GOVERNANCE DOCS

Third-Party Risk Assessment

Meridian Payments (sample)

Cobalt Ledger Systems (fictional): the cloud platform that runs customer e-wallets and daily settlement for about 240,000 customers.

ASSESSED	25 September 2026
METHOD	ISO/IEC 27001:2022 controls A.5.19 to A.5.23 with ISO/IEC 27036, NIST CSF 2.0 GV.SC and DORA Articles 28 to 30
IN SCOPE	8 scope items, 13 risks
APPETITE	Medium and below (level 9 or less) accepted without treatment
PREPARED BY	Governance Docs

Confidential. Prepared for Meridian Payments (sample). Contains details of a vendor, the service it provides, weaknesses found in due diligence and planned controls; share on a need-to-know basis.
Based on a self-assessment using information supplied by the organization. Not independently verified by Governance Docs; see "Basis of this report and limitation of liability".

CONTENTS

Where the organization's risks stand

PROCESS SCORE

92 / 100

Level 4 · Managed

Owned, justified and accepted: ready for management review and audit.

Initial | Developing | Defined | **Managed**

The score measures how complete and defensible the assessment is, not how risky the organization is.

RISKS	ABOVE APPETITE	CRITICAL	ABOVE AFTER TREATMENT	FINDINGS
13	5	0	0	4

WHAT THIS ASSESSMENT TELLS YOU

- Critical vendor: full due diligence: The service supports a critical or important function. Carry out full due diligence against evidence, put the contract terms regulators expect in place (audit rights, incident reporting, subcontracting, exit), and check whether the regulator must approve or be notified.
- No High or Critical risk remains once the planned controls are in place, so the vendor can be approved on those terms.
- 5 of 12 rated risks sit above your appetite line (Medium and below is acceptable).
- The highest risk is R-01, the vendor's service is unavailable for a long period, at level 15 (High), owned by Chief Operating Officer.
- Planned treatment brings the number of risks above the line from 5 to 0.

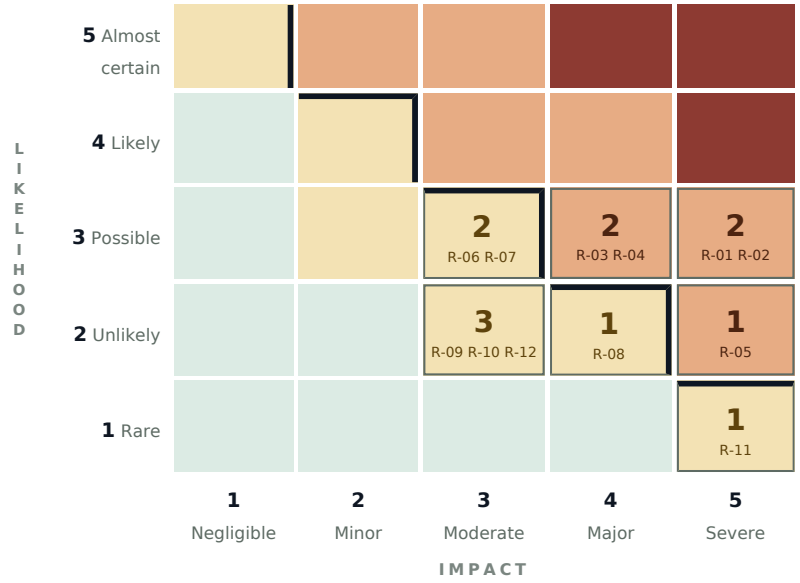
DO THESE FIRST

	SEVERITY	ACTION	RISKS	OWNER	DOCUMENT THAT CLOSES IT
1	MAJOR	**Not yet rated for likelihood and impact** Rate each one against the likelihood and impact scales in your criteria.	R-13	Chief Financial Officer	Risk assessment and treatment methodology
2	MAJOR	**Risk with no owner** Name an owner, by role, for each risk.	R-12	To assign	Risk assessment and treatment methodology
3	MAJOR	**Scope item with no risks identified** Link an existing risk to it, add a new one, or take it out of scope.	Platform API integration	To assign	Third-Party Inventory Register

Heat maps: today and after treatment

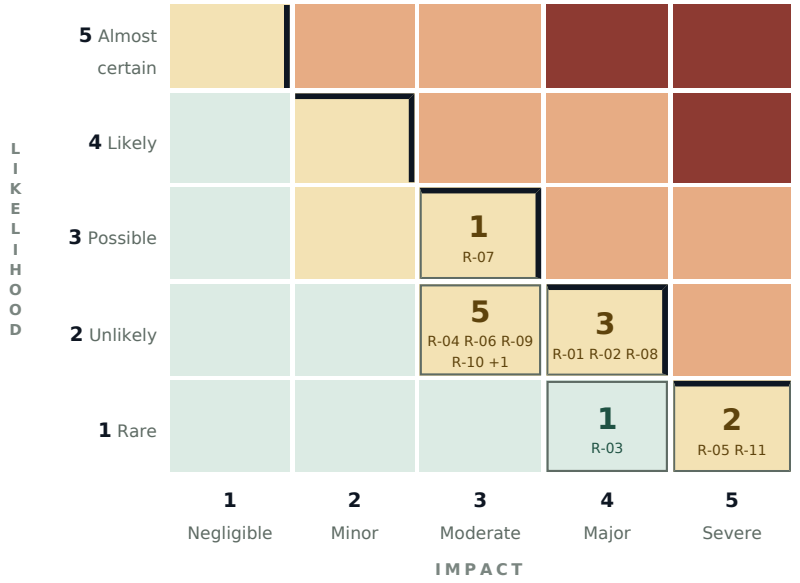
Each cell shows how many risks sit at that likelihood and impact, with their references. The heavy line is the appetite line: Medium and below (level 9 or less) is accepted without treatment. The second map shows where each risk is expected to be once its treatment is carried out; avoided risks are removed.

Current risk levels



12 of 13 risks rated.

Target levels after treatment



12 risks plotted; 0 removed by avoidance; risks above the line with no decision are not plotted.

Low 1–4 · Medium 5–9 · High 10–16 · Critical 17–25 · Appetite line

RISKS BY LEVEL

Analysis and priorities

IN ONE SENTENCE

Cobalt is a critical vendor that can be approved on conditions: the planned controls bring all five High risks within appetite, but the exit plan and the recovery time need closing first.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our assessment of Cobalt Ledger Systems supports approving it for customer wallets and settlement, on conditions. The contract must give us four-hour incident notice, a four-hour recovery time and control over its subcontractors, and we must have a tested exit plan within six months.

WHERE YOU STAND	The tiering found that Cobalt runs a critical function, customer wallets and settlement, so it is a Critical vendor needing full due diligence. You have recorded 13 risks across 8 scope items, and 12 are rated. Your process score is 92 out of 100, at the Managed level.
WHAT IT MEANS FOR THE ORGANIZATION	5 risks sit above your appetite line, all of them High. The highest are a long outage, where Cobalt's 8-hour recovery time exceeds your 4-hour tolerance, and lock-in, with no written exit plan and a 9 to 12 month migration. Planned controls bring all five within appetite, so the vendor can be approved on those terms.
WHERE TO FOCUS FIRST	Close the contract conditions first: four-hour incident notice, the named support subcontractor and the recovery time. Then write and test the exit plan, rate the cost risk, name an owner for the change of control risk, and link the API integration to at least one risk.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Write and test the exit plan** R-02 You cannot leave the vendor without serious disruption	A move would take 9 to 12 months and data exports only in the vendor's own format, so a failure would leave no orderly way out.	Agree a standard export format and name the alternative provider in the plan.	Exit Plan Template for Critical Arrangements	90 DAYS
2	**Contract a recovery time you can live with** R-01 The vendor's service is unavailable for a long period	Cobalt's 8-hour recovery time is twice your 4-hour tolerance for customer payments.	Add a 4-hour recovery time with service credits to the contract schedule.	Service Level and KPI Schedule Template	60 DAYS
3	**Close the contract conditions before signing** R-04 The vendor is slow to tell you about an incident · R-06 A subcontractor the vendor relies on fails	Without four-hour incident notice and a named support subcontractor, you could miss your own reporting deadlines and rely on a party you never assessed.	Send the amended incident notification and subcontracting clauses to Cobalt.	Incident and Breach Notification Clause Guide	30 DAYS
4	**Replace the shared support account** R-03 Attackers get in through the vendor's access to your systems	Actions under one shared administrator account cannot be traced to a person.	Set up named, time-bound accounts approved per support ticket, with session recording.	Third-Party Access Review Procedure	60 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Sign the contract with four-hour incident notice and the named subcontractor.
- Rate the cost risk and name an owner for the change of control risk.
- Link the API integration to its risks.

DAYS 31 TO 60

- Agree the 4-hour recovery time and join the next recovery test.
- Replace the shared support account with named accounts.
- Review the full penetration test report.

DAYS 61 TO 90

- Write the exit plan with a standard export format.
- Plan the exit test with Cobalt.
- Add Cobalt to the reassessment schedule for September 2027.

How critical is this vendor? The tiering

Critical vendor: full due diligence

The service supports a critical or important function. Carry out full due diligence against evidence, put the contract terms regulators expect in place (audit rights, incident reporting, subcontracting, exit), and check whether the regulator must approve or be notified.

Screening note: Sanctions, adverse media and ownership checks were clear. The platform runs customer wallets and settlement, a critical function and material outsourcing, so Cobalt is a Critical vendor regardless of the other factors. It holds customer data, connects to our core systems, relies on a cloud host and an offshore support centre, keeps its disaster recovery site in Europe, and is on a five-year contract.

Red flags	Met
Screening found a red flag: sanctions, bribery, fraud or a serious unresolved legal issue	No

Risk factors that set the tier	Met
The service supports a critical or important function, or is material outsourcing	**Yes**
The vendor will hold, see or process personal or confidential data	**Yes**
The vendor will connect to your network or systems, or hold privileged access	**Yes**
The service would be hard to replace quickly	**Yes**
The vendor relies on subcontractors for key parts of the service	**Yes**
Data is held or accessed outside your country or region	**Yes**
The contract is significant in value or length	**Yes**

The vendor profile

The service, the function it supports, the data and access involved, where it runs and who else is involved, the assurance reviewed, the contract and the way out. The data, systems, locations and subcontractors are listed with the register.

The vendor and the service	Cobalt Ledger Systems provides a multi-tenant cloud platform for e-wallets, card top-ups and end-of-day settlement, with 24/7 support.
The business function it supports	All customer wallet balances, transfers and settlement with partner banks run on the platform. If it stops, customers cannot pay or withdraw and settlement fails.
Data shared and access granted	Customer identity and contact details, wallet balances and full transaction history. Cobalt support staff have remote administrative access for incident response.
Locations and subcontractors	Primary hosting in a regional cloud data centre; disaster recovery site in Europe; second-line support from an offshore support centre run by a subcontractor.
Assurance and evidence reviewed	ISO/IEC 27001 certificate covering the platform and support; SOC 2 Type II report for the last 12 months with two exceptions, both closed; summary of an annual penetration test; completed security questionnaire.
Contract, term and spend	Five-year master services agreement under negotiation; annual fee about 1.2 million; renewal and price review at year three.
Alternatives and exit route	Two other platforms could take the service; a migration would take 9 to 12 months. No in-house fallback.
Relationship owner and vendor contacts	Relationship owner: Chief Operating Officer. Cobalt security contact and 24/7 escalation line recorded in the vendor register.

Due diligence

The checks ISO/IEC 27001 A.5.19 to A.5.23, NIST CSF 2.0 GV.SC and DORA Articles 28 to 30 point at, one question each. Every "partly" or "no" says what is missing.

Question	Answer	Explanation or evidence
Independent assurance is current and covers this service (ISO 27001 certificate, SOC 2 Type II report or equivalent)	Yes	ISO 27001 certificate scope checked; SOC 2 Type II exceptions reviewed.
The security questionnaire has been completed and the answers checked against evidence	Partly	Questionnaire checked against the SOC 2 report; only a summary of the penetration test was shared.
Vendor access is least-privilege, uses MFA and is logged	Partly	Support uses a shared administrator account with MFA; named accounts and session recording agreed.
Data is encrypted in transit and at rest	Yes	Encrypted in transit and at rest; keys managed by the cloud host.
The vendor must report incidents to you within an agreed time and support the response	Partly	Standard terms say "without undue delay"; we require notice within four hours.
The vendor's continuity and recovery plans are tested and meet your recovery needs	Partly	Disaster recovery tested yearly with an 8-hour recovery time; our tolerance is 4 hours.
The vendor's financial health has been checked	Yes	Three years of audited accounts reviewed; profitable, no significant debt.
Subcontractors are disclosed, approved and bound by the same terms	Partly	The cloud host is named; the offshore support subcontractor is not in the contract.
Data locations are agreed, and transfers have safeguards	Yes	Hosting and recovery locations written into the contract, with transfer safeguards.
A data processing agreement is in place, or no personal data is shared	Yes	Data processing agreement signed with the master agreement.
You have the right to audit the vendor, or to receive its audit reports	Partly	Annual SOC 2 reports and pooled audits; no individual on-site audit.
There is an exit plan covering transition and the return or deletion of data	Partly	Exit clause with 12 months of transition support; no exit plan written or tested yet.
The regulator has approved or been notified of the outsourcing, where that is required	Yes	Prior approval for the outsourcing requested and received.

The risks the vendor brings follow in the register, rated for the organization and its customers, with the controls that manage them and their ISO 27001, NIST or DORA references.

What was in scope

The service or business function, data shared, system or connection, vendor or subcontractor, location or data centre and people affected the assessment covered, with their owners.

Type	Scope item	Owner	Risks
Service or business function	**Customer wallets and settlement**	Chief Operating Officer	2
Data shared	**Customer identity and transaction data**	Data Protection Officer	2
System or connection	**Platform API integration**	IT Director	**0**
System or connection	**Vendor support remote access**	Chief Information Security Officer	1
Vendor or subcontractor	**Cobalt Ledger Systems**	Head of Procurement	7
Vendor or subcontractor	**Cloud hosting provider (fourth party)**	Head of Procurement	2
Vendor or subcontractor	**Offshore support centre (fourth party)**	Head of Procurement	3
Location or data centre	**Disaster recovery site in Europe**	IT Director	1

Risk register

Every risk, highest level first. Level = likelihood x impact, rated with the controls already in place. The rationale is the organization's own reason for the rating. The full scenario for each risk (threat, weakness and consequence) is in the workbook.

#	Ref	Risk scenario	Scope items	Impact type	Owner	Existing controls	L	I	Level	Rationale
1	R-01	**The vendor's service is unavailable for a long period** Weakness: No tested recovery objectives that match your own	Customer wallets and settlement, Cobalt Ledger Systems	Availability, Financial, Reputation	Chief Operating Officer	Yearly disaster recovery test	3	5	15 · High	Recovery time of 8 hours against our 4-hour tolerance; two outages over 2 hours at other clients last year.
2	R-02	**You cannot leave the vendor without serious disruption** Weakness: No exit plan, data export format or transition support	Cobalt Ledger Systems, Customer wallets and settlement	Availability, Financial	Chief Operating Officer	Exit clause with 12 months' transition support	3	5	15 · High	A move would take 9 to 12 months, and data export is only in Cobalt's own format.
3	R-03	**Attackers get in through the vendor's access to your systems** Weakness: Standing, shared or over-privileged access without MFA	Vendor support remote access, Offshore support centre (fourth party)	Confidentiality, Integrity, Availability	Chief Information Security Officer	MFA on the support account	3	4	12 · High	Support staff share one administrator account, so actions cannot be traced to a person.
4	R-04	**The vendor is slow to tell you about an incident** Weakness: No notification deadline or incident support obligation	Cobalt Ledger Systems	Confidentiality, Availability, Regulatory and legal	Head of Compliance		3	4	12 · High	Standard terms allow notice "without undue delay"; our own reporting deadlines are hours, not days.
5	R-05	**A breach at the vendor exposes your data** Weakness: Vendor security never checked against evidence	Customer identity and transaction data, Cobalt Ledger Systems	Confidentiality, Regulatory and legal, Financial, Reputation	Chief Information Security Officer	ISO 27001 certificate; SOC 2 Type II report	2	5	10 · High	Strong assurance, but a breach would expose all customer transaction history.

6	R-06	**A subcontractor the vendor relies on fails** Weakness: Fourth parties not identified or covered by the contract	Offshore support centre (fourth party), Cloud hosting provider (fourth party)	Confidentiality, Availability, Regulatory and legal	Head of Procurement	Cloud host named in the contract	3	3	9 · Medium	The offshore support subcontractor is not in the contract and was not assessed.
7	R-07	**You cannot verify the vendor's controls** Weakness: No right to audit, access or receive audit reports	Cobalt Ledger Systems	Regulatory and legal	Head of Compliance	Pooled audits; annual SOC 2 report	3	3	9 · Medium	No individual on-site audit right, though the regulator can inspect.
8	R-08	**Too many critical services depend on one provider** Weakness: Concentration never assessed; no alternative	Cloud hosting provider (fourth party)	Availability, Financial	Chief Risk Officer		2	4	8 · Medium	The same cloud host also runs our CRM and card processing.
9	R-09	**Data is processed in a country you did not expect** Weakness: Data locations not written into the contract	Disaster recovery site in Europe, Customer identity and transaction data	Confidentiality, Regulatory and legal	Data Protection Officer	Locations and transfer safeguards in the contract	2	3	6 · Medium	Recovery site in Europe; transfers covered by contract terms.
10	R-10	**The vendor subcontracts or offshores work without telling you** Weakness: No approval right over subcontracting or location changes	Offshore support centre (fourth party)	Confidentiality, Regulatory and legal	Head of Procurement	Change notice clause	2	3	6 · Medium	Cobalt has moved support work once before without notice.
11	R-12	**The vendor is acquired and priorities change** Weakness: No change of control clause or reassessment trigger	Cobalt Ledger Systems	Confidentiality, Availability, Financial	**None**		2	3	6 · Medium	Market reports suggest Cobalt is an acquisition target.
12	R-11	**The vendor fails financially** Weakness: Financial health never checked; no escrow or data retrieval rights	Cobalt Ledger Systems	Availability, Financial	Chief Financial Officer	Audited accounts reviewed	1	5	5 · Medium	Profitable, well-funded vendor with no significant debt.
13	R-13	**Costs rise sharply once you depend on the vendor** Weakness: No price protection; switching costs high	**None linked**	Financial	Chief Financial Officer		–	–	Not rated	

What will be done, by whom and by when

Every risk with a treatment decision, earliest due date first. The third-party controls listed are the ones the treatment relies on; they carry into the remediation plan template. Acceptance is the risk owner's approval of the plan and of the risk that remains.

Ref	Risk	Decision	Planned actions	Third-party controls	Owner and due date	Current to target	Accepted
R-04	**The vendor is slow to tell you about an incident** Head of Compliance	**Modify**	Amend the contract to require notice within four hours and support for our investigation.	TP.5 Incident notification deadline and response support (A.5.20; NIST GV.SC-08) TP.2 Security, confidentiality and data protection clauses in the contract (A.5.20)	Legal Counsel 31 Oct 2026	**12 · High** → **6 · Medium**	Chief Executive 22 Sep 2026
R-06	**A subcontractor the vendor relies on fails** Head of Procurement	**Modify**	Name the support subcontractor in the contract, with flow-down of our terms and approval of changes.	TP.12 Subcontracting approval and flow-down of terms (A.5.21)	Head of Procurement 31 Oct 2026	**9 · Medium** → **6 · Medium**	**Not recorded**
R-05	**A breach at the vendor exposes your data** Chief Information Security Officer	**Modify**	Review the full penetration test report under NDA and check the SOC 2 exceptions are closed each year.	TP.6 Independent assurance reviewed: certificate scope, SOC 2 report (A.5.22) TP.7 Due diligence questionnaire checked against evidence (A.5.19; NIST GV.SC-06) TP.10 Encryption of data held or sent to the vendor (A.8.24)	Chief Information Security Officer 30 Nov 2026	**10 · High** → **5 · Medium**	Chief Executive 22 Sep 2026

R-01	**The vendor's service is unavailable for a long period** Chief Operating Officer	**Modify**	Contract a 4-hour recovery time with service credits, and join the next disaster recovery test.	TP.13 Vendor continuity and recovery plans tested (A.5.30; DORA Art 30(3)) TP.3 Measurable service levels with remedies (A.5.20; DORA Art 30)	Chief Operating Officer 31 Dec 2026	15 · High → 8 · Medium	Chief Executive 22 Sep 2026
R-03	**Attackers get in through the vendor's access to your systems** Chief Information Security Officer	**Modify**	Named, time-bound accounts approved per ticket, with session recording.	TP.8 Least-privilege, time-bound vendor access with MFA (A.5.15, A.8.5) TP.9 Logging and monitoring of vendor access (A.8.15, A.8.16)	Chief Information Security Officer 31 Dec 2026	12 · High → 4 · Low	Chief Executive 22 Sep 2026
R-02	**You cannot leave the vendor without serious disruption** Chief Operating Officer	**Modify**	Write and test an exit plan with a standard export format and a named alternative provider.	TP.14 Exit plan, transition support and data return or deletion (DORA Art 28(8); NIST GV.SC-10) TP.23 Alternative supplier, escrow or in-house fallback TP.20 Concentration and substitutability assessed (DORA Art 29)	Head of Procurement 31 Mar 2027	15 · High → 8 · Medium	Chief Executive 22 Sep 2026

6 risks are within appetite (Medium and below) and need no treatment; 1 are not yet rated.

Where the assessment falls short

Each finding is a gap between the assessment as recorded and what ISO 27001 controls A.5.19 to A.5.23 ask for, with the risks it applies to and the document that closes it.

Severity	Finding	Applies to	What it means	To fix	Document that closes it
MAJOR	**Not yet rated for likelihood and impact**	R-13	Without both ratings a risk has no level, so it cannot be compared with the appetite line or placed in priority order.	Rate each one against the likelihood and impact scales in your criteria.	Risk assessment and treatment methodology
MAJOR	**Risk with no owner**	R-12	Each risk needs an owner who can put the controls in place, usually the relationship owner with security or procurement. Without one, the assessment records a risk nobody will reduce.	Name an owner, by role, for each risk.	Risk assessment and treatment methodology
MAJOR	**Scope item with no risks identified**	Platform API integration	Something you put in scope has no risk attached to it. Either it faces no credible risk, which is rare, or the identification step missed it.	Link an existing risk to it, add a new one, or take it out of scope.	Third-Party Inventory Register
MAJOR	**Limited audit rights over a critical or high-tier vendor**	Due diligence	Without audit, access or inspection rights, the vendor's controls are assumed rather than verified. DORA Article 30(3) requires unrestricted access, inspection and audit rights for critical or important functions, and outsourcing rules such as the EBA's expect them for material outsourcing.	Negotiate audit and access rights, including for regulators, or at least the right to receive independent audit reports every year.	Audit, Access and Information Rights Clause Guide

PROCESS SCORE IN DETAIL

Criteria defined Every likelihood and impact level has a definition, and the appetite line is set.	100%	11 of 11	weight 10
Scope covered Every scope item has at least one risk linked to it.	88%	7 of 8	weight 10
Risk owners named Every risk has an owner accountable for it.	92%	12 of 13	weight 15
Risks rated Every risk has a likelihood and an impact, so it has a level.	92%	12 of 13	weight 15
Ratings explained Existing controls and a rationale are recorded for each risk.	81%	21 of 26	weight 10
Treatment decided Every risk above the appetite line has a treatment option chosen.	100%	5 of 5	weight 15
Targets within appetite Treatments bring each risk to a target at or below the line.	100%	5 of 5	weight 10
Treatments scheduled Each treatment has an owner and a due date.	100%	5 of 5	weight 5
Residual risk accepted Risk owners have accepted what remains after treatment, by name and date.	100%	5 of 5	weight 10
Vendor assessment record complete Tiering, the vendor profile, due diligence, the review, the vendor's response, the decision and the reassessment date are all recorded.	84%	21 of 25	weight 25

Findings by severity

Critical Major Minor

1 · Initial (0+)

A start on a register, not yet an assessment that decisions can rest on.

2 · Developing (40+)

The risks are identified, but gaps in rating or treatment would not survive an audit.

3 · Defined (60+)

A complete, repeatable assessment with a treatment plan behind it.

4 · Managed (80+)

Owned, justified and accepted: ready for management review and audit.

The decision on the vendor

RESIDUAL RISK: CAN THE VENDOR BE APPROVED?

No High or Critical risk remains once the planned controls are in place, so the vendor can be approved on those terms.

REVIEW

Who advised	Reviewed by a risk, outsourcing or vendor management committee
Advice	Outsourcing committee: approve on condition that the contract requires incident notice within four hours, names the support subcontractor and grants on-site audit rights, and that an exit plan is written and tested within six months.
Followed	**Partly**
Why not in full	Cobalt refused individual on-site audits. The committee accepted pooled audits plus annual SOC 2 reports, with the right for the regulator to inspect.

THE VENDOR'S RESPONSE

Response	Findings shared with the vendor, and its response summarised below
Summary or reason	Cobalt agreed to four-hour incident notice, to name its support subcontractor, to replace the shared administrator account by year end and to take part in an exit test. It declined individual on-site audits.

OUTCOME AND APPROVAL

Outcome	**Approve on conditions: the planned controls are in place by the dates set**
Approved by	Chief Executive
Approved on	22 Sep 2026
Next reassessment by	30 Sep 2027

Reassess by the date above, typically every year for critical vendors, every two years for high-tier vendors and at renewal for the rest, and sooner after an incident, a change of service, new subcontractors or a change of ownership. Keep the vendor in your register of third parties with its tier, and follow the conditions through to closure.

A · APPENDIX

Criteria used and basis of this report

A third-party risk assessment rates what the vendor could do to the organization and its customers, so likelihood and impact are set against your own tolerance for disruption, loss and regulatory exposure. This is the record of the criteria every rating in this report was made against.

LIKELIHOOD SCALE

Value	Label	Definition
1	**Rare**	Not expected in the next 5 years; no known case here or in the sector
2	**Unlikely**	Could happen once in 2 to 5 years; has happened in the sector
3	**Possible**	Could happen about once a year
4	**Likely**	Expected several times a year
5	**Almost certain**	Expected monthly or more often, or already happening

IMPACT SCALE

Value	Label	Definition
1	**Negligible**	No noticeable effect on operations or customers; under 10,000
2	**Minor**	Brief disruption of a non-critical service; internal attention; 10,000 to 50,000
3	**Moderate**	A service degraded for days, or limited data exposure; customers notice; 50,000 to 250,000
4	**Major**	A critical function disrupted, or a reportable breach; regulator or media attention; 250,000 to 1 million
5	**Severe**	Critical functions stopped for a long period, or a major breach; sanctions or lasting damage; over 1 million

RISK LEVELS AND ACCEPTANCE

Band	Levels	Treatment
Low	1–4	Accepted without treatment
Medium	5–9	Accepted without treatment
High	10–16	Needs a treatment decision
Critical	17–25	Needs a treatment decision

Level = likelihood x impact. A risk above the appetite line may still be retained, but only with the risk owner's recorded acceptance.

Process score. Ten dimensions: nine for the register, each the share of risks (or of risks above the line) that meet it, and one for the completeness of the vendor assessment record. Each is multiplied by its weight and the total is scaled to 100. A dimension with nothing in scope counts in full. Any critical finding holds the level at Developing, whatever the score.

Your workbook. The Excel workbook that comes with this report is the register as a working file. Change a likelihood or impact on the Risk register sheet and every level, the heat maps on the Dashboard and the process score recalculate. It also holds the treatment plan and a list of the third-party controls your treatments rely on.

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The risks, ratings, risk levels, treatment decisions, findings, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

Third-party risk assessment for Meridian Payments (sample), generated 25 September 2026 by Governance Docs. This is a structured self-assessment based on the organization's own criteria and ratings. It is not a certification, an audit opinion or a substitute for an independent risk assessment.