



Supplier Security Review

Draft sample output — illustrative example of an independent review of supplier security information against defined business and contractual requirements.

Client	Kranitech Analytics Ltd	Supplier	the supplier
Scope	Security assessment of one supplier	Review date	04 September 2026
Material provided	Security questionnaire, security overview, data processing documentation, business continuity summary, service description and contractual security schedule	Output	Supplier security assessment + follow-up actions

Executive summary

Purpose. Kranitech Analytics Ltd requested an assessment of the supplier's security posture before onboarding or continued use of the service. The review considers the service provided, information handled, business dependency and the security expectations applicable to the supplier relationship.

Review performed. The supplier information and supporting documentation were examined against the requirements provided for the engagement. The assessment considered security governance, data handling, identity and access arrangements, service resilience, vulnerability management, service dependency, exit arrangements and assurance information where relevant.

Overall position. The available material indicates a broadly established security environment, with several relationship-specific points requiring confirmation. The main areas concern data deletion and return, recovery commitments, vulnerability disclosure, service dependency and the evidence available for continuity arrangements.

Recommended next step. Complete the supplier assessment subject to closure of the identified points. The outstanding matters should be confirmed with the supplier and, where material to the relationship, reflected in the applicable contractual or security requirements.

Assessment position

16	9	4	3
areas reviewed	adequately addressed	clarification	follow-up required

Security assessment position

Adequately addressed		9
Clarification		4
Follow-up required		3



Key supplier security concerns

01 Data return and deletion

Clarification

The supplier documentation describes data retention and deletion at a general level, but the material does not clearly define the process and timing for returning or securely deleting customer information at service termination.

Source: Service terms / data handling documentation

02 Recovery commitments

Follow-up

Business continuity information describes recovery arrangements, but the service-specific recovery objectives and the customer-facing commitments applicable to the service are not clearly stated.

Source: Service continuity documentation / contractual requirement

03 Vulnerability disclosure

Clarification

The supplier describes vulnerability management, but the available material does not clearly explain how customer-relevant vulnerabilities are communicated, including the information provided and expected communication path.

Source: Supplier security overview / vulnerability management information

04 Service dependency and concentration

Follow-up

The service relies on underlying technology and external dependencies. The available documentation does not provide sufficient visibility of the dependencies that could materially affect service availability or continuity.

Source: Service description / supplier dependency information

Recommended follow-up

High Confirm data return and deletion process

Confirm the applicable process, timing and responsibility for returning or securely deleting customer information when the service ends.

High Confirm service-specific recovery commitments

Obtain the recovery objectives applicable to the service and confirm how continuity commitments are communicated to customers.

Medium Clarify vulnerability disclosure

Confirm how material vulnerabilities affecting the service are communicated to customers and what information is provided for risk assessment.

Medium Document material service dependencies

Identify dependencies that could materially affect service delivery and clarify how dependency-related disruption is managed.



Supplier security assessment

The assessment below illustrates how supplier information can be considered against the requirements relevant to the relationship, including the evidence available and any resulting action.

Ref.	Assessment area	Supplier position	Evidence considered	Outcome
S-01	Data handling	Data handling practices are described for customer information and service operations.	Data processing documentation; service description.	Addressed
S-02	Data return & deletion	Retention and deletion are addressed, but termination-time commitments require clarification.	Data handling documentation; service terms.	Clarify
S-03	Service continuity	Continuity arrangements are described, but service-specific recovery objectives are not clearly stated.	Business continuity summary; service documentation.	Follow-up
S-04	Vulnerability management	A vulnerability management process is described; customer communication arrangements require confirmation.	Security overview; vulnerability management summary.	Clarify
S-05	Service dependencies	Underlying dependencies are referenced, but material dependency visibility is limited.	Service description; dependency information.	Follow-up
S-06	Security governance	Security responsibilities and policy ownership are described at supplier level.	Supplier security overview; governance summary.	Addressed

Overall recommendation

Proceed with clarification. The supplier presents a generally established security environment based on the information reviewed. Approval can be considered subject to closure of the identified points, particularly data return and deletion, recovery commitments, vulnerability disclosure and material service dependencies.

Overall position

Proceed with clarification

16 assessment areas reviewed
 9 addressed · 4 clarification · 3 follow-up
 Focus first on service exit, recovery, vulnerability disclosure and dependencies.

Scope and limitation

This review assesses supplier security information and documentation supplied for the engagement. It does not independently test the supplier's systems, validate technical controls or provide a legal opinion. Regulatory or contractual requirements are considered only insofar as they form part of the information and requirements provided for the review.