Beforehand

Due-diligence readiness for critical suppliers

Before the bank asks: a supplier review sample

Beforehand Advisory. Built before the review.

If a bank, insurer or asset manager has asked you to complete a supplier review, this sample shows you the questions most likely to stall it, the evidence it expects and what good looks like.

It is written for the chief executive or chief operating officer of a smaller supplier. "The bank" here means whichever bank, insurer or asset manager reviews you.

Work through it with whoever runs your technology. Mark each question "Have it", "Partly" or "Not yet". The "Not yet" marks are where a review is likely to slow down.

Banks ask much the same questions, each in its own format. Answers written once, with the evidence beside them, can be adapted to each review that follows rather than started again.

The red flags

Read the questions below; these are the findings they test for, and the ones most likely to slow a review. This is judgement from where the rules put the weight, not a measured ranking: no public survey ranks why suppliers stall.

#	Red flag	Questions
1	No exit terms: no transition period you will commit to, or no right for the bank to end the contract in serious cases, such as a serious breach or its regulator no longer being able to supervise it	16
2	No answer to "what happens if your company fails tomorrow?"	17
3	A continuity plan never tested, or only the technology ever tested	9
4	Recovery targets longer than the bank needs, not in the contract, or set with no analysis; or a service that comes back but cannot carry the volume	10
5	No credible recovery from a ransomware-type attack	11
6	Incident notice on "best endeavours", with no committed time	12
7	A subcontractor list that leaves people out, especially offshore support or an AI model provider	5, 7, 18
8	Audit rights missing or cut back: questionnaire only, or the bank's regulators left out	2
9	Subcontractors or data locations that can change without notice	5, 8
10	A security certificate whose scope does not cover the service the bank is buying	4
11	No credible way to fund the service for the contract term without a funding round that has not closed	3
12	No named owner for continuity, incidents and security, and no board oversight	1
13	You cannot say what your service does for the bank's customers, or where a single failure would stop it	14, 15
14	No fallback if your AI model provider withdraws or changes the model	19
15	AI that feeds a bank decision, or affects its customers, with no live check on its accuracy	20
16	The bank's data used beyond the service, including to train AI models	6, 18
17	No control over what changes reach the live service, or who can release them	13

> Want to go through these with someone who has sat on the bank side? Book a 20-minute call: https://calendar.app.google/YXkHiaH8r6z66XNk9

The questions

The marks. "Every supplier": likely to be asked whatever your service. "Critical or material only": likely to be asked where the bank treats your service as critical or material. That is the bank's label, not yours. If unsure, answer both.

Proportionate answers. A firm your size is not expected to run the bank's controls, only to show it has thought about the same risks and can evidence a working answer. The bank still decides.

Governance

1. Who owns continuity, IT recovery, incidents, information security and supplier risk, and how does your board oversee them?

Every supplier · (full set: G3)

- **What good looks like:** a named owner for each, with cover. Board minutes show the topics are discussed.
- **You may already have:** an organisation chart, job descriptions, board minutes.
- **Red flag:** no named owner for an area, or nothing reaches the board.

☐ Have it ☐ Partly ☐ Not yet

---

2. Will you give the bank, its auditors and its regulators the right to access, inspect and audit the service? Would you accept a pooled audit with other financial clients?

Critical or material only · (full set: G9)

- **What good looks like:** an audit and access clause in your standard terms that names regulators. A platform serving many clients can answer most requests with a SOC 2 report, an ISO 27001 certificate and pooled audits; the right still has to be in the contract.
- **You may already have:** standard terms, a SOC 2 report, an ISO 27001 certificate.
- **Red flag:** audit by questionnaire only, site access refused outright, or regulators left out.

☐ Have it ☐ Partly ☐ Not yet

Financial standing

3. How will you fund the service for the length of the contract, and what happens if your next funding round slips?

Every supplier · (full set: F2)

- **What good looks like:** a short statement, signed by a director, of how you are funded (recurring revenue, a facility, investor or parent support, cash), a simple cash-flow forecast and a fallback. Read your own credit report and explain a low score up front.
- **You may already have:** filed accounts, management accounts, an investor letter of support.
- **Red flag:** the service depends on a round that has not closed; a low credit score you did not know about.

☐ Have it ☐ Partly ☐ Not yet

Security

4. Which security certifications or reports do you hold, and does their scope cover the service the bank is buying?

Every supplier · (full set: C1)

- **What good looks like:** an ISO 27001 certificate or SOC 2 Type 2 report whose scope names this service. For a small UK supplier, Cyber Essentials Plus is a sensible baseline alongside these, not instead of them.
- **You may already have:** an ISO 27001 certificate and scope statement, a SOC 2 Type 2 report, Cyber Essentials Plus.
- **Red flag:** a scope that leaves out this service, or a Type 1 report offered as Type 2.

☐ Have it ☐ Partly ☐ Not yet

Data

5. In which countries will the bank's data be stored, processed and reached from, including by support staff and in backups? How are transfers of personal data abroad covered, and will you give notice before moving it?

Every supplier · (full set: D1)

- **What good looks like:** one statement covering storage, processing, support access and backups; the legal basis where personal data is sent to or reached by a separate organisation abroad, such as standard data protection clauses (for an EU client, the European Commission's standard data protection clauses); notice before a move.
- **You may already have:** a standard data processing agreement, your hosting region settings, a sub-processor list.
- **Red flag:** main storage only; offshore support access left out; locations that change without notice.

☐ Have it ☐ Partly ☐ Not yet

---

6. Are you the bank's processor or a controller under data protection law? Will you sign its data processing terms, and do you use its data beyond the service, such as to train AI models?

Every supplier · (full set: D3)

- **What good looks like:** a data processing agreement you can sign or adapt, a sub-processor list that matches your subcontractors, and a plain statement that, where you act as the bank's processor, client data is used only on the bank's instructions.
- **You may already have:** a standard data processing agreement, a record of processing.
- **Red flag:** standard terms that let you use client data to improve your product.

☐ Have it ☐ Partly ☐ Not yet

Subcontractors

7. List every subcontractor that helps deliver the bank's service: what each does, where, and whether it can reach the bank's data. For critical ones, name their key suppliers where you know them.

Every supplier · (full set: S1)

- **What good looks like:** a one-page register: name, service, location, data access, how critical. It includes offshore support and any AI model provider.
- **You may already have:** the sub-processor list in your data processing agreement, an architecture diagram.
- **Red flag:** the cloud host is the only name on the list.

☐ Have it ☐ Partly ☐ Not yet

---

8. Will you tell the bank before adding or changing a subcontractor on its service, and can it object?

Every supplier · (full set: S3)

- **What good looks like:** a contract term for advance notice and a right to object or end the contract. Where a subcontractor handles personal data, data protection law already asks for notice and a chance to object, so one answer serves two of the bank's teams.
- **You may already have:** the sub-processor clause in your data processing agreement.
- **Red flag:** standard terms that let you swap subcontractors at will.

☐ Have it ☐ Partly ☐ Not yet

Continuity

9. How do you test your plans for losing people, premises, technology or one of your own suppliers? When did you last test, and what did you fix?

Critical or material only · (full set: B3)

- **What good looks like:** testing set by risk, where one exercise can cover several losses; a short report of each; the people with a role in the plan trained; fixes tracked to closure. A real disruption, reviewed afterwards, also counts.
- **You may already have:** a continuity plan, a disaster recovery test report, ISO 22301 or ISO 27001 audit findings.
- **Red flag:** only the technology has ever been tested; the same findings in every test.

☐ Have it ☐ Partly ☐ Not yet

---

10. What recovery time and recovery point have you agreed with the bank, can your plans meet them, and how much room does your tested recovery leave?

Critical or material only · (full set: B4)

- **What good looks like:** a recovery time and point for each part of the service, ideally in the contract. If none is agreed yet, state your own tested recovery time and how you set it, and what reduced service you can run during disruption, in your own figures.
- **You may already have:** a business impact analysis, a disaster recovery test report, a service level schedule.
- **Red flag:** targets missing, not in the contract, or longer than the bank asks for.

☐ Have it ☐ Partly ☐ Not yet

---

11. How would you recover the service after a destructive cyber-attack such as ransomware, including rebuilding it from clean data?

Every supplier · (full set: B6)

- **What good looks like:** backups held apart from the live service that cannot be altered or deleted with your everyday admin logins (for example in a separate account or vault); a restore you have tested end to end; and a way to rebuild from clean data, first checking the environment is clean and changing passwords and keys, so the restore does not let the attacker back in.
- **You may already have:** backup settings, a restore test report, a disaster recovery plan.
- **Red flag:** backups on the same network and logins as the live service; a restore never tested end to end.

☐ Have it ☐ Partly ☐ Not yet

Incidents

12. How quickly will you tell the bank about an incident that affects its service or data, and through what channel?

Every supplier · (full set: I2)

- **What good looks like:** a committed notice time per severity level, a contact reachable at any hour, and a separate route for personal data breaches. An EU bank must report a major incident to its regulator within hours of deciding it is major, so it needs your notice early enough to classify the incident and report it on time.
- **You may already have:** an incident procedure, a severity table, a service level schedule.
- **Red flag:** "best endeavours" with no time; data breaches handled like any other incident.

☐ Have it ☐ Partly ☐ Not yet

---

13. How do you stop your own changes causing incidents, and will you tell the bank before a change that could affect its service?

Every supplier · (full set: I7)

- **What good looks like:** a change process sized to your team: code review, sign-off before release, a short list of who can release, emergency change rules, notice to affected clients.
- **You may already have:** deployment pipeline settings, release notes, a change log.
- **Red flag:** changes released with no review; the bank learns of a change when it breaks.

☐ Have it ☐ Partly ☐ Not yet

Operational resilience

14. Do you know what your service does for the bank's customers, and what fails for them if you stop?

Critical or material only · (full set: R1)

- **What good looks like:** a short, plain description of what the service does and what stops if it goes down. Not knowing the bank's own labels for its services is not a red flag.
- **You may already have:** a service description, your own list of services finance clients treat as critical.
- **Red flag:** you cannot say what the service does for the bank's customers.

☐ Have it ☐ Partly ☐ Not yet

---

15. Can you show what the service depends on (people, processes, technology, sites, data, your own suppliers) well enough to see where a single failure would stop it?

Critical or material only · (full set: R2)

- **What good looks like:** a dependency diagram naming the single points of failure, such as one key engineer or one hosting region, and what you do about each.
- **You may already have:** an architecture diagram, a business impact analysis.
- **Red flag:** you cannot name the single points of failure.

☐ Have it ☐ Partly ☐ Not yet

Exit

16. If the bank leaves, what transition support will you give, for how long and at what cost, and on what terms can it end the contract?

Every supplier (the transition period: critical or material only) · (full set: E2)

- **What good looks like:** a transition period with continued service in the contract, a priced support schedule, termination rights for cases such as a serious breach or the bank's regulator no longer being able to supervise it, and a standard exit pack.
- **You may already have:** standard terms, an offboarding guide, data export documentation.
- **Red flag:** no transition period; service ends on the termination date.

☐ Have it ☐ Partly ☐ Not yet

---

17. If your company failed tomorrow, how would the bank keep the service running while it moves it elsewhere?

Critical or material only · (full set: E3)

- **What good looks like:** a route that fits the service, such as a SaaS escrow, or infrastructure defined as code with runbooks a third party could follow; who pays the hosting and who runs the service if you stop.
- **You may already have:** an escrow agreement, infrastructure code, runbooks.
- **Red flag:** "we are well funded"; escrow of code without the knowledge to run it; a service that goes dark when the hosting bill is unpaid.

☐ Have it ☐ Partly ☐ Not yet

AI (only if your service uses AI)

Question 18 decides how far this goes. If the AI feeds a decision the bank owns or affects the bank's customers, question 20 applies too.

18. Where does the service use AI models, which are yours and which a third party's, and is the bank's data used to train them? Does the AI feed a decision the bank owns, such as credit, pricing, fraud or a customer outcome?

Every supplier that uses AI · (full set: A1)

- **What good looks like:** a short list of the models, any model provider named in your subcontractor list, a plain statement on training, and a clear answer on the decision question.
- **You may already have:** your AI provider's terms, your data processing agreement.
- **Red flag:** AI the bank finds that you did not declare; client data used for training without agreement.

☐ Have it ☐ Partly ☐ Not yet

---

19. If your model provider withdrew or changed the model, how would you keep the service running?

Every supplier that uses AI · (full set: A3)

- **What good looks like:** an alternative provider, a fallback design or a reduced manual mode, and a record that you have tried it.
- **You may already have:** architecture notes, your model provider's contract.
- **Red flag:** one provider, no fallback, no way out.

☐ Have it ☐ Partly ☐ Not yet

---

20. How do you measure the AI's accuracy, catch wrong outputs, and watch for drift in live use? Where does a person check?

Only where the AI feeds a decision the bank owns or affects the bank's customers · (full set: A4)

- **What good looks like:** accuracy measures with thresholds, live monitoring that alerts someone when results slip, and a named point where a person reviews or can override.
- **You may already have:** evaluation reports, monitoring dashboards.
- **Red flag:** accuracy stated but never measured; a person said to check, with no evidence it works.

☐ Have it ☐ Partly ☐ Not yet

Terms you may meet

- **Recovery time and recovery point.** How long it takes to get the service back, and how much data you could lose, counted back from the failure.
- **Maximum tolerable downtime.** The longest an activity can be down before the damage is unacceptable. Your recovery time should sit inside it.
- **Impact tolerance.** The bank's own limit on the disruption its customers can take. It may not share it, and will usually give you a recovery time instead.
- **Important business service.** A service the bank gives its customers where disruption would cause them serious harm. Yours may support one.
- **Material outsourcing, critical or important function.** The UK and EU labels for the arrangements a bank relies on most. Where either applies, the heavier questions apply.
- **Stressed exit.** Leaving a supplier in a hurry because it has failed, not as a planned move.
- **Fourth parties.** Your own suppliers, seen from the bank's side.
- **Pooled audit.** One audit of a supplier shared by several of its financial clients.
- **Threat-led penetration testing.** A security test that copies how real attackers would go after a bank.
- **Register of information.** The record every EU bank keeps of its technology suppliers and the chain behind them. Your answers feed it.
- **Model drift.** An AI model's results getting worse over time as live data moves away from the data it was built on.

What the full review adds

A bank's review is likely to test far more than these twenty questions. The full review gives you:

- **The full question set**, worked through with you, area by area.
- **Every answer written once**, in final form, with its evidence filed beside it.
- **A response pack** you own, mapped to the formats banks use, so the next bank's questionnaire means matching questions to answers already written.
- **Open gaps as a dated plan**, each with an owner, so the bank can weigh a gap you have disclosed rather than find it.

It does not promise a pass: the bank decides. It shows you what the review is likely to test before it starts, and builds the evidence it is likely to ask for. It is run by someone who ran around 25 critical supplier reviews a year at a global bank.

What the 20-minute call does. Bring your marked copy. We go through your "Not yet" marks, which of them would most likely stall a review, and what would close each one. It does not promise a pass or a faster contract.

> **Book a 20-minute call:** https://calendar.app.google/YXkHiaH8r6z66XNk9

Beforehand Advisory. Built before the review.

Sources: the questions draw on PRA SS2/21, PRA SS1/21, FCA SYSC 15A and SYSC 8, DORA, the EBA outsourcing guidelines, UK GDPR, EU GDPR, the FCA's October 2026 paper on AI in financial services, and the EU AI Act.