



Contract Security Requirements Review

Draft sample output — illustrative example of a professional review of contractual cybersecurity requirements.

Client	Kranitech Analytics Ltd	Agreement	Managed Cloud Services Agreement v3.1
Supplier	the supplier	Review date	04 September 2026
Scope	15 security-related provisions	Output	Security requirements review + follow-up points

Executive summary

Purpose. Kranitech Analytics Ltd requested a review of the cybersecurity provisions contained in its Managed Cloud Services Agreement with the supplier. The review focuses on obligations relating to information security, incident management, access, data handling, continuity, subcontracting and assurance.

Review performed. The security-related clauses and Schedule 4 — Security Requirements were examined individually. Each provision was considered for clarity, allocation of responsibility, level of obligation and consistency with the security expectations stated elsewhere in the agreement. Relevant reference points included the customer's internal security requirements, ISO 27001-aligned controls and applicable data protection obligations. This is a cybersecurity and contractual requirements review, not legal advice or a legal opinion.

Overall position. The agreement contains a substantial set of security obligations, but several provisions would benefit from clarification before signature. The main concerns relate to incident notification timescales, security testing frequency, subcontractor obligations and audit rights. A smaller number of clauses contain broad wording that may make the supplier's expected level of performance difficult to determine.

Recommended next step. The contract can progress to commercial or legal review once the identified security points have been considered. The report separates provisions that are adequately stated from those that may warrant amendment, clarification or further discussion.

Review position

15 provisions examined	9 adequately stated	4 clarification	2 amendment / negotiation
----------------------------------	-------------------------------	---------------------------	-------------------------------------

Provision review position

Adequately stated		9
Clarification		4
Amendment / negotiation		2



Key contractual concerns

01 Incident notification

The agreement requires notification “without undue delay”, while Schedule 4 refers to prompt notification. Neither provision establishes a defined maximum timeframe for security incidents affecting customer information.

Source: Contract clauses 8.2 and Schedule 4 §4

02 Security testing

The supplier is required to conduct periodic security testing, but the agreement does not specify a minimum frequency or define what assurance information must be made available to the customer.

Source: Schedule 4 §7 / customer security requirement

03 Subcontractors

The supplier may use subcontractors with prior notice, but the security obligations that must be passed to them are not stated in sufficient detail.

Source: Contract clause 11.3 / supplier security requirement

04 Audit rights

The customer has a general right to request security information, but the circumstances, notice period and scope of customer assurance requests are not clearly defined.

Source: Schedule 4 §9 / customer security requirement



Illustrative security requirements register

The following extract demonstrates the format used to review individual contractual security provisions. The source column shows where the requirement originates, while the review position distinguishes adequate wording from matters requiring attention.

Ref.	Requirement source	Security provision	Review position	Outcome
CSR-01	Contract §8.2	Security incidents must be notified without undue delay.	Wording is broad and lacks a defined maximum timeframe.	Clarify
CSR-02	Schedule 4 §3 / ISO 27001-aligned requirement	Supplier shall maintain an information security management framework appropriate to the service.	Requirement is clearly stated; supporting framework reference is appropriate.	Adequate
CSR-03	Schedule 4 §4	Supplier shall notify the customer promptly of incidents affecting customer data.	Meaning overlaps with §8.2 but still does not establish a measurable timeframe.	Clarify
CSR-04	Schedule 4 §5 / data protection requirement	Customer data shall be protected against unauthorised access, disclosure and loss.	Core obligation is clear and consistent with the stated data protection expectations.	Adequate
CSR-05	Schedule 4 §7	Security testing shall be performed periodically and results made available on request.	Frequency and minimum assurance expected are not defined.	Amend / negotiate
CSR-06	Clause 11.3 / supplier security requirement	Subcontractors may be appointed following prior customer notice.	The clause does not clearly require equivalent security obligations to flow down.	Amend / negotiate
CSR-07	Schedule 4 §9	Customer may request reasonable security information relating to the service.	Right is useful but scope and process for assurance requests are not defined.	Clarify
CSR-08	Schedule 4 §10 / ISO 27001-aligned requirement	Supplier shall maintain business continuity arrangements for the service.	Requirement is stated at a suitable level for the agreement.	Adequate

Suggested points for follow-up

Topic	Suggested discussion point
Incident notification	Consider a defined notification timeframe, for example 24 hours from confirmation of a security incident affecting customer information.
Security testing	Specify a minimum testing frequency and the type of assurance material to be made available to the customer.
Subcontractors	Require relevant security obligations to be passed to subcontractors handling customer systems or information.
Audit and assurance	Define reasonable parameters for customer information requests, including scope, notice and confidentiality.

Overall recommendation

Proceed with clarification. The agreement contains the main security subjects expected for the service, but four areas should be clarified and two provisions may warrant amendment or negotiation before signature. The report does not determine whether the contractual language is legally sufficient; it identifies cybersecurity requirements and wording that may merit attention by the appropriate business, security or legal owners.



Security requirements summary

This page summarises the principal security obligations identified in the agreement and the source used for the review.

Source	How it is used	Examples
Customer contract	Defines obligations that the response must address where applicable.	Incident notification, retention, assurance commitments
Customer questionnaire	Sets the customer's requested security information and response expectations.	Policies, access control, continuity, operational practices
ISO 27001:2022	Provides a recognised information-security reference where invoked by the customer or relevant to the question.	Governance, access, continuity, assurance
NIST CSF 2.0	Provides security outcome terminology where requested or used as a reference.	Identify, Protect, Detect, Respond, Recover
Applicable data protection requirements	Provides relevant obligations affecting personal or customer data.	Retention, handling, confidentiality, safeguards

Scope and limitation

This sample reviews cybersecurity and information-security requirements contained in a fictional commercial agreement. It is not a legal review, does not assess enforceability or regulatory legal applicability, and does not replace advice from qualified legal counsel. The examples are illustrative and use fictional organisations, clauses and findings.

Delivery note

The final Cysnova deliverable would be based on the contract and supporting material supplied for the engagement, with security provisions examined individually and points requiring clarification or negotiation clearly identified.