

Specimen — illustrative example

Meridian Community Credit Union 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 Risk Management Policy

Meridian Community Credit Union

Document type	policy	Version	1.0 Draft
Owner	Chief Risk Officer	Customer decision role	Board Risk Committee
Effective date	Upon customer release	Review cycle	Annual
Framework basis	RiskWoven AI practical best practices		
Jurisdiction	Ontario, Canada		
Prepared for	Meridian Community Credit Union	Industry	Financial services
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 policy establishes the requirements for identifying, assessing, contracting with, monitoring and exiting third-party relationships at Meridian Community Credit Union. It ensures that

suppliers who access member information, connect to critical systems or deliver services on which the Credit Union depends are subject to risk-proportionate oversight throughout the relationship lifecycle.

2. Scope

This policy applies to all third-party relationships where the supplier:

- a) Accesses, processes, stores or transmits member information or other confidential Credit Union data;
- b) Connects to or integrates with Credit Union systems, including the core banking system, digital banking channel, loan pre-adjudication service, member data warehouse or branch endpoints;
- c) Provides a service whose failure would impair the Credit Union's ability to serve members or meet regulatory obligations; or
- d) Acts as a subprocessor on behalf of another supplier already in scope.

All employees, contractors and agents who select, engage or manage third parties must comply with this policy. The policy does not apply to member relationships, employment relationships or arrangements with regulators.

3. Definitions

Third party: Any external organisation or individual that provides goods, services or access to the Credit Union under contract, including vendors, service providers, consultants, software licensors and outsourced function providers.

Critical supplier: A third party whose failure, compromise or misconduct could materially impair the Credit Union's operations, financial condition, member service or regulatory standing. At Meridian, this classification includes the core banking provider, the credit-scoring model vendor and the credit bureau.

Due diligence: The structured assessment of a third party's security posture, privacy practices, financial stability, regulatory standing, business continuity capability and operational resilience, conducted before engagement and periodically thereafter.

Subprocessor: A third party engaged by a supplier to perform part of the service the supplier has contracted to deliver to the Credit Union, where that performance involves access to Credit Union data or systems.

Exit plan: A documented set of arrangements that enable the Credit Union to terminate a third-party relationship, recover its data and transition the service to an alternative provider or in-house operation without unacceptable disruption to members or operations.

4. Principles

4.1 Risk proportionality. The depth of due diligence, the rigour of contractual terms and the frequency of ongoing monitoring must be proportionate to the risk the relationship presents. Higher risk demands greater scrutiny.

4.2 Accountability. Every third-party relationship has a named business owner accountable for compliance with this policy throughout the relationship lifecycle.

4.3 Transparency. The Credit Union maintains a complete, current inventory of in-scope third parties, their risk tier and the status of required assessments.

4.4 Continuity. No critical service may depend on a single supplier without a documented exit plan and, where practicable, an identified alternative.

4.5 Member protection. Member information shared with a third party remains subject to the Credit Union's privacy and security obligations. Contractual and monitoring arrangements must preserve those protections.

5. Supplier Classification

5.1 Every prospective and existing third party in scope must be classified into one of the following tiers before engagement or, for existing relationships, within the timeframe the Chief Risk Officer sets for remediation.

5.2 Classification criteria:

a) Data sensitivity: Does the supplier access, process or store member financial records, identity information, income or employment data, or other information classified as confidential or higher under the Data Classification and Handling Standard?

b) System access: Does the supplier connect to or integrate with the core banking system, digital banking channel, loan pre-adjudication service, member data warehouse, branch endpoints or other systems designated as critical?

c) Service criticality: Would the supplier's failure prevent the Credit Union from delivering core member services, processing transactions or meeting regulatory reporting obligations?

d) Business impact: Could the supplier's failure, data breach or misconduct cause material financial loss, regulatory sanction, reputational harm or member harm?

5.3 Tier definitions:

Critical: The supplier meets one or more of the following conditions: it provides the core banking platform, the credit-scoring model or credit-bureau services; it has direct access to member financial records at scale; or its failure would breach the recovery time objectives stated in the Business Continuity Policy. Critical suppliers require review by the Board Risk Committee before engagement.

Elevated: The supplier accesses member information or connects to Credit Union systems but does not meet the Critical threshold. Elevated suppliers require review by the Chief Risk Officer or delegate before engagement.

Standard: The supplier is in scope but does not access member information, does not connect to critical systems and does not provide a service whose failure would materially impair operations. Standard suppliers require review by the business owner with oversight from Procurement or the designated function.

5.4 The business owner proposes the tier. The Chief Risk Officer or delegate confirms or adjusts the classification. Disputes escalate to the Board Risk Committee.

5.5 Classification must be reassessed when the scope of the relationship changes, when the supplier's risk profile changes materially, or at the periodic reassessment required for the tier.

6. Due Diligence Requirements

6.1 No contract may be executed with a third party in scope until due diligence proportionate to the proposed tier has been completed and the required reviewer has recorded acceptance of the residual risk.

6.2 Due diligence must address the following domains, with depth scaled to tier:

a) **Security:** Evidence of the supplier's information-security controls, including independent certifications, penetration-test summaries, vulnerability-management practices and incident-response capability.

b) Privacy: Evidence that the supplier can meet the Credit Union's obligations under applicable Ontario privacy law, including data-handling practices, breach-notification capability and restrictions on secondary use.

c) Resilience: Evidence of the supplier's business-continuity and disaster-recovery capability, including recovery objectives, test results and geographic redundancy where relevant.

d) Compliance: Confirmation of the supplier's regulatory standing, including any enforcement actions, material litigation or sanctions relevant to the services proposed.

e) Financial stability: For Critical and Elevated suppliers, evidence that the supplier is financially viable and likely to remain so for the expected term of the relationship.

f) Subprocessor arrangements: Identification of any subprocessors the supplier intends to use for in-scope activities, and confirmation that those subprocessors are subject to equivalent controls.

6.3 For Critical suppliers, due diligence must include:

- Review of the supplier's most recent SOC 2 Type II report or equivalent independent assurance, with any exceptions documented and risk-assessed.
- Confirmation that the supplier does not use Credit Union member data to train machine-learning models without explicit, documented consent.
- Validation of the supplier's model-governance practices where the supplier provides credit-scoring or other algorithmic decision-support services, consistent with the AI Governance and Accountability Policy.
- Assessment of concentration risk, including the supplier's reliance on its own critical subprocessors.

6.4 For Elevated suppliers, due diligence must include at minimum a completed security questionnaire, evidence of current certifications and confirmation of breach-notification capability.

6.5 For Standard suppliers, due diligence must confirm that the supplier's practices are consistent with the Credit Union's baseline security and privacy expectations, documented through questionnaire or attestation.

6.6 Due diligence findings must be documented in the third-party risk register. High-risk findings must have a treatment plan recorded before the relationship proceeds, or the engagement must be declined.

7. Contractual Requirements

7.1 Every contract with a third party in scope must include terms that preserve the Credit Union's ability to oversee, audit and exit the relationship. The Chief Risk Officer maintains a schedule of required contractual clauses by tier.

7.2 For all in-scope suppliers, contracts must include:

- a) A clear description of the services, data and systems in scope.
- b) Confidentiality obligations at least as protective as the Credit Union's own.
- c) The supplier's obligation to comply with applicable law, including Ontario privacy legislation.
- d) The Credit Union's right to receive notice of security incidents, privacy breaches or material control failures affecting Credit Union data or services.
- e) Provisions for return or secure destruction of Credit Union data on termination.

7.3 For Critical and Elevated suppliers, contracts must additionally include:

- a) The Credit Union's right to audit the supplier's controls, or to receive and rely on independent assurance reports, on a frequency set by the Credit Union and recorded in the contract.
- b) A requirement that the supplier notify the Credit Union of a suspected or confirmed security incident or privacy breach within a timeframe set by Meridian and recorded in the contract. Meridian has not yet set this timeframe; 24 hours is a common commercial position and is offered as a starting point, not as a requirement derived from any cited control.
- c) A requirement that the supplier obtain the Credit Union's prior written consent before engaging or changing a subprocessor for in-scope activities.
- d) Business-continuity commitments, including recovery objectives consistent with the Credit Union's own where the supplier supports a critical service.
- e) Defined exit-assistance obligations, including cooperation with transition, data migration and knowledge transfer for a period set by Meridian and recorded in the contract.
- f) A prohibition on using Credit Union member data to train machine-learning models without explicit, documented consent from the Credit Union.

7.4 For suppliers providing credit-scoring, algorithmic decision-support or other AI-enabled services, contracts must require evidence of model validation and ongoing performance monitoring, consistent with the AI Governance and Accountability Policy and the Third-Party AI Review Procedure.

7.5 Deviations from required contractual terms must be documented, risk-assessed and reviewed at the tier-appropriate level before the contract is executed. Material deviations for Critical suppliers require Board Risk Committee review.

8. Review and Engagement Authority

8.1 The following review authorities apply:

Critical suppliers: Board Risk Committee, following recommendation by the Chief Risk Officer.

Elevated suppliers: Chief Risk Officer, or a delegate the Chief Risk Officer designates in writing.

Standard suppliers: Business owner, with oversight from Procurement or the designated function and periodic reporting to the Chief Risk Officer.

8.2 No engagement may proceed until the reviewer at the required level has recorded acceptance of the residual risk in the third-party risk register.

8.3 Contract execution authority is governed by the Credit Union's delegation-of-authority framework. Review under this policy does not itself confer signing authority.

9. Ongoing Monitoring

9.1 Third-party relationships do not end at contract signature. The business owner is accountable for monitoring the supplier throughout the relationship, with support from Risk, Information Security and Privacy functions as the tier requires.

9.2 Monitoring must address:

- a) Performance: Is the supplier meeting service levels and contractual commitments?
- b) Incidents: Has the supplier reported any security incidents, privacy breaches or material control failures? Has the Credit Union identified any through its own monitoring?
- c) Findings: Have independent assurance reports, audits or assessments identified new control gaps or exceptions?
- d) Material changes: Has the supplier changed ownership, financial condition, key personnel, subprocessors or the location of data processing?
- e) Regulatory developments: Has the supplier been subject to enforcement action, sanction or material litigation relevant to the services it provides?

9.3 Monitoring frequency by tier:

Critical suppliers: Continuous monitoring of incident notifications and service performance. Formal reassessment at least annually, or more frequently if the Board Risk Committee directs.

Elevated suppliers: Reassessment on a cycle set by Meridian; annual reassessment is offered as a starting point and is not derived from any cited control.

Standard suppliers: Reassessment on a cycle set by Meridian; reassessment every two years is offered as a starting point and is not derived from any cited control.

9.4 The business owner must notify the Chief Risk Officer promptly of any material change, incident or finding that could affect the supplier's risk tier or the Credit Union's exposure.

9.5 Where a supplier provides services supporting the core banking system, digital banking channel or loan pre-adjudication service, monitoring must confirm that the supplier's recovery capability remains consistent with the Credit Union's recovery time and recovery point objectives as stated in the Business Continuity Policy.

10. Subprocessor Oversight

10.1 A supplier's use of subprocessors extends the Credit Union's risk surface. Subprocessors with access to member data or critical systems must be subject to controls equivalent to those the Credit Union requires of the primary supplier.

10.2 For Critical and Elevated suppliers, the contract must require prior written consent before the supplier engages or changes a subprocessor for in-scope activities. The supplier must provide sufficient information for the Credit Union to assess the subprocessor's risk.

10.3 The business owner must maintain a record of known subprocessors for each Critical and Elevated supplier, updated when the supplier notifies a change.

10.4 Where a subprocessor presents material risk, the Chief Risk Officer may require direct due diligence, additional contractual protections or, if the risk cannot be mitigated, refusal of consent.

11. Incident Notification and Response

11.1 Contracts with Critical and Elevated suppliers must require the supplier to notify the Credit Union of a suspected or confirmed security incident or privacy breach affecting Credit Union

data or services within the timeframe recorded in the contract.

11.2 On receipt of such notification, the business owner must immediately inform the Chief Information Security Officer and the Privacy Officer. The Security Incident Response Procedure and the Privacy Breach Response Procedure govern the Credit Union's response.

11.3 Where the incident involves an AI-enabled service, the AI Incident Response Procedure applies in addition.

11.4 The business owner must document the incident, the supplier's response and any remediation in the third-party risk register. Material incidents must be reported to the Board Risk Committee.

12. Exit Planning and Offboarding

12.1 Every Critical supplier relationship must have a documented exit plan before the relationship is established. The exit plan must address:

- a) Trigger events that would require exit, including supplier failure, material breach, regulatory direction or strategic decision.
- b) Data retrieval: How the Credit Union will recover its data in a usable format.
- c) Transition: How the service will be moved to an alternative provider or brought in-house, including estimated timeline and resource requirements.
- d) Continuity: How member service will be maintained during transition, including manual fallback where applicable.
- e) Knowledge transfer: How operational knowledge held by the supplier will be transferred to the Credit Union or successor.
- f) Secure disposal: How the supplier will certify destruction of Credit Union data on termination.

12.2 For Elevated suppliers, an exit plan is required where the supplier provides a service with no readily available alternative or where transition would take longer than the notice period in the contract.

12.3 Exit plans must be reviewed at each periodic reassessment and updated when material changes occur.

12.4 On termination of any in-scope relationship, the business owner must:

- a) Confirm return or certified destruction of Credit Union data.
- b) Revoke the supplier's access to Credit Union systems and facilities.

- c) Update the third-party inventory to reflect the terminated status.
- d) Retain contract and due-diligence records in accordance with the Records Retention and Disposal Policy.

SPECIMEN

13. Exceptions

13.1 Where compliance with a requirement of this policy is not practicable, the business owner may request an exception. The request must document:

- a) The specific requirement from which exception is sought.
- b) The reason compliance is not practicable.
- c) The compensating controls or mitigations in place.
- d) The proposed duration of the exception.
- e) The residual risk accepted.

13.2 Exceptions for Critical suppliers require Board Risk Committee review. Exceptions for Elevated suppliers require Chief Risk Officer review. Exceptions for Standard suppliers require review by the Chief Risk Officer or delegate.

13.3 Exceptions must have a defined expiry date. The business owner must remediate the exception or seek renewal before expiry. Expired exceptions without renewal are reported to the Board Risk Committee.

13.4 The Chief Risk Officer maintains a register of active exceptions and reports the count and status to the Board Risk Committee at each meeting.

14. Metrics and Reporting

14.1 The Chief Risk Officer reports the following metrics to the Board Risk Committee on a frequency set by the Committee; quarterly reporting is offered as a starting point:

- a) Percentage of Critical suppliers assessed on time against the required reassessment cycle.
- b) Number of high-risk findings without a documented treatment plan.
- c) Percentage of required periodic reviews completed on time across all tiers.
- d) Number of approved exceptions past their expiry date.
- e) Number of material control failures reported by suppliers and count of overdue corrective actions.

14.2 The third-party risk register is the system of record for supplier inventory, classification, due-diligence status, findings, exceptions and incidents. The Chief Risk Officer is accountable for the register's completeness and accuracy.

14.3 Significant adverse trends or individual events with material member, financial or regulatory impact must be escalated to the Board Risk Committee promptly, outside the regular reporting cycle.

15. Roles and Responsibilities

Board Risk Committee: Reviews and accepts residual risk for Critical supplier engagements. Reviews material exceptions, incidents and adverse trends. Oversees the effectiveness of the third-party risk management programme.

Chief Risk Officer: Owns this policy. Maintains the third-party risk register and required-clause schedule. Reviews Elevated supplier engagements and exceptions. Reports metrics and material events to the Board Risk Committee.

Chief Information Security Officer: Advises on security due diligence and contractual requirements. Leads response to supplier security incidents. Monitors supplier access to Credit Union systems.

Privacy Officer: Advises on privacy due diligence and contractual requirements. Leads response to supplier privacy breaches. Confirms supplier compliance with applicable Ontario privacy law.

Business owner: Accountable for the supplier relationship from selection through exit. Proposes classification, conducts or coordinates due diligence, negotiates contracts within delegated authority, monitors performance and incidents, maintains the exit plan and ensures records are current.

Procurement (or designated function): Supports contract negotiation and execution. Confirms required clauses are included. Maintains contract repository.

16. Related Documents

This policy operates alongside the following Credit Union documents:

- AI Governance and Accountability Policy
- Privacy and Personal Information Policy
- AI Risk Management Standard
- Third-Party AI Review Procedure

- Security Incident Response Procedure
- Privacy Breach Response Procedure
- AI Incident Response Procedure
- Business Continuity Policy
- Records Retention and Disposal Policy
- Information Security Policy
- Data Classification and Handling Standard
- Access Control Policy

Where a third party provides AI-enabled services, the requirements of the AI Governance and Accountability Policy and the Third-Party AI Review Procedure apply in addition to this policy.

17. Review and Maintenance

17.1 The Chief Risk Officer reviews this policy at least annually, or sooner if material changes in regulation, risk environment or organisational structure require it.

17.2 Amendments to this policy require Board Risk Committee review before taking effect.

17.3 The Chief Risk Officer maintains a version history recording the date, nature and reviewer of each amendment.

18. Compliance and Enforcement

18.1 All employees, contractors and agents involved in selecting, engaging or managing third parties must comply with this policy.

18.2 Non-compliance may result in disciplinary action, up to and including termination of employment or contract.

18.3 The Chief Risk Officer may direct suspension of a third-party engagement that proceeds without required due diligence or review, pending remediation or escalation to the Board Risk Committee.

Owner review items

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

Type	Detail	Where
gap	The information supplied does not specify the incident-notification timeframe Meridian requires from suppliers. The policy notes that Meridian must set this value and record it in contracts; 24 hours is offered as a starting point only.	Section 7.3(b) and Section 11.1
gap	The information supplied does not specify the reassessment frequency for Elevated and Standard suppliers. The policy states these as organisational parameters to be set by Meridian, with annual and biennial starting points respectively.	Section 9.3
gap	The information supplied does not specify the exit-assistance period Meridian requires in contracts. The policy requires this to be set by Meridian and recorded in each contract.	Section 7.3(e)
gap	The information supplied does not specify the reporting frequency to the Board Risk Committee for third-party risk metrics. The policy notes this is set by the Committee, with quarterly as a starting point.	Section 14.1
gap	The information supplied references applicable Ontario privacy law but does not name the specific statute. The policy uses 'applicable Ontario privacy law' throughout. Meridian's legal advisors should confirm which of PIPEDA, Ontario-specific legislation or sector regulation applies to the Credit Union's third-party arrangements.	Sections 6.2(b), 7.2(c), 15
vague	The information supplied identifies Procurement or a designated function for contract support but does not confirm whether Meridian has a Procurement function or what the designated alternative is. The policy uses 'Procurement or the designated function' pending clarification.	Sections 5.3, 15

Information the organization must supply

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

- The incident-notification timeframe Meridian requires from Critical and Elevated suppliers (the policy offers 24 hours as a starting point).
- The reassessment frequency for Elevated suppliers (the policy offers annual as a starting point).
- The reassessment frequency for Standard suppliers (the policy offers biennial as a starting point).
- The exit-assistance period Meridian requires in contracts with Critical and Elevated suppliers.

- The reporting frequency for third-party risk metrics to the Board Risk Committee (the policy offers quarterly as a starting point).
- Confirmation of which function performs the Procurement or contract-support role described in the policy.
- Legal confirmation of the specific Ontario privacy legislation applicable to the Credit Union's third-party arrangements.

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