Before You Complete That Security Questionnaire

A practical checklist for validating requests and protecting your information

Security questionnaires are now a routine part of selling and supporting software.

They arrive via e-mail, portals and compliance platforms, and they are often treated as administrative work: download, complete, upload, submit.

In practice, they are not routine.

They involve sharing internal information about your systems, security controls, and operation, often through third-party platforms that store, structure and reuse that information. In some cases, requests are not clearly tied to a real client requirement at all.

This guide is designed to help you validate requests and control disclosure, so you respond to the right requests, in the right way, with appropriate protections in place.

Table of Contents

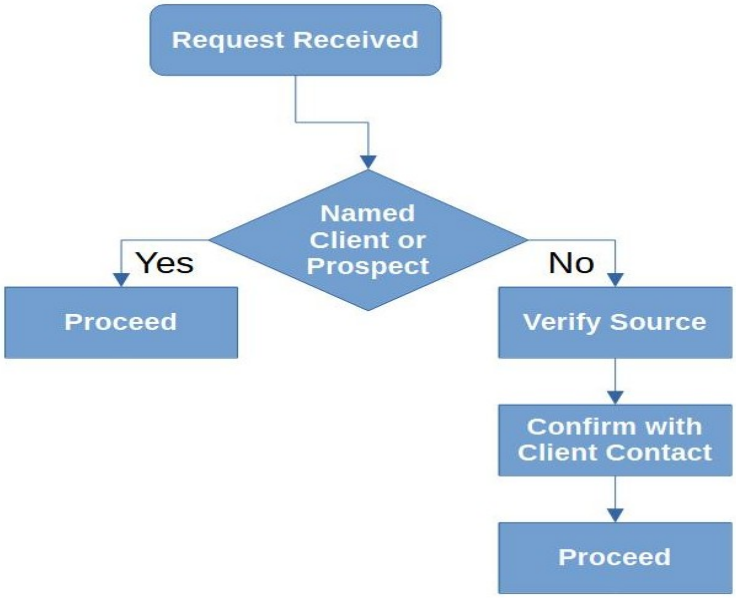
Cementarius Systems Ltd
w: cementariusconsulting.com
t: 01786 980215

1. Validate the Source of the Request

Before doing anything, establish who is actually asking for the information.

Requests increasingly arrive via platforms rather than directly from clients. This can obscure the origin. A request may appear legitimate but may not be clearly attributable to a specific client requirement.

If the source is unclear, there is a risk of responding unnecessarily or disclosing information inappropriately.



Checklist

- Is there a **named client or prospect** associated with the request?
- Is this tied to:
    - An active opportunity
    - Onboarding
    - Renewal or audit
- Did it come from a **recognised contact**?
- If via a platform:

- Does it clearly identify the client?

If unclear

- Confirm directly with your known client contact
- Verify that the request is genuine and expected

✔ **Rule:**
If you cannot clearly identify the requester, **verify before proceeding**

2. Classify the Request

Not all questionnaires are required, even if they appear formal.

Some are genuine client requirements linked to a commercial process. Others are platform-driven prompts designed to encourage vendors to provide or maintain data.

Treating all requests as mandatory leads to unnecessary work and unnecessary disclosure.

Checklist

Client driven

- Linked to a real engagement
- Has clear commercial relevance

Platform driven

- Generic “complete your profile” request
- No clear client context

Unclear

- Appears legitimate but not confirmed

Action

- Client-driven → proceed (subject to NDA)
- Platform-driven → deprioritise or ignore
- Unclear → verify

✔ **Rule:**

Do not assume every request is a client requirement

3. Confirm Confidentiality Before Sharing

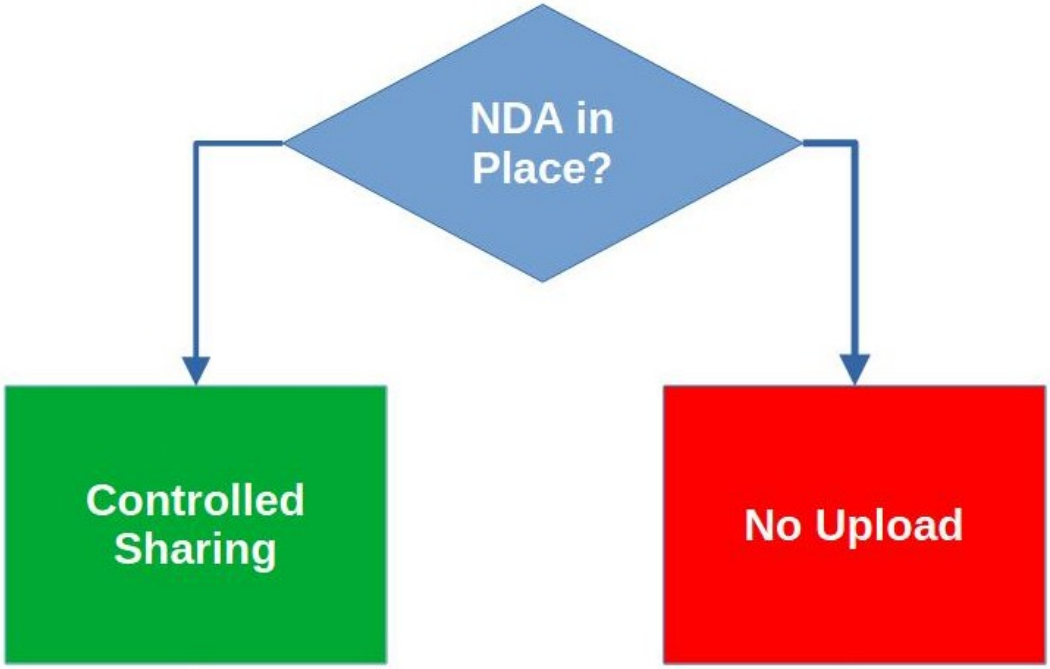
Before sharing any non-public information, confirm that confidentiality protections are in place.

For existing clients, this is typically covered by contract. For prospects, this usually requires a signed NDA.

A key point that is often overlooked:

> **If there is no NDA with the requesting party, there is no NDA covering the platform either**

The platform does not create confidentiality. It acts as a channel on behalf of the requester. If the underlying relationship is not protected, neither is the information you upload.



Checklist

- Is there a contract with confidentiality provisions?
- If not, is there a signed NDA?

- Does it allow sharing via third-party platforms?

If no NDA

- Do not share internal or non-public information
- Do not upload documents
- Do not complete detailed responses

✔ **Rule:**
No NDA → **no sharing of internal information**

4. Understand the Role of Questionnaire Platforms

Compliance platforms are often treated as simple delivery mechanisms. In practice, they behave differently.

Platforms such as OneTrust, RiskLedger, and Prevalent act as intermediaries between vendors and clients, but they also store and manage the information you provide.

Your responses are not just sent. They are retained, structured, and may be reused.

Checklist

- Will the platform:
    - Store responses long-term?
    - Allow reuse across requests?
    - Make data visible to multiple stakeholders?
    - Can you export completed questionnaires?

✔ **Principle:**
Treat platforms as **persistent repositories**, not temporary channels

5. Platform Incentives and Hidden Risks

Not all activity on compliance platforms is purely client-driven.

Many platforms have their own incentives, including building vendor profiles, generating security scores, and encouraging ongoing engagement.

These dynamics can influence how requests are presented and how urgently they appear.

Checklist

Be aware of:

- **Scoring and benchmarking**
  - Responses may contribute to a security score
  - Scores may influence vendor selection
- **Profile persistence**
  - Information may be reused across clients
  - You may be asked to keep your profile up to date
- **Data visibility**
  - Information may be accessible beyond the immediate requester
- **Commercial prompts**
  - Requests to upgrade, subscribe, or enhance visibility

✔ **Key point:** These are often **platform driven incentives**, not client requirements

6. Understand What You Are Being Asked to Share

Not all questionnaire responses carry the same level of risk.

Some information is already public or high-level. Other information can expose internal systems or vulnerabilities if shared too widely.

Understanding this distinction is essential when deciding whether to respond, what to share, and under what conditions.

> **The more detailed and internal the information, the stronger the requirement for confidentiality and control**

Information Sensitivity Levels

Low Sensitivity

- Public certifications
- High-level summaries
- Public-facing documentation

✔ Generally safe, but still validate the request

Medium Sensitivity

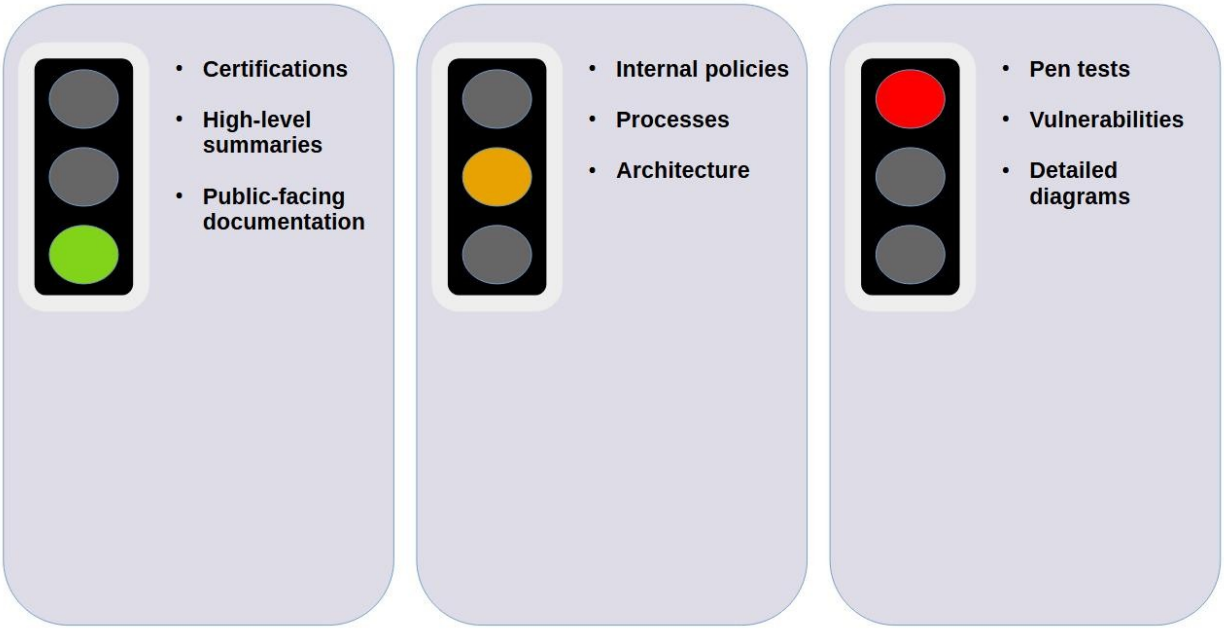
- Internal policies
- Process descriptions
- Detailed questionnaire responses
- High-level architecture

✔ Requires NDA and a validated request

High Sensitivity

- Penetration test reports
- Vulnerability scan results
- Detailed architecture diagrams
- Internal network details

✔ Strictly controlled and only shared where clearly required



Checklist

- What level of information is being requested?
- Is this appropriate for the stage of engagement?
- Is the platform an appropriate place to store it?

✔ **Rule:**
If in doubt, treat the information as **more sensitive, not less.**

7. Uploading is Disclosure

A common assumption is that information is only shared when a questionnaire is submitted.

In practice, uploading information to a platform is already a form of disclosure.

Once uploaded, data may be stored, processed, or accessible, even if not formally submitted.

Checklist

- Does the platform retain uploaded data?
- Can drafts be stored or accessed?

✔ Rule:
Upload = disclose

8. Do Not Upload Without Confidentiality in Place

Pressure to move quickly often leads to premature sharing.

Uploading “just to get started” or “to save time” can result in uncontrolled disclosure.

If confidentiality is not in place, the correct action is to wait.

Checklist

Before uploading:

- NDA or contract in place ✔
- Request validated ✔
- Client confirmed ✔

If not:

- Do not upload
- Do not partially complete
- Do not save drafts

✔ **Rule:**
No NDA → **no upload**

9. Validate Platform Requests Carefully

Some requests are not clearly attributable to a real client requirement.

These are often profile driven or platform generated requests.

Checklist

- Is there a named client behind the request?
- Can it be confirmed directly?
- Is it tied to a real engagement?
- Would the client expect a response?

Red flags

- Generic platform emails
- No identifiable client
- Requests to “complete your profile”
- No clear commercial context

✔ **Rule:**
If in doubt, **pause and verify**

10. Final Decision Check

Before proceeding, apply a final sense check.

Checklist

- Do we know who requested this?
- Is it a real client requirement?
- Has it been verified if needed?
- Is confidentiality in place?
- Are we comfortable sharing via this channel?

If any answer is unclear:

✔ **Stop and resolve before continuing**

Summary Principles

- Not every questionnaire is required
- Not every platform request is client driven
- Confidentiality must be in place before sharing
- Uploading information is a form of disclosure
- When in doubt, verify first