AI GOVERNANCE REVIEW PACK · A8

Vendor and model due diligence questionnaire

Fictional organisation, illustrative only, not a client case study. Quillmarrow Supplies Pte. Ltd. (fictional) is invented. All people are shown by role only.

Organisation	Quillmarrow Supplies Pte. Ltd. (fictional)
Document	A8 · Vendor and model due diligence questionnaire
Version	1.0
Date	30 October 2026 (illustrative)
Prepared by	Alex Lew, reviewer and sign-off
Client approver (role)	Chief Operating Officer
Label	Fictional organisation, illustrative only, not a client case study

Quillmarrow sent the same 30 questions to the three vendors whose AI features carry the most risk in the register: Fictional Helpdesk (V-01, helpdesk reply drafting and web-chat), Fictional Reorder Agent (V-02, the supplier reorder agent pilot) and Fictional Talent Screen (V-03, CV screening). The questions cover six areas: data use and training, data location and transfers, security and access, contract and accountability, model documentation and testing, and agent actions and logging.

Each answer below summarises what the vendor said or supplied by the end of fieldwork. Status shows whether evidence was provided. Missing evidence stays visible: a vendor statement without a supporting document or setting is recorded as Partial, and no gap has been filled with an assumption. Nothing here is a finding about any real company or product.

The answers were reviewed for governance purposes only. They are not a legal review of vendor terms; contract questions should be confirmed with a Singapore-qualified lawyer.

Evidence summary

Vendor	Evidence provided	Partial	Not provided	Not applicable
V-01 Fictional Helpdesk	24	6	0	0

Vendor	Evidence provided	Partial	Not provided	Not applicable
V-02 Fictional Reorder Agent	2	23	4	1
V-03 Fictional Talent Screen	0	13	15	2

Data use and training

Q	Question and evidence requested	V-01 Fictional Helpdesk	V-02 Fictional Reorder Agent	V-03 Fictional Talent Screen
Q01	**Are customer prompts, inputs or outputs used to train or improve any model?** Why: Training use may affect confidentiality and control over Quillmarrow data. Evidence: DPA or service schedule and the applicable tenant training setting.	**Evidence provided.** Says customer prompts and replies are not used for general model training. Supplied the DPA schedule and an admin-console screenshot showing the tenant setting disabled.	**Partial.** Says prompts are excluded from foundation-model training, but may be used to improve its agent workflow. Supplied a product FAQ, not a contract commitment or setting.	**Not provided.** Says data may be used to improve the service, subject to customer settings. Supplied no definition of improvement use or setting evidence.
Q02	**What data is collected, stored and processed for the service, including prompts, outputs and metadata?** Why: A clear data inventory supports data minimisation and impact assessment. Evidence: Data-flow diagram, data dictionary and retention settings.	**Evidence provided.** Says the service processes ticket text, draft replies, user IDs and usage metadata. Supplied a data-flow diagram and field inventory.	**Partial.** Says it processes stock, sales history, supplier and purchase-order data plus workflow logs. Supplied a field list, but it does not identify all metadata or retention by field.	**Partial.** Says it processes CVs and applicant details. Supplied no field-level inventory or data-flow diagram.
Q03	**Can customers control retention, deletion and use of their data?** Why: Quillmarrow needs workable controls over data kept by the vendor. Evidence: Retention and deletion schedule, tenant settings and deletion procedure.	**Partial.** Says tenant administrators can set retention and request deletion. Supplied a retention-settings guide, but no tenant-specific screenshot or deletion test.	**Partial.** Says data is deleted on request and inactive pilot data is periodically purged. Supplied no schedule or deletion evidence.	**Not provided.** Says retention depends on the customer agreement. Supplied no retention schedule, deletion procedure or setting evidence.
Q04	**How are customer data and any derived data separated between tenants?** Why: Tenant separation helps prevent one customer's information reaching another. Evidence: Architecture summary and independent security assessment covering tenant isolation.	**Evidence provided.** Says tenant data is logically separated using tenant-specific access controls. Supplied an architecture summary and a 2026 penetration-test executive summary covering isolation testing.	**Partial.** Says each customer has a separate workspace and scoped credentials. Supplied an architecture note, but no independent isolation test.	**Partial.** Says customer workspaces are separated. Supplied a short product note without technical detail or test evidence.
Q05	**Can Quillmarrow exclude selected data fields or redact sensitive content before processing?** Why: Field controls can reduce unnecessary disclosure of personal or confidential data. Evidence: Configuration guide and tenant setting or demonstration record.	**Evidence provided.** Says administrators can configure field exclusions and redact selected identifiers before AI processing. Supplied the configuration guide and a tenant-setting screenshot.	**Partial.** Says source fields can be allow-listed by the implementation team. Supplied an implementation checklist, but no configuration from Quillmarrow's tenant.	**Not provided.** Says customers can choose which CV fields to include. Supplied no field-selection guide or tenant setting.

Data location and transfers

Q	Question and evidence requested	V-01 Fictional Helpdesk	V-02 Fictional Reorder Agent	V-03 Fictional Talent Screen
Q06	**Where are customer data, backups and service logs stored and processed?** Why: Locations matter to data governance, risk review and transfer assessment. Evidence: Hosting and processing-location schedule covering primary data, backups and logs.	**Evidence provided.** Says primary tenant data is hosted in Singapore, with backups in a named regional location. Supplied a current hosting-location schedule covering data and backups.	**Partial.** Says production data is hosted in Singapore and backups in another Asia-Pacific location. Supplied a cloud-region statement, but it omits support and telemetry logs.	**Partial.** Says data is hosted in a regional cloud environment. Supplied no country-level location or processing schedule.
Q07	**Which subprocessors can access or process customer data, and where are they located?** Why: Subprocessor access can create additional transfer and oversight risks. Evidence: Current subprocessor list with purposes, access types, locations and change-notice process.	**Evidence provided.** Says subprocessors are listed in its trust centre and customers receive advance notice of material changes. Supplied a dated list with locations and service purposes.	**Partial.** Says it uses a cloud-hosting provider and an email-delivery service. Supplied names but no locations, access descriptions or change-notice terms.	**Not provided.** Says selected infrastructure providers may support the service. Supplied no named list or locations.
Q08	**Can vendor staff or support teams access Quillmarrow data from outside the hosting country?** Why: Remote access can create cross-border exposure even where data is hosted locally. Evidence: Support-access policy, role permissions and access-location records.	**Partial.** Says support access is restricted, approved and logged, including when conducted across borders. Supplied a trust-centre support-access policy, but no customer-specific access log.	**Partial.** Says engineers may access logs for support after approval. Supplied no staff-location policy or access record.	**Partial.** Says authorised staff may provide support where needed. Supplied no access policy or location details.
Q09	**How are cross-border transfers identified and controlled?** Why: Quillmarrow needs visibility of transfer routes and applicable safeguards. Evidence: Transfer map and contractual or technical safeguards for each transfer route.	**Evidence provided.** Says transfer routes are documented and governed through its DPA and subprocessor terms. Supplied a transfer summary and the relevant DPA schedule.	**Not provided.** Says its hosting and support suppliers may process data in the region. Supplied no transfer map or safeguard documents.	**Not provided.** Says regional processing may occur depending on service configuration. Supplied no transfer map or supporting terms.
Q10	**Are customer-specific data-location restrictions available?** Why: A restriction may be needed to meet Quillmarrow's approved data-handling requirements. Evidence: Product configuration guide and contractual confirmation of available location options.	**Partial.** Says location options depend on the service plan and tenant configuration. Supplied a general guide but no confirmation for Quillmarrow's proposed service.	**Partial.** Says it can select a Singapore production region for new deployments. Supplied a deployment note, but backup location and support access remain unspecified.	**Not provided.** Says location is determined by the service environment. Supplied no selectable location setting or contract commitment.

Security and access

Q	Question and evidence requested	V-01 Fictional Helpdesk	V-02 Fictional Reorder Agent	V-03 Fictional Talent Screen
Q11	**What authentication and administrator-access controls are available?** Why: Strong access controls reduce the risk of unauthorised use or disclosure. Evidence: Security policy and admin-console screenshots or configuration export.	**Evidence provided.** Says administrators can enforce multi-factor authentication, role-based access and session controls. Supplied a current access-control guide and sample admin screenshots.	**Partial.** Says administrator accounts support multi-factor authentication and role assignment. Supplied an admin guide, but no tenant configuration or access review.	**Partial.** Says accounts use passwords and administrator roles. Supplied no detailed access-control setting or evidence.
Q12	**How are privileged access and vendor staff access reviewed and logged?** Why: Review and logging make elevated access accountable and detectable. Evidence: Privileged-access procedure and a redacted access-log sample.	**Evidence provided.** Says privileged access is time-limited, approved and logged, with periodic review. Supplied the procedure and a redacted sample access log.	**Not provided.** Says founders and engineers hold administrative access. Supplied no formal review cadence or access-log sample.	**Not provided.** Says support staff can access accounts to resolve issues. Supplied no approval, review or logging procedure.
Q13	**What encryption is applied to data in transit and at rest?** Why: Encryption is a baseline safeguard for stored and transmitted data. Evidence: Security architecture summary and current encryption configuration evidence.	**Evidence provided.** Says data is encrypted in transit and at rest using standard managed controls. Supplied a 2026 security architecture summary describing the controls.	**Partial.** Says transport connections are encrypted and storage encryption is enabled by the hosting provider. Supplied a hosting configuration summary, not a full service design.	**Partial.** Says data is protected using encryption. Supplied no technical detail or configuration evidence.
Q14	**Are independent security assessments performed, and how are findings handled?** Why: Assessment evidence and remediation records help evaluate security assurance. Evidence: Recent penetration-test summary, assurance report or remediation attestation.	**Evidence provided.** Says it commissions annual penetration testing and tracks findings to closure. Supplied a 2026 penetration-test executive summary and remediation attestation.	**Not provided.** Says it completed an internal security review before launch. Supplied no independent assessment or remediation record.	**Partial.** Says security checks are performed as part of development. Supplied no assessment summary or remediation evidence.
Q15	**How are security incidents detected, reported and communicated to customers?** Why: Prompt notification supports investigation and response by the customer. Evidence: Incident-response policy and contractual notification commitment.	**Evidence provided.** Says it maintains an incident-response process and will notify affected customers under the DPA. Supplied the policy and DPA schedule.	**Partial.** Says it will contact customers if an incident affects their data. Supplied a short incident-response outline without a contractual timeframe.	**Partial.** Says it will notify customers of significant incidents. Supplied no definition, process or contractual timing.

Contract and accountability

Q	Question and evidence requested	V-01 Fictional Helpdesk	V-02 Fictional Reorder Agent	V-03 Fictional Talent Screen
Q16	**Will the vendor sign data-processing terms that define its role and instructions?** Why: Written terms clarify responsibilities and permitted processing. Evidence: Proposed DPA or data-processing schedule for the service.	**Evidence provided.** Says it will sign its standard DPA with customer-specific service details. Supplied the current DPA and processing schedule.	**Partial.** Says it is preparing a DPA for enterprise customers. Supplied a draft with unresolved security and subprocessor terms.	**Not provided.** Says its standard terms cover service operation. Supplied no DPA or processing schedule.
Q17	**What assistance does the vendor provide for data-subject requests, incidents and regulatory enquiries?** Why: Quillmarrow may need vendor support to meet its own responsibilities. Evidence: Contract schedule and operational procedures for assistance and escalation.	**Evidence provided.** Says it routes requests and incidents to a named customer contact and provides export or deletion support. Supplied a DPA schedule and support-escalation procedure.	**Partial.** Says its team will help with requests and incident enquiries. Supplied no service commitment or procedure.	**Not provided.** Says customers should contact support for assistance. Supplied no defined response or escalation process.
Q18	**How are service changes, subprocessors and material AI changes communicated?** Why: Advance notice allows Quillmarrow to assess changes before relying on them. Evidence: Contract notice terms and change-management process.	**Evidence provided.** Says it gives advance notice of material service and subprocessor changes through its trust centre and customer notices. Supplied the change-notice policy and DPA clause.	**Partial.** Says it will notify customers of material changes by email. Supplied a product FAQ, but the draft contract does not include a notice period.	**Partial.** Says product features may change over time. Supplied no specific process for notice of material model or service changes.
Q19	**What contractual commitments apply to confidentiality, security and data return or deletion at termination?** Why: These commitments govern protection and exit arrangements. Evidence: Confidentiality, security and termination clauses in the proposed contract.	**Evidence provided.** Says its DPA and service terms cover confidentiality, security and data return or deletion at termination. Supplied the relevant clauses.	**Partial.** Says it will return or delete customer data when service ends. Supplied this only in an unsigned draft order form.	**Partial.** Says customers can close their account and request deletion. Supplied no contractual wording or deletion confirmation process.
Q20	**Can Quillmarrow obtain assurance evidence and raise unresolved control concerns?** Why: A defined assurance route supports ongoing vendor oversight. Evidence: Assurance pack, customer assurance process and escalation route.	**Evidence provided.** Says it provides a trust-centre assurance pack and a route for customer security questions. Supplied a current SOC 2 Type II bridge letter and trust-centre index.	**Not provided.** Says it can answer security questions during onboarding. Supplied no assurance pack or named escalation route.	**Not provided.** Says it can respond to customer questions on request. Supplied no assurance documents or escalation route.

Model documentation and testing

Q	Question and evidence requested	V-01 Fictional Helpdesk	V-02 Fictional Reorder Agent	V-03 Fictional Talent Screen
Q21	**What does the system do, what are its intended uses and what uses are out of scope?** Why: Clear boundaries help prevent use beyond the service's evaluated purpose. Evidence: Product description, intended-use statement and limitation documentation.	**Evidence provided.** Says reply drafting supports agent-reviewed replies and the web-chat component is a separate configurable feature. Supplied product cards describing intended uses and limitations.	**Partial.** Says the agent proposes replenishment orders from inventory signals. Supplied a workflow description, but it does not fully specify out-of-scope actions.	**Not provided.** Says the service parses CVs and ranks applicants against employer criteria. Supplied no detailed intended-use or limitations document.
Q22	**What information is available about model or system versions and material updates?** Why: Version information helps investigate changes in behaviour and assess updates. Evidence: Version policy, release notes and customer change notifications.	**Evidence provided.** Says model and service changes are tracked and material changes are announced. Supplied a release-history page and change-notice policy.	**Partial.** Says it records agent workflow releases and can provide release notes. Supplied a version register, but model-version reporting depends on its upstream provider.	**Not provided.** Says the service is updated periodically. Supplied no version register or release history.
Q23	**What testing has been performed for accuracy, reliability and foreseeable failure cases?** Why: Testing evidence helps identify limitations before the service is used. Evidence: Test plan, results, known limitations and remediation records.	**Partial.** Says it tests reply-drafting quality and service reliability before releases. Supplied a 2026 testing overview, but not task-specific results for Quillmarrow's proposed configuration.	**Partial.** Says it has tested common reorder workflows and failure handling. Supplied a short internal checklist without results or independent review.	**Partial.** Says it checks parsing quality during development. Supplied a brief overview without metrics, methods or subgroup results.
Q24	**What documentation explains how the system reaches outputs and what limits apply?** Why: Useful explanations help staff assess outputs rather than treat them as authoritative. Evidence: Model or system card, explanation guide and limitations documentation.	**Evidence provided.** Says it can show the ticket text and knowledge sources used to draft a reply, but does not expose internal model reasoning. Supplied an operator guide with this distinction.	**Evidence provided.** Says each draft includes the data values and reorder rule that contributed to the proposal. Supplied a sample explanation panel and workflow guide.	**Not provided.** Says ranking reflects the employer's criteria and service configuration. Supplied no explanation guide or model documentation.
Q25	**How are fairness risks identified, tested and addressed for affected groups?** Why: Fairness evidence is important where outputs may affect people's opportunities. Evidence: Fairness assessment, test methodology, results by relevant groups and remediation record.	**Partial.** Says the reply-drafting feature is not designed to rank or make decisions about people. Supplied a product-scope note; no fairness testing report was provided.	**Not applicable.** Says the service concerns stock replenishment rather than decisions about individuals. Supplied a system description supporting that scope.	**Not provided.** Says customers should review rankings for fairness. Supplied no fairness assessment, test method or results.

Agent actions and logging

Q	Question and evidence requested	V-01 Fictional Helpdesk	V-02 Fictional Reorder Agent	V-03 Fictional Talent Screen
Q26	**Can the system take actions on external parties or make changes without a human approval?** Why: The system's autonomy determines the controls and oversight required. Evidence: Permission matrix, workflow diagram and configuration evidence for action gates.	**Evidence provided.** Says reply drafting does not send a response without a user action, while web-chat has separate customer-facing settings. Supplied workflow diagrams and admin-setting screenshots.	**Partial.** Says it can create draft purchase orders and send them by email after configured approval. Supplied a permissions matrix; it says the gate exists but has not demonstrated it working in Quillmarrow's tenant.	**Not applicable.** Says the service produces parsing and ranking results and does not contact candidates or make hiring decisions. Supplied a product-scope statement.
Q27	**Can administrators restrict the system's permitted resources, recipients and actions?** Why: Least-privilege controls limit the consequences of errors or misuse. Evidence: Permission configuration guide and tenant-specific access export.	**Partial.** Says administrators can restrict data sources, user roles and web-chat hand-off settings. Supplied a configuration guide, but no Quillmarrow tenant export.	**Partial.** Says resource scopes and supplier allow-lists are configurable. Supplied a permission template, not the deployed tenant configuration.	**Partial.** Says employer users control access to applicant records. Supplied no permission matrix or configuration evidence.
Q28	**Are proposed actions subject to approval, and can approval be bound to the exact action?** Why: Approval must apply to the specific action that will occur, not a later altered version. Evidence: Approval workflow specification, screen example and test evidence showing change invalidation.	**Evidence provided.** Says users review and approve drafted replies before sending; web-chat responses follow a separately configured workflow. Supplied workflow documentation and screen examples.	**Partial.** Says a purchase-order approval gate is available and approval is linked to the draft. Supplied a sample approval screen, but no successful or negative test from Quillmarrow's tenant.	**Not applicable.** Says rankings are available to employer users for review. Supplied no approval workflow because the service does not execute external actions.
Q29	**What actions and decisions are logged, and can logs be exported for review?** Why: Audit records support reconstruction, oversight and incident investigation. Evidence: Sample audit-log export with event fields, timestamps, actor and action outcomes.	**Evidence provided.** Says it records user approvals, sends, escalations and configuration changes. Supplied a redacted sample audit-log export.	**Evidence provided.** Says it logs source data timestamps, draft changes, approvals, stop conditions and send outcomes. Supplied a sample audit-log export with event identifiers and timestamps.	**Not provided.** Says user activity is recorded for account administration. Supplied no sample log or evidence that ranking inputs and outputs are captured.
Q30	**Can the system be paused or disabled, and what happens to pending actions?** Why: A reliable stop mechanism helps contain failures and uncertain actions. Evidence: Pause or disable procedure, queued-action behaviour and test record.	**Evidence provided.** Says administrators can disable AI drafting and web-chat separately; pending drafts remain unsent. Supplied the disable procedure and a service test note.	**Partial.** Says an administrator can pause new runs and queued purchase orders remain drafts. Supplied an operational runbook, but no tenant test showing queued-order behaviour.	**Partial.** Says administrators can suspend user access to the service. Supplied a settings screenshot, but no record-retention or pending-processing test.

What the answers mean for each use

Vendor	Linked use	Position after fieldwork	Recommendation	Owner role
V-01 Fictional Helpdesk	AI-02 helpdesk drafting (Tier 2); AI-12 web-chat bot (Tier 3, not live)	Strong evidence on training use, data location, security and contract. Open: retention and deletion confirmed for Quillmarrow's tenant (Q03), task-specific testing (Q23), and web-chat permissions set up in the tenant (Q27).	Keep AI-02 approved with a person approving each reply. Do not start the web-chat pilot until Q27 is evidenced and the hand-off controls in A6 are configured.	Head of Customer Service
V-02 Fictional Reorder Agent	AI-03 supplier reorder agent (Tier 3, pilot)	Good logging evidence (Q29). Most other answers are statements, a draft DPA or templates. The approval gate, supplier allow-list and pause are described but not shown working in Quillmarrow's tenant (Q27, Q28, Q30).	Keep the pilot in draft-only mode until the tests in A7 pass in the tenant and the DPA is signed.	Purchasing Lead with the IT Manager
V-03 Fictional Talent Screen	AI-04 CV screening (Tier 3, on hold)	No answer is backed by evidence. Training use (Q01), data location (Q06, Q07), retention (Q03), the DPA (Q16), explanation (Q24) and fairness testing (Q25) are all missing.	Do not proceed in the current form. Keep AI-04 on hold, as set out in AIA-03.	HR Manager; decision by the Managing Director

Follow-up requests

ID	Request	Vendor	Owner role	Due
VF-01	Screenshot of tenant retention and deletion settings, and the web-chat permission configuration	V-01	Head of Customer Service	Day 30
VF-02	Signed DPA with subprocessor list, locations and change-notice period	V-02	Purchasing Lead	Day 30
VF-03	Recorded test in Quillmarrow's tenant: an order blocked without approval, an off-list supplier blocked, and a pause that holds queued orders as drafts	V-02	Purchasing Lead with the IT Manager	Before pilot widens
VF-04	Independent security assessment summary or a dated plan to obtain one	V-02	IT Manager	Day 60
VF-05	Only if management reopens AI-04: training-use setting, country-level hosting, DPA, explanation guide and fairness test method and results	V-03	HR Manager	Before any reconsideration

Each answer that arrives is filed against its question number, and its status in the workbook is updated. A status only moves to Evidence provided when the document, setting or test record is on file.

How this maps to the reference frameworks

- **Model AI Governance Framework for Generative AI (May 2024).** The accountability dimension expects responsibility to be shared sensibly along the supply chain. The questionnaire makes that split explicit for each vendor, and the follow-up requests close the gaps that sit on the vendor's side.

- **Model AI Governance Framework for Agentic AI (January 2026).** Its first dimension, assessing and bounding the risks upfront, is why the agent questions (Q26 to Q30) ask for permissions, approval gates and a pause shown working in the tenant, not just described.
- **PDPC Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems (March 2024).** These are relevant to AI-04, where applicants' personal data would feed a ranking. The missing answers for V-03 are the information Quillmarrow would need before it could explain the use to applicants.
- **Model AI Governance Framework, Second Edition (January 2020).** Operations management and stakeholder communication rely on knowing how a vendor's system was tested and how it changes, which Q21 to Q25 cover.
- **AI Verify (11 principles).** The questions map mainly to transparency, data governance, security, robustness, fairness, accountability, and human agency and oversight. This is a process-level mapping only; no AI Verify technical tests were run.

About this sample

Fictional organisation, illustrative only, not a client case study. Quillmarrow Supplies Pte. Ltd., its people, vendors, findings and dates are invented. Nothing in this document reports a client result.

I personally review and sign off every deliverable. You appoint your own DPO. I support them.

This is practical compliance support, not legal advice. For legal advice, use a Singapore-qualified lawyer.

What's not included

- Legal advice, legal opinions on vendor terms or regulatory representation.
- AI Verify technical testing, model benchmarking, penetration testing or security engineering, unless the relevant work is separately scoped.
- Building an AI system, implementing integrations or changing live permissions and configurations.
- Certification, a compliance guarantee or an assurance that a model cannot fail.
- An organisation-wide ISO/IEC 42001 readiness engagement unless expressly included in the quote.
- Healthcare-sector work or on-site delivery.

ISO/IEC 42001 work is a readiness check only, never certification. Questions about this sample: DM @alewyl1 on X, or ask for a free intro call (coffee chat).