



Compliance Quick Scan

Draft sample output — illustrative example of a focused review of existing documentation against defined security and compliance requirements.

Client	Kranitech Analytics Ltd	Framework	ISO 27001:2022
Scope	Information security governance and access control	Review date	04 September 2026
Material provided	Information Security Policy, Access Control Policy, Risk Register, Incident Response Policy, Supplier Security Procedure	Output	Gap report + remediation priorities

Executive summary

Purpose. Kranitech Analytics Ltd requested a focused review of its existing cybersecurity documentation against the defined ISO 27001:2022 requirements within the agreed scope. The review is intended to identify documented gaps and areas requiring attention without performing a full certification readiness assessment.

Review performed. The five documents provided were examined against the requirements relevant to information security governance and access control. The review considered whether the documented arrangements address the requirement, whether responsibilities and processes are sufficiently described, and whether supporting documentation appears complete.

Overall position. The documentation shows a reasonable foundation, but several areas require improvement. The principal issues relate to risk treatment tracking, privileged access review evidence, incident escalation criteria and supplier security requirements. These findings should be addressed before the documentation is relied upon as evidence of full alignment.

Recommended next step. Address the identified gaps in order of importance, update the affected documents and retain supporting evidence where applicable. The scan provides a practical starting point for deciding where further work is required.

Compliance snapshot

18	10	5	3
requirements reviewed	aligned	partial alignment	gaps

Requirement position





Key gaps and areas requiring attention

01 Risk treatment tracking

Gap

The risk register records identified risks and owners, but the available material does not consistently show treatment decisions, target dates and closure status for each risk.

Source: ISO 27001:2022 — risk treatment / documented information

02 Privileged access review

Partial alignment

The Access Control Policy requires periodic access review, but no defined review frequency or evidence of completed privileged-access reviews was included in the material provided.

Source: ISO 27001:2022 — access control

03 Incident escalation criteria

Partial alignment

The Incident Response Policy describes incident handling but does not clearly define escalation thresholds or responsibilities for incidents with significant business impact.

Source: ISO 27001:2022 — incident management

04 Supplier security requirements

Gap

The Supplier Security Procedure refers to supplier assessment but does not clearly define the minimum security requirements to be applied to higher-risk suppliers.

Source: ISO 27001:2022 — supplier relationships

Recommended improvements

High Define risk treatment status and target dates

Update the risk register so treatment decisions, owners, target dates and closure status can be tracked consistently.

High Formalise privileged access review evidence

Set a defined review frequency and retain evidence showing completion and follow-up of privileged access reviews.

Medium Clarify incident escalation thresholds

Add criteria for escalation, including responsibilities and notification paths for material security incidents.

Medium Strengthen supplier security requirements

Define minimum security expectations for suppliers according to service criticality, data access and risk.

Gap register

The register below illustrates how findings can be recorded against the agreed requirements, with the current documentation position and recommended improvement.

Ref.	Requirement area	Current position	Recommended improvement	Status
R-01	Risk treatment	Risk treatment decisions and target dates are not consistently recorded.	Update the risk register to show treatment decision, owner, target date and closure status.	Gap
R-02	Privileged access	Periodic review is stated, but frequency and completed review evidence are not defined.	Set review frequency and retain evidence of completed privileged-access reviews.	Partial
R-03	Incident escalation	Incident handling is documented, but escalation thresholds are not sufficiently clear.	Define materiality thresholds, escalation responsibilities and notification paths.	Partial
R-04	Supplier security	Supplier assessment is described, but minimum security requirements for higher-risk suppliers are not defined.	Introduce minimum security requirements linked to supplier risk and service criticality.	Gap
R-05	Security responsibilities	Core responsibilities are described across policies, but ownership is not always explicit for control activities.	Clarify accountable owners for recurring security activities and document review responsibilities.	Partial
R-06	Policy review	Policy review is required, but evidence of the latest review is not consistently referenced.	Record review dates, approver and resulting actions for each relevant policy.	Aligned

Overall compliance snapshot

Based on the documentation reviewed within the agreed scope, the organisation demonstrates a reasonable level of documented alignment, with several areas requiring improvement. The findings do not represent a certification assessment and should not be interpreted as a statement of compliance with ISO 27001 as a whole.

Overall position

18 requirements reviewed

Improvements required

10 aligned · 5 partial · 3 gaps

Priority should be given to the four key areas identified on page 2.

Scope and limitation

This review covers only the defined scope and the documents provided for the engagement. It does not independently verify technical controls, test systems or determine legal/regulatory applicability. The findings reflect the documentation available at the time of review.