

Security Questionnaire Support

Draft sample output — illustrative example of a professionally prepared customer security questionnaire response package.

Client	Northbridge Analytics Ltd	Questionnaire	Customer Security Assessment v4.2
Package	Standard · 100 questions	Review date	04 September 2026
Material provided	Policies, ISO certificate, previous questionnaire responses and supporting notes	Output	Completed response package + clarification points

Executive summary

Purpose. Northbridge Analytics Ltd engaged Cysnova to support completion of a 100-question customer security assessment. The questionnaire covers information-security governance, access management, incident handling, business continuity, data handling and assurance activities. The intended outcome is a customer-ready response set, while clearly identifying any questions that cannot be answered from the information available.

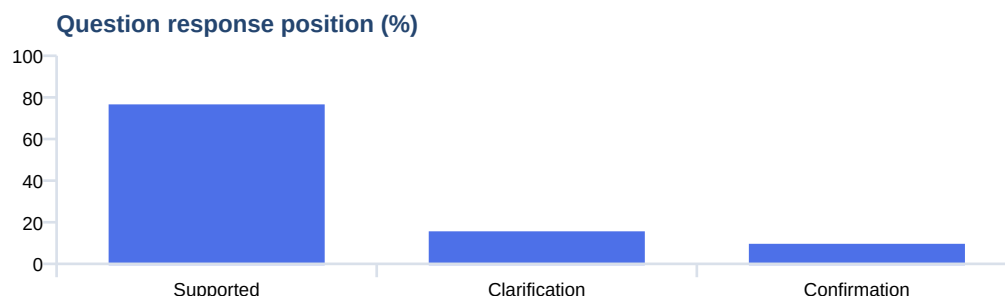
Work performed. Each question was reviewed individually by a cybersecurity professional. Responses were prepared from the information supplied by the client and relevant supporting material, including existing policies, certification material and previous questionnaire responses. Where a question referred to a specific customer expectation or contractual requirement, that source was considered alongside the organisation's own documentation. No unsupported claim was introduced where the available material was insufficient.

Response quality and coverage. The questionnaire is substantially completed. 76 questions are supported by the material reviewed, 15 require clarification or additional supporting detail, and 9 require direct confirmation from the client before submission. Existing material has been used where relevant to reduce duplication and maintain consistent terminology across related answers.

Key conclusion. The response package is suitable for final client review, subject to closure of the identified open points. The principal items concern the incident notification timeframe, customer-specific data retention and the frequency of independent security testing. These points are explicitly flagged in the response register rather than inferred from generic policy language.

Response position

100 questions reviewed	76 supported	15 clarification	9 confirmation
----------------------------------	------------------------	----------------------------	--------------------------



Key points requiring attention

01	Incident notification The customer questionnaire requires notification within 24 hours. The client's existing policy refers to prompt notification but does not state a fixed timeframe. Requirement source: Customer contractual requirement
-----------	--

02

Data retention

The customer asks for a defined retention period. The available policy establishes a general retention principle but does not confirm a customer-specific period.

Requirement source: Customer requirement + data protection obligation

03

Independent testing

The customer asks whether independent security testing is performed annually. Available material confirms periodic testing but does not evidence an annual frequency.

Requirement source: Customer questionnaire + ISO 27001-aligned requirement

SAMPLE

Illustrative response register

This extract shows how the completed response can identify the source of each requirement, use existing material and distinguish supported answers from points requiring confirmation. The full deliverable would contain the customer's questionnaire with responses prepared throughout.

Ref.	Requirement source	Customer question	Prepared response	Status
SEC-01	Customer questionnaire / ISO 27001:2022	Do you maintain a formal information security policy?	Yes. The Information Security Policy is maintained and reviewed periodically.	Support ed
SEC-07	Customer questionnaire / ISO 27001:2022	Do you operate access controls based on least privilege?	Yes. Access is assigned according to role and business need. Supporting policy material was considered.	Support ed
INC-04	Customer contract	Will security incidents affecting the customer be reported within 24 hours?	Current material supports prompt notification but does not confirm a 24-hour commitment. Client confirmation required.	Confirm
DAT-11	Customer contract / data protection requirement	What is the retention period for customer data?	A general retention policy is available, but no customer-specific period is stated. Please confirm the applicable commitment.	Confirm
ASS-03	Customer questionnaire / ISO 27001-aligned requirement	Is independent security testing performed at least annually?	Periodic independent testing is performed. Annual frequency was not evidenced in the supplied material.	Clarify
BCP-06	Customer questionnaire / ISO 27001:2022	Do you maintain business continuity and disaster recovery arrangements?	Yes. Business continuity and recovery arrangements are documented and subject to periodic review.	Support ed

Requirement source overview

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

Client confirmation points

- Confirm whether a 24-hour incident notification commitment can be accepted.
- Confirm the retention period or contractual rule applicable to customer data.
- Confirm whether independent security testing is formally required annually.
- Confirm any customer-specific wording that must appear in the final questionnaire.

Delivery note

This sample represents a manually prepared professional service. The work is performed by a cybersecurity professional using the information and material provided by the client; it is not an automated answer-generation service. Unsupported answers are not invented and points requiring client input are clearly flagged.