AI GOVERNANCE REVIEW PACK · A9

Management report and action plan

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	A9 · Management report and action plan
Version	1.0
Date	30 October 2026 (illustrative)
Prepared by	Alex Lew, reviewer and sign-off
Client approver (role)	Managing Director
Label	Fictional organisation, illustrative only, not a client case study

Addressed to the Managing Director and Chief Operating Officer.

1. Executive summary

Quillmarrow's illustrative review covers 20 AI uses, three fictional vendors, three impact assessments and one supplier reorder agent pilot. It considers the information supplied in the AI-use register, oversight matrix and vendor questionnaire, together with the case-file scope and engagement facts.

Overall position: Amber, with Red issues requiring management attention. Quillmarrow now has an agreed register and an allocation of owners and oversight responsibilities. These provide a starting point, but they do not, by themselves, demonstrate that settings are configured or that staff follow the intended process. Evidence is complete for some uses and partial or missing for others.

The most urgent concern is AI-03, the supplier reorder agent. The pilot's default configuration could send purchase orders without approval. V-02 says an approval gate is available, but has not shown it working in Quillmarrow's tenant. The agreed rule is that the Purchasing Lead approves **every** purchase order before the agent sends it. Sending should remain disabled until that gate, the approved limits and the controls in A7 are configured and demonstrated.

AI-04, the proposed CV-screening and ranking service, remains on hold and is **not recommended in its current form**. The proposal raises the risk of automated decisions affecting applicants, but the supplied evidence does not establish the precise decision workflow. No screening or ranking should take place while the hold applies. V-03 has supplied substantial partial or missing evidence, including no fairness assessment or test results.

Staff use of ChatGPT on personal accounts requires clear communication and a managed route to an approved tool. The supplied facts do not establish which staff used it, what was submitted or whether personal data was exposed. Those points need proportionate investigation, not assumed conclusions.

Area	Summary
Red	Agent sending controls are unproven; the CV-screening proposal lacks evidence and remains on hold.
Amber	Staff rules, personal-data handling, vendor assurance, transparency and incident arrangements need implementation or evidence.

Area	Summary
Green	The agreed register, tiering and oversight assignments provide a documented basis for ownership and control. Green does not mean every control has been tested.

Five management decisions are needed:

1. **MD:** confirm that AI-03 may continue only after the approval gate and other pilot controls are demonstrated.
2. **MD:** maintain the hold on AI-04 and do not proceed with the proposal in its current form.
3. **COO:** approve the AI-use policy and the move from personal ChatGPT accounts to an approved tool.
4. **COO:** appoint the register owner and require quarterly review and vendor-feature change notification.
5. **MD:** require approval of AI-12's pilot design and controls before any customer-facing pilot.

2. Scope and approach

The illustrative engagement spans about two weeks and is fully remote. It comprises interviews with role holders, document review and workflow walk-throughs using descriptions and made-up or de-identified samples only. No client personal data was put into AI tools.

The report draws on A1 scope, A2 register, A3 tiering, A4 policy, A5 impact assessments, A6 oversight matrix, A7 agent permissions and audit-trail specification, and A8 vendor questionnaire. A10 is a separate ISO/IEC 42001 readiness excerpt.

The register uses Tier 1 Low, Tier 2 Medium, Tier 3 High and Not permitted as business working categories, not statutory classifications. This review did not include technical testing, verification of live configurations or legal advice. Vendor statements and sample documents are not treated as proof of Quillmarrow-specific operation.

3. Overall RAG by area

The ratings express management priority from the supplied information. An evidence gap is not, on its own, proof that a control has failed.

Area	RAG	Reason
Inventory and ownership	Green	A2 now lists 20 uses with owners, tiers and statuses; ongoing ownership and quarterly maintenance need formal confirmation.
Staff use rules	Amber	Personal-account use was found, while the policy and staff acknowledgement need approval and implementation evidence.
Personal data in AI tools	Amber	Restrictions are defined for AI-06, but actual inputs, tool settings and several vendor data flows remain unconfirmed.
Human oversight	Amber	A6 assigns decisions to people, but evidence that the checks operate consistently is incomplete for several uses.
Agents and write actions	Red	AI-03 could send without approval in its pilot default configuration; tenant-specific approval and stop controls are unproven.
Vendor evidence	Amber	V-01 has mostly provided evidence; V-02 and V-03 have substantial partial or missing responses.
Customer transparency	Amber	Web-chat pilot design, escalation and customer-facing controls are not supplied; AI-11 consent and audience checks remain open.
Incident handling	Amber	A near-miss is reported, but an AI-specific incident route and test evidence are not supplied.

4. Top five findings

F1. Personal ChatGPT accounts need a controlled transition

What we found. Staff use of ChatGPT on personal accounts was found before clear AI-use rules were in place. AI-06 is now restricted: no customer, staff or supplier personal data may be submitted through those accounts, and permitted work must move to an approved tool. The user population, prompt history and exposure assessment have not been supplied.

Why it matters. Without a known user population and agreed working route, Quillmarrow cannot tell whether the restriction is understood or whether work has moved to a tool the business has approved. It would also be wrong to conclude, without evidence, either that personal data was entered or that no exposure occurred.

Recommendation. The COO should approve and communicate A4, identify users through a proportionate staff enquiry, assess any reported incidents through the DPO-led route and arrange an approved alternative. Do not ask staff to provide unnecessary prompt contents. Record completion and remaining exceptions.

Owner	Priority
COO, supported by IT Manager and Head of Operations as DPO	High

F2. The reorder agent's approval gate is not demonstrated

What we found. AI-03 is a Tier 3 High pilot. Its pilot default configuration could send purchase orders without approval. V-02 says a gate is available and approval can be linked to the draft, but supplied only a sample screen, not a successful or negative test in Quillmarrow's tenant. A2 and A6 require the Purchasing Lead to approve every purchase order before the agent sends it.

Why it matters. An agent-sent order can create a commercial commitment. A policy instruction or a vendor sample does not prevent an unapproved send. The permissions, supplier list, spend limits, operating hours, kill switch and logs also need tenant-specific evidence.

Recommendation. Keep agent sending disabled until the Purchasing Lead's exact-order approval gate and A7 controls are configured and demonstrated. The MD and Finance Director should approve documented per-order and per-day limits before the pilot. Orders outside the approved supplier list must be blocked. Stop on failed or uncertain checks, and retain a tested pause route.

Owner	Priority
Purchasing Lead, supported by IT Manager; escalation to MD	High

F3. CV screening should remain on hold

What we found. AI-04 is a proposed CV-parsing and candidate-ranking service. The requested use raises a risk of automatic decisions about applicants, but the supplied material does not establish that the proposed configuration would itself make final automatic decisions. V-03 has not supplied a fairness assessment, testing method or results, and important data-processing and permissions evidence is missing.

Why it matters. Screening or ranking can affect who receives further consideration even where a person formally makes the final decision. Missing information prevents a reasoned assessment of the inputs, limitations, potential unfairness and meaningful human involvement.

Recommendation. Maintain the hold and do not proceed with V-03 in its current form. No screening or ranking use should take place while the hold applies. Any reconsideration should begin with a documented proposed workflow, vendor evidence and AIA-03 review; the MD must approve reconsideration and controls before use. The HR Manager should consult the DPO and obtain Singapore-qualified legal advice where needed.

Owner	Priority
HR Manager; decision and escalation to MD	High

F4. Vendor assurance is uneven

What we found. A8 classifies each vendor's response to 30 questions as follows:

Vendor	Evidence provided	Partial	Not provided	Not applicable
V-01 Fictional Helpdesk	24	6	0	0
V-02 Fictional Reorder Agent	3	22	4	1
V-03 Fictional Talent Screen	0	13	15	2

These are questionnaire status counts, not independent assurance scores. "Evidence provided" does not necessarily mean that a control has been tested in Quillmarrow's configuration.

Why it matters. V-01's open points include tenant-specific retention, deletion and location settings, task-specific testing and permissions. V-02's gaps include improvement use, processing locations and subprocessors, independent security assessment, contractual terms, tenant testing, approval and pause behaviour. V-03 has significant gaps in data handling, fairness, processing terms and testing.

Recommendation. Obtain and assess the missing evidence against the actual intended use. Prioritise V-02 controls before any agent sending and V-03 evidence before reconsidering its hold. For V-01, verify the relevant tenant settings and task-specific evidence before relying on them. Record decisions and unresolved risks rather than treating a questionnaire as closure.

Owner	Priority
IT Manager, with DPO and relevant use owners	High

F5. The register needs a durable owner and change route

What we found. The review triggers include staff use without clear rules and the helpdesk vendor switching on AI reply drafting. A2 now provides a single agreed inventory and identifies a use owner for each entry. The evidence does not establish who owned a consolidated register before the review or whether a formal vendor-feature review route existed.

Why it matters. A vendor-enabled feature can enter a workflow before its data, oversight and customer effects have been considered. A one-off register will become stale unless someone maintains it and use owners report changes.

Recommendation. The COO should appoint a register owner, require quarterly review by use owners and establish a route for the IT Manager to flag new or materially changed vendor features. AI-02 should remain subject to a Customer Service user checking and approving every reply before sending. Verify that process and its settings rather than assuming it is in force.

Owner	Priority
COO; register owner to be appointed	High

5. Other observations

- **AI-07 and AI-10:** the register identifies complete evidence for image-review arrangements and invoice-extraction controls respectively. Preserve and periodically refresh those records; this review did not independently test them.

- **AI-11:** reminders remain restricted pending the consent check. The Head of Marketing must approve the check, audience rules and sending configuration before reminders are sent; the DPO should be consulted.
- **AI-12:** the web-chat bot is not yet live. Any customer-facing pilot needs MD approval and controls, with Customer Service reviewing pilot responses before use.
- **AI-13 and AI-15:** the tool or vendor and supporting settings or review evidence are missing. Confirm them before relying on the stated oversight.
- **AI-16 and AI-17:** Finance staff make each credit decision; automatic credit-limit changes are not permitted. Staff must review fraud flags before adverse action on an order.
- **Shared-folder near-miss:** the brief link-sharing event is a prompt to examine access and escalation arrangements. Its cause, extent and whether any notification duty arose are not established here.

6. Decisions needed

Decision	Options	Recommendation	Decision owner	By when
AI-03 pilot	Stop; continue only after controls; or permit sending on current evidence	Continue only after the gate, limits and A7 controls are demonstrated; otherwise keep sending disabled.	MD	Before agent sending
AI-04 proposal	Maintain hold; seek evidence for reconsideration; or proceed now	Maintain hold; do not proceed in current form. Any reconsideration requires documented evidence and MD approval.	MD	Before any screening or ranking
Staff policy and approved tool	Approve A4 and transition; revise A4; or defer	Approve A4 subject to management review, communicate restrictions and move permitted work to an approved tool.	COO	Day 30
Register governance	Appoint an owner and quarterly cycle; or leave maintenance informal	Appoint an owner and require use-owner and vendor-change updates.	COO	Day 30
AI-12 customer-facing pilot	Approve a controlled pilot design after evidence; keep not live; or launch now	Keep not live until the MD approves the design and controls; require Customer Service review of pilot responses.	MD	Before customer-facing pilot

7. 30/60/90-day action plan

The day markers are proposed intervals from management acceptance of this report. They are planning targets, not evidence that actions have been completed. A use-specific gate remains binding even if a target date is missed.

ID	Action	Owner role	Due	Closure evidence
A01	Review and approve A4, including the personal-account restriction and escalation route.	COO	Day 30	Approved policy and recorded management decision.
A02	Communicate the policy to relevant staff and obtain acknowledgement.	COO	Day 30	Issued communication and acknowledgement record, with exceptions tracked.
A03	Identify personal ChatGPT account users and direct permitted work to an approved tool; assess reported exposure without collecting unnecessary prompt content.	IT Manager	Day 30	User-transition record, outstanding exceptions and any incident referrals.

ID	Action	Owner role	Due	Closure evidence
A04	Appoint the A2 register owner and establish a quarterly review with use owners.	COO	Day 30	Appointment record, review schedule and first assigned owner list.
A05	Keep AI-03 sending disabled until pilot controls are proven; confirm the current configuration with the managed service provider.	IT Manager	Day 30	Configuration record and confirmation that sending is disabled, or a dated exception escalated to the MD.
A06	Document and obtain MD and Finance Director approval of AI-03 per-order and per-day limits, supplier list and pilot hours.	Purchasing Lead	Day 30	Approved pilot-bounds record and supplier-recipient list.
A07	Configure the AI-03 Purchasing Lead approval gate, permissions, stop conditions, kill switch and logs in line with A7.	IT Manager	Day 60	Tenant configuration record linked to A7 and approved bounds.
A08	Test AI-03 successful approval, rejected and changed orders, unapproved suppliers, limit breaches, pause and queued-order behaviour.	IT Manager	Day 60	Dated test scripts, results, defects and closure decisions using made-up data.
A09	Maintain AI-04 on hold and document what evidence and approvals would be needed for any reconsideration.	HR Manager	Day 30	Hold confirmation and evidence-request list linked to AIA-03.
A10	Follow up V-01 tenant retention, deletion, location, task-specific testing and permissions.	IT Manager	Day 60	Vendor responses and Quillmarrow tenant evidence, with unresolved gaps recorded.
A11	Follow up V-02 on improvement use, locations, subprocessors, security assessment, processing terms, approval and pause evidence.	IT Manager	Day 60	Evidence tracker with documents, assessment and outstanding items.
A12	Request V-03 data handling, processing terms, permissions, testing and fairness evidence; do not treat the request as permission to use the service.	HR Manager	Day 60	Vendor response and gap assessment linked to the continued hold.
A13	Consult the DPO on AI-11 consent and audience rules; obtain legal input where appropriate before the Head of Marketing decides.	Head of Marketing	Day 60	DPO consultation, any legal advice record and approved or rejected consent, audience and sending configuration.
A14	Define AI-12 pilot design, permissions, Customer Service review, escalation and test evidence for MD decision before customer-facing use.	Head of Customer Service	Day 60	Pilot design, test results and dated MD decision; or record that the bot remains not live.
A15	Confirm AI-13 assistant, vendor and repository access, and AI-15 translation tool and data handling.	IT Manager	Day 60	Tool inventory entries, settings evidence and use-owner review records.
A16	Establish an AI incident route covering reporting, containment, DPO escalation and decisions on external notification; test the route with a scenario.	Head of Operations, as DPO	Day 60	Incident procedure, scenario-test record, assigned improvements and owners.
A17	Train use owners and relevant staff on approval, data restrictions, suspicious content and incident escalation.	COO	Day 90	Training material, attendance or completion record and follow-up for absences.
A18	Verify that AI-02 replies require Customer Service review and that vendor-enabled AI changes enter the review route.	Head of Customer Service	Day 90	Workflow evidence, sample review records using appropriate data and change-notification procedure.
A19	Carry out the first quarterly register review, including evidence status, owner confirmation and changes to uses.	Appointed register owner	Day 90	Dated review record, updated A2 and assigned outstanding actions.

ID	Action	Owner role	Due	Closure evidence
A20	Review overdue actions and residual risks with the COO and MD; decide whether any pilot remains paused.	COO	Day 90	Management review record, decisions, owners and revised target dates.

For A08, a failed test does not close the action. The defect must be corrected and retested, or sending must remain disabled. The same principle applies to other actions where the closure evidence reveals an unresolved control gap.

8. Mapping to AI Verify principles

This table maps the supplied information to the **AI Verify testing framework (AI Verify Foundation)** principles and process checks only. **No AI Verify technical tests were run.** "What Quillmarrow has now" distinguishes a documented requirement or supplied record from evidence that a control operates.

Principle	What Quillmarrow has now	Gap	Related actions
Transparency	A2 identifies uses and owners; AI-12 is stated as not live.	Customer-facing pilot design and communication are not supplied.	A04, A14, A19
Explainability	Human checks are assigned for relevant outputs and decisions.	The information available to reviewers, including sources and limitations, is not consistently evidenced.	A08, A14, A18
Repeatability/ reproducibility	A2 and A6 describe intended workflows; V-02 supplied an internal checklist.	Tenant test scripts, results and change records are missing for AI-03.	A07, A08, A19
Safety	AI-04 is on hold; AI-03 requires human approval; AI-16 automatic decisions are not permitted.	Operating safeguards and failure handling need evidence for the affected uses.	A05, A08, A09
Security	A near-miss has been identified; vendor security responses are recorded in A8.	Tenant permissions and V-02 independent assessment evidence are incomplete.	A07, A10, A11, A16
Robustness	Some uses have documented oversight; AI-14 has an accuracy check and override log.	Failure and exception testing is not supplied for the agent or web-chat pilot.	A08, A14
Fairness	AI-04 is on hold pending reconsideration.	V-03 supplied no fairness assessment, method or results.	A09, A12
Data governance	AI-06 restricts personal-data input; DPO responsibility is assigned.	Actual use, vendor data flows, retention and tenant settings are not fully known.	A03, A10, A11, A12, A13
Accountability	A2 and A6 assign use owners and approvers; the MD approves High-tier uses.	A durable register owner and evidence of ongoing reviews are needed.	A04, A19, A20
Human agency and oversight	A6 specifies human-in-the-loop or human-over-the-loop arrangements for each use.	AI-03's gate and several other workflows have not been demonstrated in the relevant configuration.	A07, A08, A14, A18
Inclusive growth, societal and environmental well-being	The tiering method considers potential harm to people.	No broader impact assessment or supporting evidence is supplied for this principle.	A09, A12, A19

9. Mapping to other references

These mappings identify relevant management processes; they do not establish compliance or legal conclusions.

Reference and area	Application to findings and actions
Model AI Governance Framework, Second Edition (PDPC and IMDA, January 2020): internal governance structures and measures	F1 and F5; approve policy, assign register ownership and review actions through A01–A04 and A19–A20.
Same framework: determining the level of human involvement in AI-augmented decision-making	F2 and F3; retain the Purchasing Lead gate and AI-04 hold through A05–A09.
Same framework: operations management	F2 and F4; configure, test and monitor the agent and obtain vendor evidence through A07–A12.
Same framework: stakeholder interaction and communication	AI-11 and AI-12; address consent, pilot design and customer-facing oversight through A13–A14.
Model AI Governance Framework for Generative AI (IMDA and AI Verify Foundation, May 2024): accountability; data; trusted development and deployment; incident reporting; testing and assurance; security	F1, F2 and F4; relevant actions include A01–A03, A07–A12 and A16–A18. The other dimensions are not assessed in detail in this report.
Model AI Governance Framework for Agentic AI (IMDA, January 2026): assess and bound the risks upfront	F2; approve AI-03 limits, suppliers and hours through A06.
Same framework: make humans meaningfully accountable	F2; retain Purchasing Lead approval and MD oversight through A05–A08.
Same framework: implement technical controls and processes	F2 and F4; configure and test A7 controls and pursue V-02 evidence through A07–A08 and A11.
Same framework: enable end-user responsibility	F1 and F2; communicate restrictions and train staff through A02–A03 and A17.
PDPC Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems (March 2024)	F3 and F4; document intended processing, consult the DPO and seek qualified legal advice where needed through A09–A13.

10. Limitations of this review

- Findings are illustrative and based on the supplied case facts, register, oversight matrix and questionnaire summaries. They are not real client outcomes.
- The engagement uses remote interviews, document review and described workflows with made-up or de-identified samples. No client personal data was put into AI tools.
- No technical testing, tenant inspection, live control verification or independent vendor assessment was performed as part of this report.
- Evidence labelled complete in A2 is reported as supplied in the register; this report does not independently verify its operation.
- Vendor questionnaire counts describe the status of responses, not the effectiveness of a vendor’s controls. Sample screens and logs do not prove tenant-specific behaviour.
- The review does not establish what was entered into personal ChatGPT accounts, whether personal data was exposed, or the legal consequences of the shared-folder near-miss.
- No legal advice or legal conclusions are provided. Where legal obligations, consent, transfers or incident notification need assessment, Quillmarrow should consult a Singapore-qualified lawyer. The Head of Operations remains Quillmarrow’s appointed DPO; the reviewer supports but does not replace that role.

- The framework mappings are governance and process mappings. No AI Verify technical tests were run. A10 is an ISO/IEC 42001 readiness excerpt, not certification.
- Recommendations, target dates and RAG ratings require management decision and should be revisited when missing evidence becomes available.

11. Sign-off

I personally review and sign off every deliverable.

Capacity	Role	Signature	Date
Prepared and signed off by	The reviewer		
Accepted by	COO		
Approved by	MD		

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).