AI GOVERNANCE REVIEW PACK · A6

Human oversight decision matrix

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	A6 · Human oversight decision matrix
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

The matrix sets out who is responsible for checking, monitoring and intervening in each of Quillmarrow's 20 AI uses. It is an operational guide: it does not by itself prove that an approval happened, that a setting works or that an owner has reviewed an output. Where evidence is missing, the owner must retain the relevant restriction and follow up rather than assume the control is operating.

Approve, monitor and intervene

Approve means a named role examines the information needed to make a decision and can accept, amend or reject it. Approval must happen at the point specified in the matrix. For example, the Purchasing Lead must approve each AI-03 purchase order before the agent sends it. Approval of a High-tier use by the Managing Director (MD) is a separate decision from approval of an individual action.

Monitor means the named owner or operator checks whether the use continues to operate within its agreed purpose and boundaries. Depending on the use, this may involve reviewing individual outputs, exceptions, complaints, action logs or periodic performance records. For AI-14, the Purchasing Lead reviews forecast exceptions and stock decisions rather than approving every forecast.

Intervene means the responsible person can correct an output, reject an action, pause the workflow or escalate the issue. The matrix should identify who can intervene and what they can do. If a person cannot reach the control or does not have authority to stop an action, recording them as the overseer is not enough.

Choosing the level of human involvement

The **Model AI Governance Framework, Second Edition (PDPC and IMDA, January 2020)** describes three arrangements:

- **Human-in-the-loop:** a person reviews and makes the relevant decision before an action or output takes effect.
- **Human-over-the-loop:** a person monitors the system and can intervene, including by reviewing exceptions.
- **Human-out-of-the-loop:** the system makes or carries out the relevant decision without human intervention at that point.

The reviewer chose the arrangement for each use by considering the severity and reversibility of potential harm, alongside the information involved and the system's autonomy. There is no single arrangement for every use. A draft that can be corrected before publication calls for a different check from an agent able to send a purchase order or a recommendation affecting a credit decision.

The loop label describes the intended oversight, not proof that it operates. In particular, an approval gate must be demonstrated before it is relied upon. A hold or prohibition remains in place even if a possible future human-review process has been described.

How to read the matrix

Each row corresponds to an AI use in the register. Read it across to identify the use and its **loop label**, the person who **approves**, who **monitors**, and who can **intervene**. The **reversibility** column explains how readily an error can be corrected; **harm if wrong** describes the potential consequence. The status and conditions in the register still apply.

The listed role is accountable for the specified action, but an authorised user may perform a check where the register permits it. Owners should make clear how checks are recorded and how staff reach the person who can intervene.

Uses requiring the tightest oversight

- **AI-03 — supplier reorder agent.** An incorrectly sent purchase order could create a commitment that is difficult to undo. The Purchasing Lead must approve every order before sending. The agent must also have per-order and per-day limits and block orders outside the approved supplier list. Technical bounds, the approval workflow and test evidence have not been supplied; these controls are requirements, not verified settings.
- **AI-12 — customer web-chat bot.** A customer-facing response could mislead someone or disclose information before an error is corrected. The bot is not yet live and may be piloted only after controls are approved. Customer Service must review pilot responses before any customer-facing use. Pilot design, permissions, escalation and test evidence are missing.

- **AI-16 — credit-limit recommendation.** A credit decision may materially affect a B2B customer and can be difficult to reverse. The Finance Director or authorised finance staff make the decision; automatic decisions and automatic limit changes are not permitted. The vendor, inputs, recommendation logic and decision records have not been supplied.

AI-04 also remains on hold: no candidate screening or ranking may occur until the hold is reconsidered and controls are approved.

Keeping the matrix current

The **COO owns the matrix**. Use owners should tell the COO when the AI use register changes, including a change to purpose, owner, data, permissions, status or required approval. The COO updates the matrix with the register and refers High-tier approval decisions to the MD. An incident, failed control or proposed expansion should also prompt a review.

Evidence that oversight operated

Useful evidence includes a dated output or action record, the approver’s identity and decision, exception and intervention logs, and records of corrections or pauses. For AI-03, an order record should link the specific purchase order to the Purchasing Lead’s approval and the subsequent send outcome. Configuration and test evidence are needed to support claims about technical gates; an approval record alone does not prove those gates work.

The full matrix follows and is also supplied as an XLSX workbook.

Open items before this matrix is relied on

- AI-03 supplier reorder agent: the approval gate and kill switch must be shown working in Quillmarrow's own tenant (see A7) before the pilot widens. Owner: Purchasing Lead with the IT Manager.
- AI-12 web-chat bot: hand-off to a person, the out-of-scope message list and transcript sampling must be set up before any customer-facing pilot. Owner: Head of Customer Service.
- AI-16 credit-limit recommendations: Finance to keep a record of each human credit decision, including when a recommendation was overridden. Owner: Finance Director.
- All Tier 3 uses: first quarterly evidence check to be filed with the register. Owner: COO.

Approval

Role	Action	Date
Reviewer (Alex Lew)	Prepared and signed off	
Chief Operating Officer	Accepted as the working oversight matrix	
Head of Operations (DPO)	Consulted on uses involving personal data	

The matrix, part 1: who approves, monitors and intervenes

ID	Use	Owner role	Tier	Loop	Approve	Monitor	Intervene
AI-01	Catalogue product description drafting	Head of Marketing	Tier 1 Low	Human-in-the-loop	Head of Marketing approves factual claims and final copy before publication.	Head of Marketing reviews each draft; retain the approved copy and review record.	If a claim is unsupported or content is unsuitable, withhold publication and correct the draft; Head of Marketing may pause use.
AI-02	Helpdesk reply drafting	Head of Customer Service	Tier 2 Medium	Human-in-the-loop	A Customer Service user approves each reply before sending.	Head of Customer Service reviews a sample of replies weekly and all complaints; retain review and complaint records.	If a reply is inaccurate, exposes personal data or prompts a complaint, pause the feature, correct the reply and investigate; Head of Customer Service may pause it.
AI-03	Supplier reorder agent pilot	Purchasing Lead	Tier 3 High	Human-in-the-loop	Purchasing Lead approves every purchase order before the agent sends it. Before the pilot, MD and Finance Director approve documented per-order and per-day spend limits; orders outside the approved supplier list are blocked.	Purchasing Lead checks each proposed and sent order and reconciles the pilot log daily; retain approvals, blocks and order records.	On an out-of-limit, unapproved-supplier, duplicate or incorrect order, stop sending, pause the agent and contact the supplier to contain the order; Purchasing Lead may pause it.
AI-04	CV screening and candidate ranking	HR Manager	Tier 3 High	Human-in-the-loop	No screening or ranking use while on hold; MD must approve any reconsideration before use.	HR Manager checks that the hold remains in place during each recruitment cycle; retain the hold check and any proposed-change record.	If CVs are processed or ranked, stop the use, restrict access and assess what data was handled; HR Manager may stop it.
AI-05	Microsoft 365 Copilot for email, documents and spreadsheets	IT Manager	Tier 2 Medium	Human-in-the-loop	The user checks and approves each output and recipient before using or sharing it.	IT Manager reviews access and settings quarterly, confirming details that are client-reported or to be confirmed; retain review records and reported incidents.	If information is exposed or access is inappropriate, stop the affected use, restrict access and investigate; IT Manager may suspend access.
AI-06	ChatGPT on staff personal accounts	COO	Tier 2 Medium	Human-in-the-loop	No personal account use for customer, staff or supplier personal data; permitted work must move to an approved tool.	COO reviews reported use and incidents monthly; retain restriction acknowledgements and incident records.	If personal data or confidential information is entered, stop use, report and assess the exposure; COO may direct staff to stop using the account for work.
AI-07	Marketing banner image generation	Head of Marketing	Tier 1 Low	Human-in-the-loop	Head of Marketing approves each image before publication.	Head of Marketing reviews each image and the image review log monthly; retain prompts, review decisions and approved images.	If an image is misleading, unsuitable or raises a rights concern, withhold or remove it and pause generation pending review; Head of Marketing may intervene.
AI-08	Meeting transcription and summaries	IT Manager	Tier 2 Medium	Human-in-the-loop	Meeting organiser checks the transcript and summary before circulation.	IT Manager reviews settings and retention quarterly; organisers retain checked summaries and note corrections or circulation limits.	If a summary misstates a decision or includes information for the wrong audience, stop circulation, correct or delete it and review access; meeting organiser may intervene.

ID	Use	Owner role	Tier	Loop	Approve	Monitor	Intervene
AI-09	Sales quotation drafting assistant	Sales Manager	Tier 2 Medium	Human-in-the-loop	Sales Manager or authorised salesperson verifies prices and terms before sending each quotation.	Sales Manager samples quotations monthly against approved sources; retain the check and any correction record.	If a price, term or recipient is wrong, stop the quotation, correct it and notify the customer if already sent; Sales Manager may pause use.
AI-10	Supplier invoice data extraction	Finance Director	Tier 2 Medium	Human-in-the-loop	Finance checks extracted fields against the invoice before posting or payment.	Finance Director reviews monthly reconciliation and exceptions; retain reconciliation and correction records.	If extracted details do not match the invoice or a payment is at risk, stop posting or payment and correct the entry; Finance Director may suspend the feature.
AI-11	Reorder reminder emails to web-shop customers	Head of Marketing	Tier 2 Medium	Human-in-the-loop	No reminder is sent until the Head of Marketing approves the consent check, audience rules and sending configuration.	Head of Marketing checks each campaign before release and reviews complaints and suppression records monthly.	If consent or audience rules are unclear, or an unintended message is sent, pause the campaign and investigate; Head of Marketing may stop sending.
AI-12	Customer web-chat bot on the online store	Head of Customer Service	Tier 3 High	Human-in-the-loop	No customer-facing pilot until the MD approves the High-tier use and the pilot controls; Customer Service reviews pilot responses before use.	Head of Customer Service reviews pilot conversations daily and records escalations, errors and complaints.	If the bot gives harmful or materially incorrect advice, exposes data or fails to escalate, switch off the pilot and investigate; Head of Customer Service may switch it off.
AI-13	Code assistant used by the outsourced web developer	IT Manager	Tier 1 Low	Human-in-the-loop	IT Manager confirms the assistant and repository access before use; the outsourced developer's code changes require human review before approval.	IT Manager reviews access quarterly and records code-review exceptions and reported incidents.	If code exposes data, bypasses controls or causes a defect, stop deployment, roll back the change where feasible and suspend assistant access; IT Manager may intervene.
AI-14	Demand forecasting in the inventory system	Purchasing Lead	Tier 2 Medium	Human-over-the-loop	Not required for each forecast: it is advisory; Purchasing Lead approves resulting stock decisions.	Purchasing Lead reviews exceptions during each stock-planning cycle and the quarterly accuracy check; retain overrides and review results.	If forecasts materially diverge from stock or sales evidence, disregard the forecast, use manual planning and ask the system owner to investigate; Purchasing Lead may suspend reliance.
AI-15	Translation of supplier correspondence	Purchasing Lead	Tier 1 Low	Human-in-the-loop	Purchasing user checks material terms before responding or placing an order.	Purchasing Lead reviews translations used for commitments during each purchasing cycle; retain the checked correspondence or correction record.	If a translation changes a price, delivery date or commitment, stop the response or order and obtain a reliable translation; Purchasing Lead may pause use.
AI-16	Credit-limit recommendation for B2B accounts	Finance Director	Tier 3 High	Human-in-the-loop	Finance Director or authorised finance staff make each credit decision; automatic limit changes are not permitted.	Finance Director reviews recommendations and decision records monthly; retain the recommendation, human rationale and any challenge.	If a limit changes automatically or a recommendation appears unsupported, stop reliance, restore human decision-making and review affected accounts; Finance Director may suspend the feature.

ID	Use	Owner role	Tier	Loop	Approve	Monitor	Intervene
AI-17	Fraud flagging on web-shop orders	Finance Director	Tier 2 Medium	Human-in-the-loop	Staff review a flag before taking adverse action on an order.	Finance Director reviews flagged orders, outcomes and disputes monthly; retain review and correction records.	If false flags recur or orders are blocked without review, pause adverse actions and investigate the provider settings; Finance Director may suspend reliance.
AI-18	Delivery route suggestions	Head of Operations	Tier 1 Low	Human-over-the-loop	Not required for each suggestion: partner operations review exceptions and decide route changes.	Head of Operations reviews partner route exceptions and delivery complaints monthly; retain partner review and issue records.	If route suggestions cause repeated delays, expose unnecessary data or create a safety concern, ask the partner to stop relying on them while investigated; Head of Operations may request suspension.
AI-19	Internal HR policy Q&A assistant	HR Manager	Tier 2 Medium	Human-in-the-loop	HR Manager approves pilot access and source material; HR checks answers before they guide decisions or personal cases.	HR Manager reviews pilot questions and answer samples weekly; retain corrections, escalations and access review records.	If the assistant uses unauthorised employee records or gives materially incorrect guidance, pause the pilot, restrict access and correct affected guidance; HR Manager may pause it.
AI-20	Social media reply drafting	Head of Marketing	Tier 1 Low	Human-in-the-loop	Head of Marketing or authorised user checks and approves each reply before posting.	Head of Marketing reviews posted replies and complaints weekly; retain approval and correction records.	If a reply is inaccurate, discloses personal information or attracts a complaint, remove or correct it and pause drafting pending review; Head of Marketing may intervene.

The matrix, part 2: reversibility, escalation, evidence and review

ID	Reversibility	Harm if wrong	Escalate to	Evidence of operation	Review cadence and trigger
AI-01	Easily reversible: drafts can be edited before publication.	Incorrect product specifications could mislead buyers.	COO	Retained draft, source facts, reviewer approval and final published copy.	Annual; also on: tool access changes; personal data proposed for prompts; inaccurate or misleading catalogue copy
AI-02	Reversible with effort: a sent reply can be corrected, but the customer has already received it.	A misleading reply could confuse a customer or disclose their information.	COO	Reply approval history, weekly sample review and complaint or incident log.	Every six months; also on: vendor enables new AI feature; replies can be sent without review; Malaysia orders enter scope; any complaint about a sent reply
AI-03	Hard to reverse: a supplier may act on an emailed order.	Unauthorised or incorrect orders could create financial loss or disrupt stock.	Managing Director (MD)	Configured supplier allow-list and spend limits; pre-send approval, blocked-action and sent-order logs.	Quarterly; also on: pilot scope or supplier list changes; order limits change; any unauthorised, duplicate or incorrect order
AI-04	Reversible with effort: candidate data may be processed and a ranking could affect recruitment decisions.	A flawed ranking could unfairly disadvantage a candidate.	Managing Director (MD)	Recruitment workflow hold record and any access or processing incident record.	Quarterly; also on: hR seeks to lift the hold; vendor or ranking method changes; candidate complaint or suspected unfair outcome
AI-05	Reversible with effort: drafts can be corrected, but shared information may already have been seen.	Inaccurate content or unintended sharing could affect customers, staff or suppliers.	COO	User review records where retained, quarterly access and settings review, and incident log.	Every six months; also on: licence or configuration changes; new data categories used; sharing incident or material output error
AI-06	Hard to reverse: submitted prompts may not be recoverable by Quillmarrow.	Personal or confidential information could be exposed outside approved company controls.	Managing Director (MD)	Staff acknowledgements, reported-use review and incident or exposure records.	Every six months; also on: personal data is found in prompts; approved-tool decision; material change in staff use
AI-07	Easily reversible: an unpublished image can be replaced; a published banner can be removed.	An unsuitable or misleading image could damage customer trust.	COO	Tool settings, approved prompt guide and image review log.	Annual; also on: personal data or third-party likenesses proposed; tool or publication workflow changes; image complaint
AI-08	Reversible with effort: circulated summaries may need correction and recipients may already have read them.	A false record or unintended disclosure could affect staff or business decisions.	COO	Organiser approval or correction record, circulation list and quarterly settings review.	Every six months; also on: new meeting types or external attendees; settings change; sensitive information appears in an unintended summary
AI-09	Reversible with effort: a sent quotation may need withdrawal or correction.	Incorrect prices or terms could mislead a customer or create a commercial dispute.	COO	Approved source reference, quotation review record and correction log.	Every six months; also on: assistant gains sending or pricing authority; new customer data used; quotation error or complaint
AI-10	Reversible with effort: accounting entries can be corrected, but payments may be difficult to recover.	Incorrect supplier or payment details could lead to inaccurate records or misdirected payment.	Managing Director (MD)	Configuration export, posting permissions and monthly reconciliation.	Every six months; also on: feature gains posting or payment authority; extraction errors recur; accounting workflow changes

ID	Reversibility	Harm if wrong	Escalate to	Evidence of operation	Review cadence and trigger
AI-11	Hard to reverse: a sent marketing email cannot be recalled.	Customers could receive unwanted messages or have order information used inappropriately.	COO	Consent and audience approval, campaign release record, suppression list and complaint log.	Every six months; also on: consent check completed; audience or data use changes; any complaint or unintended message
AI-12	Reversible with effort: a response cannot be withdrawn after a customer has read it.	Customers could act on incorrect information or disclose personal data without suitable support.	Managing Director (MD)	Pilot approval, access and escalation settings, reviewed conversation samples and incident log.	Quarterly; also on: before pilot or launch; bot gains access to order records; any harmful answer or customer complaint
AI-13	Reversible with effort: code can be rolled back, but deployed defects may affect the web shop.	An unsafe code change could expose information or disrupt online ordering.	COO	Vendor and access confirmation, code-review record, deployment approval and incident log.	Annual; also on: vendor or repository access identified; code is generated for sensitive workflows; defect or suspected disclosure
AI-14	Reversible with effort: a forecast can be overridden, but resulting stock decisions may already be in motion.	Poor forecasts could contribute to shortages or excess stock.	COO	Forecast method note, override log and quarterly accuracy check.	Every six months; also on: forecasting feature or inputs change; material stock discrepancy; system begins placing orders
AI-15	Reversible with effort: a sent response or order may require clarification or correction.	A mistranslated term could cause a supplier dispute or incorrect order.	COO	Identified tool and settings, checked correspondence and correction record.	Annual; also on: tool identified or changed; personal data is translated; mistranslation affects a commercial commitment
AI-16	Reversible with effort: a limit can be changed back, but customer access or terms may already be affected.	An unsuitable limit could unfairly restrict a business customer or expose Quillmarrow to credit risk.	Managing Director (MD)	Recommendation and decision log showing human rationale and confirmation that no automatic change occurred.	Quarterly; also on: any proposal for automated decisions; vendor or input changes; customer challenge or suspected adverse outcome
AI-17	Reversible with effort: an order can be released, but fulfilment or customer experience may already be affected.	A legitimate customer's order could be delayed or wrongly rejected.	COO	Provider settings review, staff flag decisions, dispute and correction log.	Every six months; also on: feature begins blocking orders automatically; false-flag pattern; provider or data-input change
AI-18	Reversible with effort: a route can be changed, but a delivery may already be delayed.	Poor routing could delay customer orders or expose delivery details unnecessarily.	COO	Partner data-processing terms, confirmed route data fields and retained exception review records.	Annual; also on: partner system changes; data shared expands; route issue or customer complaint
AI-19	Reversible with effort: guidance can be corrected, but staff may already have acted on it.	Incorrect HR guidance could mislead staff about workplace policies or processes.	COO	Pilot approval, source and access check, reviewed answer log and correction record.	Every six months; also on: pilot expands; assistant accesses employee records; incorrect answer affects a staff decision
AI-20	Reversible with effort: a post can be removed, but it may already have been seen or copied.	A public error or disclosure could harm a customer or Quillmarrow's reputation.	COO	Draft-to-post approval record, published reply and correction or complaint log.	Annual; also on: tool gains posting permission; personal data used in prompts; public error or customer complaint

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).