AI GOVERNANCE REVIEW PACK · A5-2

AI impact assessment AIA-02: Supplier reorder agent pilot

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	A5-2 · AI impact assessment AIA-02: Supplier reorder agent pilot
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

1. Summary

Item	Assessment
AI use	AI-03: Supplier reorder agent pilot
Owner	Purchasing Lead
Tool	Fictional Reorder Agent, supplied by V-02
Tier	Tier 3 High, a working business category rather than a statutory classification
Oversight	Human-in-the-loop: the agent sends nothing until the Purchasing Lead approves each purchase order
Recommendation	Continue the pilot only behind a demonstrated approval gate and with bounded permissions. No autonomous sending.
Decision needed	Managing Director (MD) to decide whether the High-tier pilot may continue under the proposed conditions. No MD decision has been supplied.
Evidence status	Partial: V-02 has described the approval gate, bounds and pause and supplied templates (A8 Q27 to Q30), but nothing yet shows them working in Quillmarrow's tenant, and the limits themselves have not been set.

The agent has a write action: it can email purchase orders to suppliers. An incorrect or unauthorised send may create a commercial commitment that is difficult to reverse. The conditions below are therefore safeguards to be demonstrated, not a description of controls already proven to work.

2. Description of the workflow

The proposed pilot covers **eight approved suppliers in Singapore only**. The approved list, supplier contact details and technical enforcement have not been supplied.

The intended workflow is:

1. The agent reads stock levels and sales velocity from the relevant inventory information.

2. It reads the supplier price lists made available for the pilot.
3. It identifies a possible reorder and prepares a draft purchase order containing the supplier, items, quantities and applicable commercial details.
4. The Purchasing Lead reviews the draft against current stock information, supplier terms and the approved pilot limits.
5. The Purchasing Lead approves or rejects the specific draft. If it is changed after approval, it must be submitted for approval again.
6. Only after the required approval may the agent email that purchase order to the approved supplier.
7. The system records the proposed action, decision and send outcome for review.

The agent's claimed ability to send a purchase order does not establish that the approval gate works in Quillmarrow's environment. The technical bounds, approval workflow and tenant test evidence are missing. Until the gate and bounds are demonstrated, no agent-sent purchase order should be released.

3. Data

The proposed inputs are primarily commercial: stock levels, sales velocity, supplier price lists and purchase-order details. Supplier contact persons' names and email addresses are personal data. A draft or log may also contain staff identifiers, approval decisions, timestamps and correspondence.

The exact fields read, retained or transmitted by V-02 have not been confirmed. Quillmarrow also needs the vendor's applicable processing locations, support-access arrangements, retention periods, deletion process and any use of inputs for model or service improvement. A general vendor statement is not a substitute for the settings and terms applicable to this pilot.

The Head of Operations, as DPO, should review the confirmed data flow. Any question about legal obligations or cross-border handling should be confirmed with a Singapore-qualified lawyer.

4. What could go wrong

The ratings below are illustrative business judgements. Residual ratings assume the proposed controls are implemented and working; that has not been established. Existing controls are the stated or required oversight arrangements, not evidence of operation.

ID	Risk	Likelihood	Impact	Existing control	Proposed control	Provisional residual rating	Owner
R1	The agent proposes or sends the wrong quantity.	M	H	Purchasing Lead approval is required.	Show stock, sales velocity, proposed quantity and source timestamps; require a check against current records.	Medium	Purchasing Lead
R2	A duplicate order is sent after a retry or repeated run.	M	H	Approval is required for each order.	Check open orders and use a unique order reference; stop uncertain retries for human review.	Medium	Purchasing Lead

ID	Risk	Likelihood	Impact	Existing control	Proposed control	Provisional residual rating	Owner
R3	An out-of-date price list produces an incorrect order.	M	H	Purchasing Lead reviews the draft.	Show the price-list source and date; stop when the approved source is missing or stale.	Medium	Purchasing Lead
R4	An order is addressed to the wrong supplier or recipient.	M	H	Pilot is limited to approved suppliers.	Enforce the approved supplier and recipient list; display the recipient for approval.	Medium	IT Manager
R5	Instructions embedded in a supplier email or price-list file redirect the agent.	M	H	Technical bounds have not been evidenced.	Treat external content as untrusted data; restrict instructions and test injection scenarios with made-up material.	Medium	IT Manager
R6	Orders exceed the authorised per-order or daily spending limit.	M	H	Each order requires approval; limits are not supplied.	Set and enforce both limits, calculate the running daily total and stop exceptions.	Medium	Finance Director
R7	The agent acts outside approved operating hours or sends while staff cannot respond.	M	M	Operating hours are not supplied.	Configure approved hours and prevent sending outside them; queue drafts for later review.	Low	IT Manager
R8	Logs are missing, incomplete or altered, preventing reconstruction of an order.	M	H	V-02 supplied a sample log; tenant logging is unconfirmed.	Capture and protect the events in A7; test export, access and retention.	Medium	IT Manager
R9	A vendor model or workflow update changes agent behaviour.	M	H	Vendor change notification and tenant controls are not established.	Review material changes, pause affected actions and retest the gate and bounds before resumption.	Medium	IT Manager
R10	A send fails or has an uncertain outcome, and an automatic retry creates an unintended order.	M	H	No verified retry procedure is supplied.	Stop on uncertain delivery; require a person to confirm status before any retry.	Medium	Purchasing Lead

5. Bounding the risks upfront

The following bounds apply to the proposed pilot. Their configuration and operation must be demonstrated before agent sending is permitted.

Boundary	Proposed rule	Evidence or decision needed
Allowed actions	Read the approved stock, sales-velocity and supplier-price sources; prepare purchase-order drafts; send an approved order to an approved supplier.	Source and action permissions, with a test of the permitted workflow.
Not allowed	Send without Purchasing Lead approval; add or change supplier recipients; place orders with suppliers outside the pilot; change price lists, budgets or approval settings; act beyond the approved limits.	Permission matrix and negative tests showing that prohibited actions are blocked.
Per-order limit	Each order must be within a limit approved by the appropriate business authority.	The limit and its enforcement are **not supplied**.
Per-day limit	Aggregate orders must remain within an approved daily limit.	The limit, calculation method and treatment of reversals or uncertain sends are **not supplied**.
Suppliers	Only the eight approved pilot suppliers in Singapore.	Named supplier and recipient list, its owner, approval record and enforcement test are **not supplied**.
Operating hours	Sending is permitted only during approved hours.	Hours, time-zone treatment and out-of-hours handling are **not supplied**.
Data sources	Use only approved, current sources needed for the pilot.	Source inventory, access settings and freshness criteria are **not supplied**.

The Finance Director should help determine appropriate spend limits. The Purchasing Lead should maintain the business-approved supplier list, with the IT Manager implementing and testing the corresponding restrictions. The MD's pilot decision should refer to the agreed bounds rather than leave them implicit.

6. Human accountability

The **Purchasing Lead must approve each purchase order before it is sent**. Approval must relate to the exact draft and recipient to be sent; a material change after approval must invalidate the approval and require a fresh decision.

The Finance Director is the backup for escalation and an additional approver where required. This does **not** replace the Purchasing Lead's mandatory approval under the agreed register. If the Purchasing Lead is unavailable, the order must not be sent under the current rule. Any proposal for the Finance Director to act as a substitute requires an updated register and MD approval before that arrangement is used.

Before approving, the Purchasing Lead should see and check:

- Supplier identity, approved recipient and confirmation that the supplier is within the pilot list.
- Items, quantities, units and delivery details against current stock and business need.
- The price-list source and date, relevant terms and the order total.
- The applicable per-order limit and the remaining daily limit.
- Open or recently sent orders that could make the draft a duplicate.
- The source timestamps, exceptions and any missing or uncertain information.
- The exact purchase order and email to be sent.

The approver must be able to reject or return a draft for correction. Approval is an active decision, not a routine acknowledgement. The decision and any subsequent change must be recorded.

7. Technical controls and processes

The IT Manager should coordinate implementation and testing with the outsourced managed service provider and V-02. The **A7 agent permissions and audit-trail specification** sets out the detailed permissions and records required for this pilot.

Stop conditions

The agent should stop rather than send when:

- Approval is absent, expired, invalidated by a change or cannot be verified.
- A supplier or recipient is outside the approved list.
- A per-order or daily limit would be exceeded or cannot be calculated reliably.
- Required stock, price-list or supplier information is missing, stale or inconsistent.
- A possible duplicate, conflicting instruction or suspected prompt injection is detected.
- The action is outside approved hours, logging is unavailable, or the send outcome is uncertain.

A stop should generate an exception for the Purchasing Lead to review. It must not silently fall back to autonomous sending.

Kill switch and logs

The IT Manager should own the technical kill switch, with the Purchasing Lead able to request an immediate pause. The switch should disable further agent sends and place pending actions in a safe state. Its operation, including what happens to queued orders, must be tested and documented before use.

Logs should support reconstruction of each run: source references and timestamps; draft and version; supplier and recipient; checks and exceptions; approver and decision; changes after approval; send attempt and outcome; and pauses or overrides. Access, retention and export arrangements must be defined. Sample logs supplied by V-02 do not establish that Quillmarrow's pilot records these events.

After a material model, workflow, permission or supplier-list change, the IT Manager and Purchasing Lead should assess whether to pause and retest. No technical test is reported as having been run in this assessment.

8. End-user responsibility

Purchasing staff should receive practical training before participating. It should cover the pilot boundaries, source and quantity checks, duplicate detection, handling of stale information, rejection and escalation, suspected prompt injection, and how to request a pause. The Purchasing Lead remains responsible for each approval.

The pilot suppliers should receive a clear notice, agreed by Quillmarrow, explaining that purchase-order drafts may be prepared with agent assistance and that an authorised human approves orders before sending. The notice should identify a business contact for questionable or duplicate orders. Supplier notice wording and the method of delivery have not been supplied.

9. Vendor evidence status

The earlier fictional V-02 questionnaire records vendor statements and general samples. These do not prove controls in Quillmarrow's tenant.

Topic	Recorded vendor response or material	Gap for the pilot
Workflow and permissions	V-02 supplied a workflow description and permission template.	Quillmarrow-specific source, action and recipient permissions are missing.

Topic	Recorded vendor response or material	Gap for the pilot
Approval gate	V-02 says a gate exists and supplied a sample approval screen.	No successful or negative test in Quillmarrow's tenant; exact-draft binding and change invalidation are unproven.
Logs	V-02 supplied a sample audit-log export with event identifiers and timestamps.	Tenant log coverage, protection, retention and export are unconfirmed.
Pause	V-02 supplied an operational runbook and says queued orders remain drafts.	No tenant test of the kill switch or queued-order behaviour.
Testing	V-02 supplied a short internal checklist.	Results for the pilot, negative tests, prompt-injection tests and remediation records are missing.
Contract and data	V-02 supplied a draft DPA with unresolved terms and partial information about locations and data use.	Applicable signed terms, complete data flow, subprocessors, locations, retention and training or improvement use remain unconfirmed.
Change management	V-02 says it will notify customers of material changes.	A contractual notice period and an agreed retesting process have not been supplied.

10. Framework mapping

This is a governance mapping, not a finding of compliance. AI Verify is mapped to principles and process checks only; **no technical tests were run**.

Framework	Area, dimension or principle	Pilot application
Model AI Governance Framework for Agentic AI (IMDA, January 2026)	Assess and bound the risks upfront	Define suppliers, actions, spend limits, sources and hours before sending is enabled.
Model AI Governance Framework for Agentic AI (IMDA, January 2026)	Make humans meaningfully accountable	Assign the Purchasing Lead's approval, escalation and MD decision.
Model AI Governance Framework for Agentic AI (IMDA, January 2026)	Implement technical controls and processes	Enforce the gate, stop conditions, kill switch and audit trail; test their operation.
Model AI Governance Framework for Agentic AI (IMDA, January 2026)	Enable end-user responsibility	Train staff and give pilot suppliers a route to raise questionable orders.
Model AI Governance Framework, Second Edition (PDPC and IMDA, January 2020)	Internal governance; human involvement; operations management; stakeholder interaction and communication	Set ownership, human-in-the-loop approval, operating controls and supplier communication.
AI Verify testing framework (AI Verify Foundation)	Transparency; explainability; safety; security; robustness; data governance; accountability; human agency and oversight	Document the proposed action and sources, restrictions, approval, exceptions and review as process checks.

11. Pilot exit criteria

Before any wider rollout is considered, Quillmarrow should have:

1. A documented pilot scope, MD decision, approved supplier list, hours and per-order and daily limits.
2. Tenant-specific evidence that the Purchasing Lead must approve the exact order before every send, including a test that a changed order requires fresh approval.

3. Successful tests of prohibited actions, duplicate detection, stale data, limit breaches, unapproved recipients, prompt injection and uncertain sends.
4. A tested kill switch and documented safe handling of queued orders.
5. Complete, accessible logs and evidence that an order can be reconstructed from source to outcome.
6. Resolved or explicitly accepted vendor, contract, data-handling and security gaps, with DPO and legal review where appropriate.
7. Training records, an agreed supplier notice, and a documented review of pilot exceptions and corrective actions.
8. A fresh risk assessment and MD decision covering any proposed wider scope.

These are conditions for consideration, not achieved results. Wider rollout must not be inferred from completion of the pilot alone.

12. Unresolved decisions

Decision or missing evidence	Owner	Date
Whether the High-tier pilot may continue under the stated conditions.	MD	Open
Per-order and daily limits, including treatment of uncertain sends.	Finance Director	Open
Identity and approved recipients of the eight Singapore pilot suppliers.	Purchasing Lead	Open
Operating hours, source freshness rules and exception handling.	Purchasing Lead and IT Manager	Open
Tenant implementation and test of approval, bounds, logging and kill switch.	IT Manager	Open
Applicable vendor contract, processing locations, retention and data-use terms.	Head of Operations, as DPO, and IT Manager	Open
Whether any change to the mandatory Purchasing Lead approval is proposed.	MD	Open

13. Sign-off

Capacity	Role	Signature	Date
Prepared by	The reviewer		
Reviewed by	Purchasing Lead		
Finance comment	Finance Director		
DPO comment	Head of Operations, as DPO		
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).