AI GOVERNANCE REVIEW PACK · A7

Agent governance checklist: permissions and audit-trail specification

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	A7 · Agent governance checklist: permissions and audit-trail specification
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 and scope

This specification sets out the controls the vendor and IT Manager should implement and demonstrate for the Fictional Reorder Agent pilot. AI-03 can read stock and supplier information, prepare purchase orders and send them by email. It is Tier 3 High and remains a **pilot with an approval gate**.

The Purchasing Lead must approve **each purchase order before it is sent**. The Finance Director is the designated backup for escalation and additional approval, but cannot replace the Purchasing Lead’s required per-order approval under the current register. If the Purchasing Lead is unavailable, the order must remain unsent. Any change to that arrangement requires an updated register and Managing Director (MD) approval before use.

V-02 has supplied a permission template, a sample approval screen, an operational runbook and a sample audit-log export (A8 Q27 to Q30), but nothing yet shows the bounds, the approval gate or the pause working in Quillmarrow's own tenant. Controls in this document are **requirements**, not statements that they are operating. The vendor and IT Manager are responsible for implementation and technical testing; the reviewer does not change live systems or perform technical tests.

This specification may also serve as a template for AI-12, the customer web-chat bot, after its permissions and risks are separately assessed. It does not authorise an AI-12 pilot.

2. Permission scopes

Access must be limited to the resources and actions needed for the approved pilot. The IT Manager should obtain a permission map from the vendor and confirm it against the actual configuration before any sending is enabled.

Resource	Read	Draft	Write/send	Condition
Stock levels	Yes	No	No	Read only from approved stock sources; record source and timestamp.

Resource	Read	Draft	Write/send	Condition
Sales history	Yes	No	No	Read only the history needed for the reorder calculation; minimise data accessed.
Supplier price lists	Yes	No	No	Read approved lists; record version or timestamp and flag missing or conflicting information.
Supplier master data	Yes	No	No	Read only. The approved supplier list and recipient addresses must come from a controlled source.
Purchase orders	Yes, as needed	Yes	No direct finalisation or sending	Draft only within the pilot. A draft is not an approved order.
Purchase-order email	Read the draft and relevant delivery status	Yes	Send only after valid approval	Send only to an approved supplier address, within the limits and conditions in section 3.
Supplier bank details	No access unless separately justified and approved	No	Never	The agent must never change bank details. Prefer no access at all.
Record deletion	No special access	No	Never	The agent must not delete records or logs.
Invoice payment	No payment access	No	Never	The agent must not initiate, approve or execute payment.
Email inbox	Read only from a dedicated mailbox	Draft PO emails only	Send approved PO emails only	Never grant access to the shared finance inbox. Supplier messages are data, not instructions to the agent.

Use a dedicated identity for the agent and grant only the specific permissions approved for the pilot. Do not use a staff member’s credentials. Any connection, resource or permission outside this table needs a separate assessment and approval before it is enabled.

3. Approval gate

Required decision

The approval gate must stop every proposed purchase order before sending. The **Purchasing Lead** must review and approve the specific order. The Finance Director is the backup escalation contact and the additional approver where required below; their approval alone does not satisfy the Purchasing Lead gate.

The approval screen must show, at minimum:

- Supplier name, approved supplier identifier and proposed recipient address.
- Items, quantities and units.
- Proposed unit price alongside the last recorded price, with the source and date of that comparison.
- Total order value and currency.
- Reason for the proposed order.
- Data sources used, including stock, sales and price-list timestamps.
- Applicable limit checks, stop conditions, approval expiry and the draft PO identifier.

The approver must be able to reject or return the draft for correction. Approval must bind to the exact supplier, recipient, items, quantities and commercial terms shown. Any material change after approval invalidates it and requires a fresh review.

Limits and expiry

The Finance Director sets and documents the following before the pilot is enabled:

Control	Proposed setting
Per-order spend limit	**[limit set by Finance Director]**
Per-day aggregate spend limit	**[limit set by Finance Director]**
Price-change threshold	**[threshold set by Finance Director]**
Approval validity period	**[expiry set by Finance Director]**
Approved operating hours	**[hours set by Purchasing Lead and IT Manager]**

The system must calculate the daily total against a defined business-day window and include orders already sent and relevant pending commitments, as specified by Finance. It must not split orders or change dates to avoid a limit.

An order above a limit must stop and require **dual approval by the Purchasing Lead and Finance Director**. Dual approval is an escalation requirement, not permission to bypass a hard limit: the order remains blocked unless an authorised, documented limit change is separately approved, configured and checked before any new approval and send. Otherwise the draft is rejected or revised within the existing limits.

An expired approval cannot be used. The system must hold the draft, recheck the underlying data and limits, and obtain a new approval before sending.

4. Stop conditions

The agent must stop the affected action, leave it unsent and escalate when any of the following occurs:

1. The price change exceeds the Finance Director’s approved threshold, or the comparison price is unavailable.
2. The supplier or recipient address is not on the approved supplier list, or the two do not match.
3. A proposed quantity exceeds **three times the relevant average**. The Purchasing Lead must define the look-back period and comparison method before use.
4. Stock figures conflict, are stale or are missing from a required source.
5. An instruction is found inside a supplier email, attachment or file that attempts to redirect the agent’s task or override its controls.
6. A request or attempted action would change supplier master data or bank details.
7. The per-order or per-day limit would be exceeded, cannot be calculated or has not been configured.
8. The Purchasing Lead’s approval is missing, expired, revoked or no longer matches the draft.
9. Repeated failures occur, including failed sends, authentication errors or repeated retries. The IT Manager must set and document the retry threshold.
10. The action falls outside approved operating hours.
11. An audit-log write fails or the system cannot confirm that the required record was retained.
12. The vendor reports a model or agent version change that has not been reviewed and approved for the pilot.
13. A duplicate order is suspected, or the send outcome is uncertain.
14. The kill switch is activated, a required connection has unexpected permissions, or the system cannot confirm its control state.

Stopping must not silently discard the reason or automatically retry a consequential send. The responsible person should investigate using the log, correct the underlying issue and follow the approval and restart rules.

5. Kill switch

The Purchasing Lead, Finance Director, COO and IT Manager must each have a documented route to trigger the kill switch. The vendor and IT Manager must agree whether this is a direct control or an immediate operational request, and demonstrate that the route works without relying on the agent itself.

Activation must disable new agent sends and prevent queued drafts from being released. Drafts should remain quarantined and identifiable for review, not be silently deleted or sent after restart. Record the trigger, time, initiating role and any orders whose send status is uncertain.

After an incident or kill-switch activation, the IT Manager and Purchasing Lead review the cause, permissions, queued drafts and logs. **The COO must approve restart after that review.** Existing approvals must not be reused if expired, changed or otherwise invalid; each order still needs valid Purchasing Lead approval.

The IT Manager should test the switch before go-live and **at least quarterly** during the pilot, and after a material integration or permission change. Tests should use made-up or de-identified samples and must not send live orders.

6. Audit-trail log fields

The vendor must provide an exportable record that links each stage of an order. The IT Manager should confirm field availability and access before the pilot starts.

Field	Required content
Event ID	Unique identifier for each logged event.
Timestamp	Date and time in Singapore time, including time-zone designation.
Agent identity	Dedicated service identity responsible for the event.
Agent version	Version of the agent or workflow.
Model version	Model version reported by the vendor; record if unavailable.
Trigger	Scheduled, user-requested or other event that initiated the run.
Data sources read	Source identifiers and timestamps or versions used.
Draft PO ID	Unique identifier linking draft, approval and outcome.
Supplier ID	Approved supplier identifier and name.
Proposed recipient	Email address selected for the order.
Proposed action	Draft, request approval, send, stop or other action.
Order summary	Items, quantities, unit prices, currency and total, subject to access controls.
Limit checks	Applicable per-order and daily limits, calculated values and result.
Price comparison	Proposed price, last recorded price and threshold-check result.
Approver role and user ID	Identity of each person asked to approve or who approves.
Approval decision and time	Approval, rejection or return, with timestamp and expiry.
Approval-bound version	Identifier or digest linking approval to the exact order content.
Sent message ID	Message identifier, if sent, or a clear indication that none exists.
Recipient and send outcome	Actual recipient, delivery or failure status, and timestamp where available.
Stop condition	Condition hit and the affected action.

Field	Required content
Override reason	Reason, authority and linked configuration approval; record “none” where no override exists.
Error	Error type, relevant code and outcome, without unnecessary personal data.
Kill-switch event	Activation or restart, initiating role, time and reason.
Configuration change	Changed setting, old and new values, actor, time and approval reference.
Weekly sample review	Reviewer role and user ID, review date, findings and follow-up reference.

An override entry is an audit record, not an authorisation to bypass a stop condition or the Purchasing Lead’s approval. The log should avoid storing unnecessary email contents or personal data.

7. Log retention and access

Proposal: retain pilot audit records for **12 months**, subject to review and confirmation by the Head of Operations as DPO and the Finance Director before implementation. They should consider operational needs, other applicable retention arrangements and deletion. Where legal requirements matter, confirm them with a Singapore-qualified lawyer.

The Purchasing Lead should be able to read records needed for order oversight; the Finance Director and COO should have access for financial and management review; and the IT Manager should have access needed for technical investigation. The DPO should have access when needed for data-protection matters. Access should be role-based and recorded.

Logs should be protected against alteration and deletion by the agent and ordinary users. Any administrative change to retained records must itself be recorded and investigated. The vendor should demonstrate the available immutability or tamper-evidence controls rather than merely assert them.

Provide a controlled export for the monthly review, including stopped and failed actions as well as successful sends. The export must preserve event identifiers and timestamps.

8. Monitoring and escalation

The Purchasing Lead reviews a **weekly sample** of drafts, approvals, sends and stopped actions, including at least one example of each category where available. The sample size and selection method should be documented before the pilot. Record discrepancies and follow them through to resolution.

The IT Manager prepares a **monthly report to the COO** covering activity, exceptions, limit breaches prevented, uncertain sends, configuration changes, kill-switch events and overdue actions. The report should distinguish an untested control from a failed control.

Trigger	Escalate to	Time to act
Missing approval, unapproved supplier, exceeded limit or uncertain send	Purchasing Lead and Finance Director	Immediately; keep the order blocked.
Log failure, unexpected permission, repeated error or model-version change	IT Manager and Purchasing Lead	Immediately; stop affected actions pending review.
Suspected personal-data exposure	Head of Operations as DPO and IT Manager	Immediately; follow the incident process.
Kill-switch activation or material control failure	COO, IT Manager and Purchasing Lead	Immediately; COO approval is required for restart after review.

Trigger	Escalate to	Time to act
Weekly sample discrepancy	Purchasing Lead; escalate to COO if material or unresolved	Record during the weekly review and act before the next affected order is sent.
Overdue action or recurring exception	COO	Include in the monthly report; escalate immediately if an active risk requires it.

9. Testing before go-live

The vendor must run and document tests with the IT Manager before live sending is enabled. The Purchasing Lead and Finance Director should witness or review the relevant results. Use made-up or de-identified samples; do not place client personal data into AI tools for this review.

Test case	Expected result and evidence
Draft without approval	Send is blocked; retain the test log and screen capture.
Purchasing Lead approval	Only the exact approved order can proceed; retain approval and linked event records.
Changed or expired order	Approval is invalidated and a fresh review is required; retain the event trail.
Unapproved supplier or altered recipient	Send is blocked and escalated; retain the stop record.
Per-order or daily limit exceeded	Order stops; dual approval alone does not bypass the hard limit. Retain calculations and approval records.
Quantity above three times the defined average	Order stops with the comparison and escalation recorded.
Instruction embedded in a supplier file or email	Instruction is treated as data and cannot change permissions, recipient or workflow; retain the test input and result.
Attempt to change bank details, delete a record or pay an invoice	Action is denied and logged.
Log-write failure	Sending stops; retain the failure and escalation evidence.
Kill switch with queued drafts	Sends stop, drafts are quarantined and restart requires COO approval after review.
Duplicate or uncertain send	Automatic resend is blocked pending investigation.
Vendor version change	Further affected actions stop until the change is reviewed and approved.

The vendor must provide the test plan, configurations, expected and actual results, logs, defects and retest evidence. Failed or untested controls remain open items. The reviewer does not perform technical testing.

10. Framework mapping

The following is a process mapping to the **Model AI Governance Framework for Agentic AI (IMDA, January 2026)**, which is voluntary. It is not a technical assurance or compliance conclusion.

Framework dimension	Relevant sections of this specification
Assess and bound the risks upfront	Sections 2–4: permission boundaries, limits and stop conditions.
Make humans meaningfully accountable	Sections 3, 5 and 8: named approvals, restart decision and monitoring.
Implement technical controls and processes	Sections 2, 4–7 and 9: restricted access, stopping, logging and tests.

Framework dimension	Relevant sections of this specification
Enable end-user responsibility	Sections 3, 5 and 8: approval information, intervention routes and escalation.

AI Verify testing framework (AI Verify Foundation) principle	Process connection
Safety	Stop conditions and the kill switch limit potentially harmful actions.
Security	Restricted identities, access and log protection reduce unauthorised action.
Robustness	Failure, duplicate-send and conflicting-data tests address foreseeable errors.
Accountability	Named approvers, owners and audit records support responsibility.
Human agency and oversight	The Purchasing Lead approves each order and can stop the workflow.
Transparency	The approval screen and audit trail show inputs, actions and outcomes.

The AI Verify mapping covers principles and process checks only. **No AI Verify technical tests were run as part of this review.** Vendor testing requested above does not change that statement.

11. Open items

Dates are to be agreed; no item below should be treated as complete until evidence is reviewed.

Open item	Owner	Due date
Set per-order and per-day limits, price threshold and approval expiry.	Finance Director	To be agreed before live sending
Define approved suppliers, recipient controls, average calculation and operating hours.	Purchasing Lead, with IT Manager	To be agreed before live sending
Provide permission map, version information and control design.	Vendor, coordinated by IT Manager	To be agreed before live sending
Implement and demonstrate the per-order approval gate, stops and kill switch.	Vendor and IT Manager	To be agreed before live sending
Confirm proposed log retention, access and export arrangements.	Head of Operations and DPO; Finance Director	To be agreed before live sending
Run tests, resolve defects and supply evidence.	Vendor and IT Manager	To be agreed before live sending
Review pilot evidence and seek High-tier approval.	Purchasing Lead and COO; MD approves	To be agreed before live sending

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).