

Specimen — illustrative example

Pemberton Home Goods is a fictional organisation. This document comes from the scenario described on riskwoven.com/examples, and is not an assessment of any real entity. It is advisory output to support your own decisions: not legal advice, not a certification, and not an audit.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

Third-Party AI Review Procedure

Pemberton Home Goods

Document type	procedure	Version	1.0 Draft
Owner	Director of Digital	Customer decision role	Chief Operating Officer
Effective date	Upon customer release	Review cycle	Annual
Framework basis	RiskWoven AI practical best practices		
Jurisdiction	Canada and the United States		
Prepared for	Pemberton Home Goods	Industry	Retail
Organization size	101-500	Locations	Not specified

Advisory draft for accountable-owner and professional review. Validate legal, regulatory, contractual, technical and operational requirements before customer release. This is not legal advice, a certification, or a compliance determination.

1. Purpose

This procedure establishes the steps Pemberton Home Goods follows to evaluate, review and monitor AI-enabled suppliers before and during their engagement. It ensures that third-party AI

services meet the organisation's requirements for security, privacy, transparency and accountability, and that residual risks are understood and accepted at the appropriate level before any supplier processes Pemberton Home Goods data or influences customer-facing decisions.

2. Scope

This procedure applies to any supplier whose product or service incorporates artificial intelligence, machine learning or automated decision-making that will:

- Process Pemberton Home Goods data, including customer, employee or operational information.
- Generate, influence or automate decisions presented to customers or used in business operations.
- Integrate with Pemberton Home Goods systems, including the Shopify Plus storefront, the personalisation platform, order management, the loyalty database or the point-of-sale estate.

It covers new supplier engagements, material changes to existing AI supplier services, and contract renewals where the AI capability has changed since the last review.

3. Definitions

AI provider: A supplier that offers a product or service incorporating artificial intelligence, machine learning or automated decision-making, whether as the primary function or as an embedded capability within a broader service.

Training use: Any use of Pemberton Home Goods data—including prompts, inputs, outputs, feedback or corrections—to train, fine-tune, improve or benchmark a model, whether for the benefit of Pemberton Home Goods or the provider's general model.

Subprocessor: A third party engaged by the AI provider to process Pemberton Home Goods data on the provider's behalf, including hosting providers, annotation services and downstream model providers.

Model change: A modification to the AI system that could alter its outputs, accuracy, behaviour or risk profile, including model retraining, architecture changes, prompt or system instruction updates, and changes to the data sources the model relies on.

Exit capability: The ability to terminate the supplier relationship and recover or confirm deletion of all Pemberton Home Goods data, including any derived data, embeddings or model artefacts, within a defined period and in a usable format.

4. Roles and Responsibilities

Requesting Business Owner: The manager or director sponsoring the use of the AI supplier. Responsible for documenting the use case, data flows and business criticality, and for confirming ongoing compliance with review conditions.

Director of Digital (Document Owner): Responsible for maintaining this procedure, coordinating reviews, and ensuring findings are recorded. Leads the technical and governance assessment.

Privacy Officer: Assesses privacy implications, data handling commitments and alignment with the Privacy and Personal Information Policy.

IT Manager: Assesses security controls, integration risks and alignment with the Information Security Policy. Escalates incidents to the Chief Operating Officer.

Chief Operating Officer (Review Authority): Reviews and accepts residual risk for Critical-tier AI suppliers. May delegate Elevated-tier reviews to the Director of Digital.

Finance Director: Consulted immediately for any AI supplier that touches the payment path or could affect payment-industry compliance.

5. Procedure Overview

The review follows five stages:

- 5.1 Intake and Use-Case Documentation
- 5.2 Due-Diligence Assessment
- 5.3 Findings, Contract Requirements and Residual Risk
- 5.4 Review Decision and Recording
- 5.5 Ongoing Monitoring and Exit

Each stage must be completed in sequence. A supplier may not process Pemberton Home Goods data or be integrated into production systems until the review decision is recorded.

6. Stage 1 — Intake and Use-Case Documentation

Step 1: Requesting Business Owner completes the AI Supplier Intake Form, recording:

- Supplier name and service description.
- Business use case and the problem the AI capability addresses.
- Data categories to be shared with or accessed by the supplier, classified per the Data Classification and Handling Standard.
- Decisions the AI will generate, influence or automate, and who is affected.
- Integration points with Pemberton Home Goods systems.
- Business criticality: Critical, Elevated or Standard, applying the tiers in the Third-Party Risk Management Policy.

Step 2: Requesting Business Owner submits the completed form to the Director of Digital.

Step 3: Director of Digital confirms the form is complete and assigns a risk tier. Critical-tier suppliers include any that touch the commerce platform, the personalisation vendor, the payment processor or the loyalty database. Elevated-tier suppliers include marketing and analytics suppliers. Standard-tier covers all others.

Step 4: Director of Digital notifies the Privacy Officer and IT Manager that a review is required, and the Finance Director if the supplier touches the payment path.

7. Stage 2 — Due-Diligence Assessment

The Director of Digital coordinates the assessment. Each domain is assessed by the responsible party.

7.1 Security Assessment (IT Manager)

Step 5: IT Manager requests and reviews the supplier's security documentation, including certifications, penetration test summaries and incident history.

Step 6: IT Manager assesses:

- Data encryption in transit and at rest.
- Access controls and authentication for Pemberton Home Goods data.
- Logging and monitoring of access to Pemberton Home Goods data.
- Incident detection and response capability.
- Alignment with the Information Security Policy.

Step 7: IT Manager records findings and any gaps.

7.2 Privacy Assessment (Privacy Officer)

Step 8: Privacy Officer requests and reviews the supplier's privacy documentation, including data processing agreements and privacy notices.

Step 9: Privacy Officer assesses:

- Lawful basis for processing and alignment with Pemberton Home Goods consent and contract positions.
- Data minimisation and purpose limitation.
- Retention periods and deletion commitments.
- Subprocessor disclosure and flow-down of obligations.
- Cross-border transfer mechanisms, confirming data remains within Canada and the United States unless explicitly justified and documented.
- Alignment with the Privacy and Personal Information Policy.

Step 10: Privacy Officer records findings and any gaps.

7.3 Model Governance and Training Use (Director of Digital)

Step 11: Director of Digital requests and reviews the supplier's model governance documentation.

Step 12: Director of Digital assesses:

- Whether the supplier uses Pemberton Home Goods data for training, fine-tuning or model improvement. The required position is no training on customer data.
- How the supplier manages model versioning and change control.
- Whether the supplier commits to notifying Pemberton Home Goods of material model changes before they take effect, and the notice period offered.
- How the supplier tests for bias, accuracy degradation and unintended outputs.

Step 13: Director of Digital records findings and any gaps.

7.4 Output Quality, Human Oversight and Transparency (Director of Digital and Requesting Business Owner)

Step 14: Director of Digital and Requesting Business Owner assess:

- How output quality is measured and monitored by the supplier.
- Whether the integration design preserves the human oversight required by the AI Acceptable Use Policy—specifically, that a support agent reads and sends every drafted reply, and that a merchandising manager sets and reviews pricing bounds weekly.
- Whether customers can be informed that AI is involved in decisions affecting them, and whether opt-out is supported. Customers must be able to opt out of personalisation without losing service.
- Whether the supplier provides explanations or audit trails for individual outputs when required.

Step 15: Director of Digital records findings and any gaps.

7.5 Subprocessor and Downstream Disclosure (Privacy Officer)

Step 16: Privacy Officer confirms the supplier has disclosed all subprocessors that will process Pemberton Home Goods data.

Step 17: Privacy Officer assesses whether subprocessor obligations flow down, including the prohibition on training use and the requirement to honour opt-out and deletion downstream.

Step 18: Privacy Officer records findings and any gaps.

8. Stage 3 — Findings, Contract Requirements and Residual Risk

Step 19: Director of Digital consolidates findings from all assessors into a single AI Supplier Review Record.

Step 20: Director of Digital identifies contract requirements that must be in place before the supplier is engaged. At minimum, contracts with AI providers must include:

- Prohibition on training use of Pemberton Home Goods data.
- Commitment to honour opt-out and deletion requests downstream.
- Breach notification within a deadline set by Pemberton Home Goods and recorded in the contract. Pemberton Home Goods has not yet set this deadline; 24 hours is offered as a starting point and is not derived from any cited control.
- Disclosure of subprocessors and advance notice of subprocessor changes.
- Evidence of payment-industry compliance where the payment path is touched.
- Commitment to notify Pemberton Home Goods of material model changes before they take effect, with a notice period set by Pemberton Home Goods and recorded in the contract.
- Exit provisions confirming data return or certified deletion within a period set by Pemberton Home Goods and recorded in the contract.

Step 21: Director of Digital documents any gaps that cannot be closed by contract, the compensating controls proposed, and the residual risk.

Step 22: Director of Digital assigns a residual risk rating: Low, Moderate, High or Unacceptable. Unacceptable means the engagement may not proceed.

9. Stage 4 — Review Decision and Recording

Step 23: For Critical-tier suppliers, the Director of Digital presents the AI Supplier Review Record to the Chief Operating Officer for review.

Step 24: Chief Operating Officer reviews the findings, contract requirements, compensating controls and residual risk. The Chief Operating Officer may:

- Accept the residual risk and record the review as complete.

- Require additional controls or contract terms before accepting.
- Decline the engagement.

Step 25: For Elevated-tier suppliers, the Director of Digital may complete the review, unless the residual risk is rated High, in which case the Chief Operating Officer reviews.

Step 26: For Standard-tier suppliers, the Director of Digital completes the review.

Step 27: Director of Digital records the review decision, the date, the reviewer, any conditions, and the next review date in the AI Supplier Register.

Step 28: Director of Digital notifies the Requesting Business Owner of the outcome. If the review is complete with conditions, the Requesting Business Owner is responsible for confirming the conditions are met before the supplier is engaged.

10. Stage 5 — Ongoing Monitoring and Exit

10.1 Ongoing Monitoring

Step 29: Requesting Business Owner monitors the supplier's performance and compliance with contract terms on an ongoing basis.

Step 30: Director of Digital schedules a full re-review at least annually, or sooner if a material change occurs. Material changes include:

- Changes to the data categories shared with the supplier.
- Changes to the decisions the AI influences.
- Model changes notified by the supplier.
- Security or privacy incidents involving the supplier.
- Changes to subprocessors.

Step 31: If the supplier notifies a material model change, the Director of Digital assesses whether the change affects the original risk rating and whether additional review is required before the change takes effect.

Step 32: If a security or privacy incident occurs involving the supplier, the IT Manager and Privacy Officer follow the Security Incident Response Procedure and Privacy Breach Response Procedure respectively, and the Director of Digital records the incident in the AI Supplier Register.

10.2 Exit

Step 33: When the supplier relationship ends, the Requesting Business Owner notifies the Director of Digital.

Step 34: Director of Digital confirms with the supplier that all Pemberton Home Goods data, including derived data, embeddings and model artefacts, has been returned in a usable format or securely deleted.

Step 35: Director of Digital obtains written certification of deletion from the supplier.

Step 36: Director of Digital records the exit date and deletion confirmation in the AI Supplier Register.

11. Records and Metrics

The Director of Digital maintains the following records:

- AI Supplier Intake Forms.
- AI Supplier Review Records, including findings, contract requirements, residual risk and review decisions.
- AI Supplier Register, listing all reviewed suppliers, their tier, review dates, conditions, next review dates and exit dates.

The following metrics are reported to the Chief Operating Officer on a frequency set by Pemberton Home Goods (quarterly is offered as a starting point):

- Number of AI suppliers reviewed before use.
- Number of contract gaps identified and their treatment status.
- Percentage of required reviews completed on time.
- Number of exceptions past their expiry date.
- Number of material control failures and overdue corrective actions.

12. Related Documents

- AI Acceptable Use Policy
- AI Governance and Accountability Policy

- AI Risk Management Standard
- AI Incident Response Procedure
- Third-Party Risk Management Policy
- Privacy and Personal Information Policy
- Privacy Breach Response Procedure
- Information Security Policy
- Security Incident Response Procedure
- Data Classification and Handling Standard
- Records Retention and Disposal Policy

SPECIMEN

13. Review and Maintenance

The Director of Digital reviews this procedure at least annually, or sooner following a material incident, regulatory change or organisational change affecting AI supplier risk. Changes are reviewed by the Chief Operating Officer before taking effect.

Owner review items

The drafting process identified the following in the supplied answers. Resolve each before customer release.

Type	Detail	Where
gap	No verified framework controls were supplied. This procedure is based on RiskWoven AI practical best practices as stated in the specification, but no specific control identifiers or citations are available to reference.	Entire document
gap	The organisation has not specified the breach notification deadline to require from AI suppliers. The procedure notes this as an organisational parameter with 24 hours offered as a starting point.	Section 8, Step 20
gap	The organisation has not specified the notice period required for material model changes. This must be set and recorded in contracts.	Section 8, Step 20
gap	The organisation has not specified the period within which data must be returned or deleted at exit. This must be set and recorded in contracts.	Section 8, Step 20
gap	The reporting frequency for metrics is not specified. Quarterly is offered as a starting point.	Section 11
gap	The AI Supplier Intake Form and AI Supplier Review Record templates are referenced but not provided. The organisation must create or adopt these templates.	Sections 6, 8, 9
vague	The existing Third-Party Risk Management Policy is referenced for supplier tiers, but its text was not provided. The organisation must confirm the tier definitions in this procedure align with that policy.	Section 6, Step 3

Information the organization must supply

These values were not available from the intake and are required before this document can operate:

- Breach notification deadline to require from AI suppliers (24 hours is offered as a starting point).
- Notice period required from suppliers for material model changes before they take effect.
- Period within which data must be returned or securely deleted at contract exit.
- Reporting frequency for AI supplier metrics (quarterly is offered as a starting point).
- AI Supplier Intake Form template or confirmation that one will be created.
- AI Supplier Review Record template or confirmation that one will be created.
- Confirmation that the supplier tier definitions in this procedure align with the Third-Party Risk Management Policy.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

SPECIMEN