspace roles (illustrative evidence date: 2 Sep 2026).

PARTIALLY SUPPORTED	**Buyer-facing wording:** The current vendor inventory identifies third-party services used for application hosting, database services, source-code operations, and business productivity. Which of these providers process customer data as subprocessors has not yet been fully scoped, so this should not yet be presented as a finalized subprocessor disclosure.

FOUNDER-ONLY NOTE Confirm the data-processing role of each provider before presenting a buyer-facing subprocessor list. A vendor being used by the company does not automatically make it a subprocessor of customer data.

08	How often do you review privileged access to production systems?

What the buyer is actually asking The buyer wants a defined review cadence and evidence that privileged access is periodically reassessed.

Evidence identified

- Current list of named production administrators (illustrative evidence date: 2 Sep 2026).

NEEDS CLARIFICATION	**Buyer-facing wording:** Current privileged administrators can be identified. A formal recurring access-review cadence and dated review record have not yet been evidenced. We can provide the current administrator scope and clarify the review evidence required.

FOUNDER-ONLY NOTE If no formal cadence exists, do not invent one. Clarify whether the buyer needs a current access list, a dated review record, or a policy requirement.

4. Founder-only gap and action map

This page is not intended to be forwarded to the buyer unchanged. It is the founder's private map of what can be answered now, what must be scoped, and what requires additional work or independent assurance.

#	Action	Why it matters	Priority	Owner
1	Confirm MFA coverage beyond GitHub	Before claiming “all production access”	**High**	Founder / system admin
2	Capture backup retention evidence and perform/document restore test	Moves backup answer from self-attested toward supported	**High**	Founder / technical lead
3	Create a practical incident-response plan and record first tabletop/test	Closes a genuine operational/documentation gap	**High**	Founder
4	Clarify buyer pentest requirement (scope, recency, mandatory vs pilot exception)	Avoids wasting time if this is a hard gate	**High**	Founder / buyer contact
5	Clarify whether SOC 2 Type II is mandatory for current opportunity	Determines whether evidence mapping can progress the deal	**High**	Founder / procurement
6	Confirm provider data-processing roles and finalize scoped subprocessor list	Prevents vendor inventory from being mistaken for a customer-data subprocessor disclosure	**Medium**	Founder
7	Define and record privileged-access review cadence	Creates evidence for future reviews	**Medium**	Founder / technical lead

What not to send Vauntico

Do not send passwords, API keys, private keys, access tokens, live credentials, unredacted secrets, or unnecessary customer personal data. Redact company names, deal values, and identifiers you prefer to keep private. If in doubt, ask before sending.

What this example does not prove

- It does not certify the fictional company as secure or compliant.
- It does not replace SOC 2, ISO 27001, an independent audit, or a penetration test when the buyer requires one.
- It does not guarantee buyer acceptance or deal closure.
- It does not convert a founder statement into verified evidence.

Diligence Rescue - R1,500 once

Security questionnaire help for one live buyer request. Fit is confirmed before payment.

No audit, certification, independent assurance, buyer acceptance, or deal-closure guarantee.

Suggested CTA: See if Diligence Rescue fits