IQM4007

LEVEL 4 · INDIVIDUAL WRITTEN DOSSIER WITH THREE REQUIRED PARTS.

INTO QUALIFICATIONS

Business Law and Governance

Legal case brief and governance report

STAFF ONLY · Staff marking and administration guide

Assessment
IQM4007 A1

Sample set
2026-S

Status
SAMPLE ASSESSMENT

Response length
Indicative 2,000 words; maximum 2,200 words (+10%), excluding references and appendices unless current local instructions state otherwise.

Total marks
100

Release timing
at coursework release

Administration and delivery

- Give candidates the complete case facts and clarify that missing facts are intended evidence gaps, not invitations to invent facts.
- Check word limit and OSCOLA citations/bibliography; do not treat one bibliography style as a substitute for legal footnotes.
- Provide one supervised progress checkpoint and retain development evidence. AI planning only under module-guide instructions.
- The model answer is a reasoned sample, not legal advice and not the only defensible conclusion.

Mark scheme and indicative content

A_case_brief [See allocation marks]

Facts: the parties agreed price and scope, and BrightPath confirmed CSV export before Northbank paid a deposit. The later signed terms provide a 30-day cure period and a liability cap; they do not state that the launch date is a condition. Issues: whether a contract was formed and on what terms; whether late delivery and unusable export amount to breach; what loss is recoverable; whether the cap applies and is enforceable on the facts. The proposal, acceptance qualified by CSV capability, and written confirmation support formation on the agreed scope and price, with CSV export included.

The signed terms likely form part of the contract, but the sequence and any inconsistent terms should be checked. A 20 July launch was later than the 1 June target. Since the date is not expressly a condition, lateness alone does not automatically establish a right to terminate; its importance, surrounding facts and contractual construction matter. The failed export is more directly a failure to provide an expressly confirmed feature. Northbank gave notice and allowed the stipulated 30 days; the partial fix left two years of records unusable, so it may argue the defect remains uncured.

Recoverable contract damages aim to compensate proven loss subject to causation, remoteness, mitigation, and the contract terms. The £2,400 temporary administrator cost is documented and appears plausibly connected to the failure, subject to proof and reasonableness. The £1,000 documented part of lost contribution may be recoverable if causation and reasonable certainty are shown; unsupported £600 should not be presented as established. The £8,000 replacement claim is presently speculative without a quote and must avoid double recovery.

The liability cap may limit recovery, but its scope, incorporation, construction and any applicable statutory controls require analysis; facts about bargaining power, notice, reasonableness, and the parties' status are missing. The sound conclusion is conditional: Northbank has a credible breach claim concerning CSV functionality and delay, but termination and damages cannot be predicted conclusively without the full contract, evidence of loss, cure communications, and legal review.

Business significance: contract governance should define acceptance tests, critical dates, data portability, cure/termination rights, liability allocation, and escalation before implementation.

B_governance_report [See allocation marks]

The board approved a material technology dependency without a written risk assessment or accountable sponsor. This weakens oversight, creates unclear ownership of acceptance and remediation, and makes escalation reactive. Customer repair histories were accessible to all supplier staff in a shared test environment. Even without evidence of access, this is an avoidable confidentiality and security exposure. Northbank should establish whether personal data is present, identify controller/processor roles and contractual duties, preserve logs, restrict access, and assess whether any personal-data breach occurred.

It should not notify regulators or customers solely on speculation; a documented risk assessment should determine applicable duties and time limits. Termination now could protect data and service continuity but may interrupt bookings and incur replacement cost. Continuing without safeguards would preserve service but prolong operational and data risk. A time-limited negotiated remediation is preferable if BrightPath can promptly deliver a tested export, evidence access controls, and meet a documented recovery plan; reserve rights and prepare a migration fallback.

The board should appoint an accountable project owner, require independent acceptance tests, least-privilege access, named supplier accounts, access logging, retention/deletion rules, incident notification obligations, backup/export tests, milestone payments, and quarterly supplier-risk review. Record decision rationale and conflicts, oversee remediation, and report residual risk. Do not treat a contract cap as a substitute for operational control.

Immediate actions: freeze unnecessary test access; preserve logs; validate the data inventory; secure a tested export; quantify and evidence loss; obtain replacement quotations; review full executed terms; obtain specialist advice before termination or litigation. Longer term, maintain a supplier register, risk tiers, standard contract clauses and a board dashboard for critical technology projects.

A_case_brief_extension [See allocation marks]

The evidence sequence matters. The operations manager's 3 March reply was conditional on CSV export; BrightPath's same-day written confirmation appears to answer that condition before Northbank paid the deposit. This gives Northbank a strong factual basis to say CSV capability formed part of the agreed scope. The 8 March standard terms arrived later, but both parties electronically signed them on 10 March. The signed terms may govern the cure process and cap, while the earlier confirmation may remain part of the scope unless the later document clearly varies it.

The complete document set, signature workflow, any order-of-precedence clause, and what the signatories understood should be reviewed. The court or decision-maker would construe the documents as a whole rather than select a sentence in isolation. The 1 June date is described in the signed terms as a target, and there is no express statement that time is of the essence or that delay automatically permits termination. The 20 July launch is late, but the legal significance depends on whether the target was contractual, whether BrightPath gave assurances that Northbank relied upon, and what practical consequences were foreseeable.

A delay may support a claim for proven losses even if it does not justify termination. The CSV function is stronger: it was specifically raised, confirmed and then unavailable for two years of repair histories after the cure period. The partial export may be inadequate if the contract required usable export of the full repair history. Northbank should define the export acceptance test in measurable terms and give BrightPath a precise defect schedule; it should preserve the 25 July notice and evidence showing whether the 30-day cure period ran from that notice and how the 24 August partial fix was assessed.

The loss analysis should separate established expenditure from estimates. The £2,400 administrator cost is documented, but Northbank must show it was a reasonable response to the export failure, not an unrelated staffing expense. Of the estimated £1,600 lost contribution, £1,000 is supported by records; the remaining £600 is not yet evidenced. For each cancelled booking, retain booking, cancellation and replacement/mitigation records and calculate contribution rather than gross revenue. The £8,000 replacement figure has no quotation, and any recovery must avoid duplication with the cost of continued remediation or value already received.

The £18,000 implementation fee and £400 support payment are contract payments, not automatically losses. Northbank should obtain at least one replacement quote and compare migration, training, support and data-conversion costs. The liability cap's wording refers to fees paid in the previous three months, but the record gives only £18,000 implementation and £400 support; the meaning of 'fees'

and relevant period is uncertain. A signed cap is not automatically decisive: review incorporation, scope, statutory controls relevant to this business contract and the parties' circumstances.

Do not promise recovery beyond the cap or assume the cap defeats every remedy. A negotiated repair, partial refund, replacement support or agreed exit could be more proportionate than immediate litigation if data can be secured and operations maintained. The conclusion remains conditional on the full contract, timely notice, proof of loss and data facts.

B_governance_report_extension [See allocation marks]

The shared test environment creates a control weakness even though no unauthorised access is known. The board should ask whether repair histories identify customers or contain other personal information, who had credentials, whether access logs are available, what purpose the supplier had, and whether the test environment used real or masked records. Until those questions are answered, treat access as a risk to investigate, not as proof of disclosure.

Restrict supplier access to named personnel with a current business need; disable broad shared accounts; rotate credentials if appropriate; preserve logs before making changes that could destroy evidence; and record why any account remains enabled. If personal data is involved, the organisation should assess the event under its applicable data-protection responsibilities and contractual incident terms, record the risk decision and seek specialist advice on any notification duty and timing.

Customer or regulator communication should be accurate and based on the evidence and applicable threshold, not automatic or suppressed for reputational reasons. Three options are available. Immediate termination may stop ongoing access and create leverage, but it could interrupt online bookings and leave the only system holding repair data unavailable. It also risks a dispute about termination rights, cure completion and liability limitation. Continuing without conditions is the weakest option because it accepts unresolved export and access risk.

A time-limited remediation agreement is the proportionate first step if BrightPath can provide a complete, independently tested CSV export, restrict and evidence supplier access, restore or supply usable records, and meet a dated recovery plan. Northbank should reserve contractual rights in writing, avoid language that waives claims, and obtain advice before termination. In parallel, prepare a fallback migration and identify what information staff need to continue safe repairs. If BrightPath misses a milestone or fails the objective export test, the board can move to an agreed exit or termination after reviewing the contract.

The control plan should have an owner and evidence at each gate. Within 48 hours, the project sponsor should freeze unnecessary test access, preserve access records, identify real versus test data, and appoint a data-protection contact. Within five working days, BrightPath should provide named-account lists, access logs, data-flow details and a complete export plan; Northbank's operational owner should test the CSV against agreed fields, record counts and date ranges. Within ten working days, the board should review a replacement quote, migration time, backup/restore test, loss schedule and supplier response.

Any unresolved high risk should be explicitly accepted by the board with an expiry date, or the service should be paused. Before future procurement, require a documented business owner, risk assessment, data inventory, security review, acceptance criteria, test evidence, service levels, transition assistance, audit rights, incident notification, deletion certification and a proportionate liability position. Quarterly supplier review should track delivery milestones, defects, data access, continuity and open actions.

The objective is not paperwork for its own sake; it is to make someone accountable for whether the system performs safely and whether Northbank can recover its information.

C_checklist_operating_detail [See allocation marks]

Use the checklist as a board decision control with three recorded columns: owner, due date and evidence. At project approval, the board sponsor signs the risk assessment and confirms who has authority to accept deviations. Before go-live, the operational owner signs a test record that includes a full two-year CSV export, field reconciliation, duplicate/missing-record check, and restore/import test. Supplier access is approved by the data contact for named users and time-limited; the access review records date, purpose and removal. A monthly dashboard flags overdue defects, failed exports, unapproved accounts and unmitigated risks.

Any failed acceptance test, unexplained data access or missed cure milestone triggers escalation to the sponsor within one working day and a documented pause/continue decision. Before closure, Northbank obtains a usable export, confirms transition support, records where copies remain, and receives deletion evidence for unnecessary supplier-held data. The board closes the issue only when the operational owner confirms evidence, not merely when the supplier says a fix is complete.

C_checklist [See allocation marks]

- Named board sponsor and operational project owner recorded; decision rights and escalation route defined.
- Signed scope and acceptance criteria include required data exports, interoperability, test cases, owners and pass/fail evidence.
- Milestones, dependencies, cure periods, termination/transition assistance, fees, and liability terms reviewed before signature.
- Data inventory and controller/processor roles documented; minimum necessary test data used; access limited to named, time-bound accounts.
- Supplier access logged and reviewed; encryption, secure transfer, retention/deletion, backup and incident escalation tested.
- Go-live requires independent acceptance sign-off, tested export/restore, staff training, and open-risk approval.
- Monthly delivery and defect review; quarterly supplier risk, performance, data access and continuity review; actions assigned and tracked.
- Incident response identifies decision owner, evidence preservation, risk assessment, and notification route; do not assume that every incident is reportable.

Assessment rubric

Criterion	Marks	Marking focus
A	35	Issue spotting/facts (5); accurate legal principles and authority use (10); application/reasoning (12); remedies/outcome/business significance (8). Credit conditional conclusions and expressly identified evidence gaps.
B	50	Governance/control diagnosis (10); legal/operational/ethical risk and consequence analysis (12); evidence and alternative options (10); proportionate prioritised recommendations (12); coherent professional structure and integration (6).

Criterion	Marks	Marking focus
C	15	Operational usability and accountability (5); relevant prevention/detection/response controls (5); fit to identified risks and clear trigger/owner/evidence (3); professional concise drafting (2).

Standardisation guidance

- A student may argue for termination or continuation if the uncertainty, service continuity, evidence, proportionality and data risks are handled explicitly. Accept equivalent controls. Do not award full credit for treating suspected exposure as proven breach or for asserting that termination is automatic.