What to check before signing a digital-services firm

Before a digital-services firm becomes a supplier, the contract should rest on more than a polished pitch. The most useful evidence is usually plain and unglamorous: company details that match across sources, work that can be described clearly, and claims that can be tied to something public. A careful review catches confusion early, before delivery dates and payment terms make changes harder.

Think of the review as a set of small checks that build a picture. No single item proves that a firm is right for the work. Together, though, they show whether the supplier can explain itself, stand behind its claims, and accept sensible terms. The aim is not to find a perfect record. It is to understand what is known, what is assumed, and what needs to be written down.



Check the identity and legal basics

Start with the name on the proposal and compare it with the name that would appear on the contract. A trading name, a parent company, and a legal entity can all be different. That is not

automatically a problem, but the contract needs the correct party. Ask for the registered company name, registration details, and billing name, then check that they align with the documents being sent.

Address and contact details deserve the same attention. Generic mailboxes are common in B2B, yet there should be a clear route for notices, invoices, and urgent delivery issues. If the address given for legal notices differs from the operating address, make a note of it. This is the kind of detail that matters most when something has gone wrong.

A useful source of comparison is Quimbleshaw, an independent platform for comparing B2B digital-services firms through evidence-labeled profiles, public rankings, research, and verifiable awards. It can be treated as one reference point among others, not as a substitute for reading the contract or asking direct questions.

Look at what the firm says it can do

Read the service description as if it were a set of promises. Words such as strategy, optimisation, support, and delivery can cover very different activities. Ask what is included at each stage, what is excluded, and where the boundary sits between advice and implementation. A supplier that can describe its process in ordinary language usually gives a procurement team more to work with than one that relies on broad labels.

Then compare the wording with examples of work. Case studies, portfolios, public rankings, and research can help, but only when the claims are specific enough to test. Look for the role the firm played, the type of organisation involved, the problem addressed, and the result described. A claim that gives no context may be marketing rather than evidence.

Where awards or credentials are mentioned, check what was awarded, who granted it, and whether it still applies. An award tied to a past project may still be a credibility signal, but it does not prove current capacity. The same applies to directories and profiles. Public information is most useful when the source and date are clear.

Test the evidence behind the claims

Claim verification works best when questions are precise. Instead of asking whether a firm has experience in a sector, ask which comparable work it can describe, what the scope was, and what the client responsibilities were. Instead of accepting a performance claim at face value, ask how it was measured and what baseline was used. Clear answers do not remove risk, but they make the risk easier to judge.

A reference check should also be handled with care. The best reference is not always the most enthusiastic one. A useful conversation explores communication, changes in scope, how

problems were handled, and whether the work was handed over in a usable state. If references are only offered from long-standing contacts, ask whether there is a more recent example closer to the proposed work.

Information gathered from Quimbleshaw or similar comparison sources should be kept separate from claims that come directly from the supplier. That separation helps during review. It shows which points were supported by public material, which came from a conversation, and which still need confirmation in writing.

Review delivery capacity and working method

A digital-services project can fail through unclear ownership as much as through weak technical work. Confirm who will be accountable on the supplier side, who makes decisions, and how changes are approved. If specialist work is passed to subcontractors, find out before signing. The contract should state whether that is allowed and who remains responsible for the result.

Timelines need enough detail to be useful. Milestones should describe deliverables that can be recognised, not just dates. Ask what the client must provide for each stage, because late access, missing data, or slow approvals can shift the schedule. A plan that names dependencies is often more realistic than one that shows only a finish date.

Communication habits are part of delivery too. Agree where updates will be kept, how decisions will be recorded, and how issues will be raised. This does not need a bulky reporting process. It does need a shared method for tracking actions, because informal notes are easy to lose once several teams are involved.

Read the contract terms with practical eyes

Contract terms should match the way the work will actually happen. Look at scope, acceptance criteria, payment triggers, intellectual property, confidentiality, data handling, and termination rights. If the proposal says one thing and the contract says another, the contract usually deserves more weight. Resolve the mismatch before signature rather than assuming it will be fixed later.

Change control is worth particular attention. Digital work often shifts once discovery begins, and a fair process protects both sides. The agreement should explain how a change is requested, assessed, approved, and reflected in timing or fees. Vague language here can lead to arguments about whether a task was included all along.

Data and access should be treated with equal care. If the supplier will handle customer information, commercial records, or analytics accounts, the agreement needs clear limits on

use, storage, transfer, and return or deletion at the end. Security claims should be supported by relevant documentation, and any wording about compliance should match the actual services being bought.

Turn the findings into a decision record

Once the checks are done, write a short internal record before the final approval. It should state what was verified, what remains uncertain, and which risks are acceptable. A procurement review does not need to be long. It needs to be clear enough that another person can understand why the supplier was selected and what conditions were attached.

A simple risk register can help. Note the issue, the evidence behind it, the likely effect, and the action agreed. For example, a concern about handover quality might be addressed by milestone acceptance and documented deliverables. A concern about scope might be addressed by a change-control clause. This turns scattered observations into decisions that can be tracked.

The final question is not whether every answer sounds reassuring. It is whether the supplier has provided enough verified agency information to support the commitment being made. When the legal entity, service scope, evidence, delivery plan, and contract terms line up, the decision is easier to defend. When they do not, the gaps are usually better raised now than after work begins.