AI GOVERNANCE REVIEW PACK · A1

Engagement scope sheet

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	A1 · Engagement scope sheet
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

1. Purpose of the review

Quillmarrow has asked for a practical review of how it uses, oversees and plans to use AI across its office-supplies business. The review covers the Singapore operation and the identified Malaysia delivery-partner workflow. It is designed to give management a clear record of uses, decisions, conditions and evidence gaps, rather than a declaration that every system is safe or compliant.

The review responds to staff use of ChatGPT and Microsoft 365 Copilot without clear rules; the helpdesk vendor enabling AI reply drafting; the supplier reorder agent pilot; and a proposed CV-screening vendor. It also responds to an enterprise customer's supplier AI questionnaire, the near-miss involving a link-shared customer-records folder, and the appointment of a new DPO.

2. Objectives

The review supports six management decisions:

- **What is in use:** establish an inventory of the 20 identified uses, their owners, purposes, information categories and current status.
- **What needs closer review:** apply Quillmarrow's working risk tiers and assess the uses selected for full impact assessment.
- **What staff may do:** set practical conditions for approved, restricted, pilot and on-hold uses.
- **Where people must remain in control:** define approvals, monitoring and intervention for outputs and agent actions.
- **What to ask vendors:** identify material gaps in vendor, model, data-handling and agent-control evidence.
- **What management should do next:** provide a prioritised action plan, owners and decisions for the COO and MD.

3. In-scope AI uses

The tiers are working categories for Quillmarrow, not statutory classifications. Register entries record the use and its evidence status; they do not establish that controls have been implemented or tested.

ID	Use	Owner role	Depth of review
AI-01	Catalogue product description drafting	Head of Marketing	Register and controls
AI-02	Helpdesk reply drafting	Head of Customer Service	Full impact assessment
AI-03	Supplier reorder agent pilot	Purchasing Lead	Full impact assessment
AI-04	CV screening and candidate ranking	HR Manager	Full impact assessment
AI-05	Microsoft 365 Copilot for email, documents and spreadsheets	IT Manager	Register and controls
AI-06	ChatGPT on staff personal accounts	COO	Register and controls
AI-07	Marketing banner image generation	Head of Marketing	Register and controls
AI-08	Meeting transcription and summaries	IT Manager	Register and controls
AI-09	Sales quotation drafting assistant	Sales Manager	Register and controls
AI-10	Supplier invoice data extraction	Finance Director	Register and controls
AI-11	Reorder reminder emails to web-shop customers	Head of Marketing	Register and controls
AI-12	Customer web-chat bot on the online store	Head of Customer Service	Register and controls plus oversight design
AI-13	Code assistant used by the outsourced web developer	IT Manager	Register and controls
AI-14	Demand forecasting in the inventory system	Purchasing Lead	Register only
AI-15	Translation of supplier correspondence	Purchasing Lead	Register and controls
AI-16	Credit-limit recommendation for B2B accounts	Finance Director	Register and controls plus oversight design
AI-17	Fraud flagging on web-shop orders	Finance Director	Register and controls
AI-18	Delivery route suggestions	Head of Operations	Register only
AI-19	Internal HR policy Q&A assistant	HR Manager	Register and controls
AI-20	Social media reply drafting	Head of Marketing	Register and controls

The full impact assessments are AIA-01 for AI-02, AIA-02 for AI-03 and AIA-03 for AI-04. AI-12 and AI-16 receive oversight design but not full impact assessments in this engagement. AI-03 remains a pilot with an approval gate; AI-04 remains on hold, with a recommendation not to proceed in its current form.

4. Out of scope for this engagement

This engagement does not include an organisation-wide ISO/IEC 42001 readiness review beyond the optional excerpt identified below. It does not include negotiating vendor contracts, undertaking a full procurement exercise, auditing the Malaysia fulfilment partner or investigating the shared-folder near-miss as a separate incident engagement.

The review can identify questions and evidence gaps for Quillmarrow to pursue. It does not independently verify vendor statements or replace the organisation's operational, data-protection or legal decisions.

5. Deliverables

ID	Deliverable	Format	Purpose
A0	Pack cover and decisions	PDF, DOCX	Orient management to the pack, the decisions it supports and its limits.
A1	Engagement scope sheet	PDF, DOCX	Record the agreed review boundary, responsibilities and acceptance process.
A2	AI use register	XLSX, PDF	Record the 20 uses, owners, tiers, statuses and evidence gaps.
A3	Practical risk tiering method	PDF, DOCX	Explain the working tiers and the factors used to distinguish the uses.
A4	AI-use policy	PDF, DOCX	Set out practical rules and escalation expectations for staff.
A5	AI impact assessments AIA-01 to AIA-03	PDF, DOCX	Assess AI-02, AI-03 and AI-04, including decisions and missing evidence.
A6	Human oversight decision matrix	XLSX, PDF	Record required approvals, monitoring, intervention and evidence for each use.
A7	Agent governance checklist: permissions and audit-trail specification	PDF, DOCX	Specify boundaries, approval gates, stop conditions and records for agent actions.
A8	Vendor and model due diligence	XLSX, PDF	Provide vendor questions, responses, evidence status and follow-up points.
A9	Management report and action plan	PDF, DOCX	Present findings, decisions, owners and priorities for management approval.
A10	Optional ISO/IEC 42001 readiness check (excerpt)	PDF, DOCX	Illustrate selected readiness considerations if expressly included in the quote.

A10 is a readiness excerpt only. It is not certification or an organisation-wide readiness assessment.

6. What I need from you

Quillmarrow should provide a list of known AI tools, vendor AI features and agent workflows, including informal staff use and proposed uses. For each, the relevant owner should describe its purpose, users, information categories, permissions, outputs and the decisions or actions it supports.

Please provide existing policies, relevant vendor terms, settings and documentation through the agreed sharing arrangement. The relevant teams should explain how workflows operate in practice, identify uncertainty and approve decisions within their authority. The IT Manager should coordinate with the managed service provider where configuration information is needed.

Fieldwork uses descriptions and made-up or de-identified samples only. Do not provide the customer database. No client personal data is put into AI tools as part of this review.

7. Timeline

The engagement is planned as a fully remote review over about two weeks.

Phase	Activity
Days 1–2	Kick-off, confirm scope and owners, and assemble the AI inventory.

Phase	Activity
Days 3–6	Role-holder interviews, workflow walk-throughs and vendor questions.
Days 7–9	Prepare impact assessments, oversight design and draft deliverables.
Day 10	Quillmarrow review round and consolidated comments.
Days 11–12	Revisions and management read-out.

Review rounds are **a set number agreed in the quote**. Timing depends on access to role holders, the completeness of the inventory and documents, vendor response times, the complexity of agent permissions, and prompt consolidated feedback. Missing evidence will be recorded as missing rather than assumed.

8. Roles and responsibilities

Role	Responsibility
COO	Sponsors the AI programme, owns this review and coordinates management decisions.
Head of Operations and DPO	Advises Quillmarrow on its data-protection processes and coordinates relevant follow-up.
Use owners	Describe actual workflows, identify evidence gaps and review their entries and proposed controls.
IT Manager	Coordinates technical information and the outsourced managed service provider; confirms settings where available.
MD	Approves High-tier uses and signs the management report.
Reviewer	Conducts the review, prepares the deliverables and records findings, proposed actions and limitations.

Quillmarrow appoints its own DPO. The reviewer supports them.

9. Acceptance

Each deliverable is reviewed by the relevant owner role: use owners review their register entries and assessments; the IT Manager reviews technical descriptions; the Head of Operations and DPO reviews data-protection matters; and the COO reviews the overall pack. The reviewer will ask Quillmarrow to provide comments in one consolidated response for each agreed review round.

Acceptance means that the relevant owner has reviewed the deliverable, material comments have been addressed or recorded, and any remaining evidence gaps or decisions are visible. The MD signs the management report. Acceptance does not turn missing evidence into verified evidence.

I personally review and sign off every deliverable.

10. What affects the fixed price

The scope is affected by the number and complexity of AI uses, agent permissions, available vendor evidence, existing documentation, the number of impact assessments and the review process. Any extra work is quoted before it starts.

11. 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.

Where a legal point arises, Quillmarrow should confirm it with a Singapore-qualified lawyer.

12. Assumptions and dependencies

- Quillmarrow identifies the relevant owners and makes them available for remote interviews and reviews.
- The inventory reflects the uses disclosed during fieldwork; undisclosed tools or workflows may require a scope change.
- Vendor statements, settings and controls are assessed only to the extent evidence is made available; no technical tests are run.
- Quillmarrow decides whether to approve, restrict, pause or stop a use and remains responsible for implementation.
- The optional readiness excerpt is prepared only if expressly included in the quote; any additional work is agreed before it starts.

13. Reference frameworks

The review maps Quillmarrow's practices to these references. Mapping is to principles, dimensions and process checks; it is not a compliance opinion.

- Model AI Governance Framework, Second Edition (PDPC and IMDA, January 2020), including its approach to human-in-the-loop, human-over-the-loop and human-out-of-the-loop.
- Model AI Governance Framework for Generative AI (IMDA and AI Verify Foundation, May 2024), for staff use of generative tools such as AI-02, AI-05 and AI-06.
- Model AI Governance Framework for Agentic AI (IMDA, January 2026), a voluntary framework, for the supplier reorder agent (AI-03).
- PDPC Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems (March 2024), for uses such as AI-04 and AI-16.
- AI Verify testing framework, 11 principles, mapped at principle and process-check level only. No technical tests are run.
- ISO/IEC 42001:2023, for the optional readiness excerpt only.

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).