

Specimen — illustrative example

Halden Precision Manufacturing 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.

Business Continuity Policy

Halden Precision Manufacturing

Document type	policy	Version	1.0 Draft
Owner	Plant Operations Manager	Customer decision role	Chief Operating Officer
Effective date	Upon customer release	Review cycle	Annual
Framework basis	RiskWoven AI practical best practices		
Jurisdiction	Ontario, Canada		
Prepared for	Halden Precision Manufacturing	Industry	Precision manufacturing
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 governs how Halden Precision Manufacturing identifies, protects and recovers its critical manufacturing and business services when disruption occurs. It establishes the

mandate for business impact analysis, recovery objectives, continuity planning, and plan testing across the organisation's people, facilities, technology, information and supply chain. The goal is to maintain safe, compliant and commercially viable operations through any disruption and to restore normal production at a pace that reflects the business consequences of downtime.

2. Scope

This policy applies to:

- All production lines, quality systems and supporting business functions operated by Halden Precision Manufacturing;
- All employees, contractors and on-call personnel who operate, maintain or support those functions across all three production shifts and the weekend maintenance window;
- All technology systems, facilities, information assets and third-party suppliers on which critical services depend;
- Suppliers classified as critical under the Third-Party Risk Management Policy, including the vision system vendor, the controls integrator and the maintenance analytics provider.

This policy does not duplicate the Information Security Policy, the Third-Party Risk Management Policy, the Privacy and Personal Information Policy or the Records Retention and Disposal Policy. Where continuity obligations intersect with those instruments, this policy states the continuity-specific mandate and defers the detailed requirements to the relevant sibling document.

3. Policy Owner and Accountabilities

Policy owner: The Plant Operations Manager owns this policy. The Plant Operations Manager is accountable for maintaining the business impact analysis, keeping continuity plans current, scheduling and recording exercises, and reporting the metrics in Section 9 to the Chief Operating Officer.

Review authority: The Chief Operating Officer holds review authority for this policy and for all recovery objectives set under it. No recovery objective, continuity strategy or material exception takes effect until the Chief Operating Officer has reviewed and recorded that review.

Quality Manager: The Quality Manager reviews this policy on the annual cycle defined in Section 10 and reviews continuity plans that affect the quality records system.

Controls Engineer: The Controls Engineer is responsible for the technical execution of continuity and recovery activities for production line control systems, including fallback activation and system restoration.

All employees: Every employee is responsible for knowing the continuity arrangements that apply to their role and for following those arrangements when activated.

4. Definitions

Critical service: A product, service or function whose loss or degradation for longer than its defined recovery time objective would cause unacceptable harm to production output, customer commitments, regulatory compliance or personnel safety. Critical services are identified through the business impact analysis and listed in the continuity register.

Business impact analysis (BIA): A structured assessment that identifies critical services, quantifies the consequences of disruption over time, determines the maximum tolerable period of disruption, and establishes the recovery objectives and priorities that this policy requires.

Recovery time objective (RTO): The maximum elapsed time from the point of disruption to the point at which a critical service must be restored to an acceptable operating level. RTOs are set by the Chief Operating Officer following the BIA.

Recovery point objective (RPO): The maximum age of data or process state that can be lost when a critical service is restored. RPOs are set by the Chief Operating Officer following the BIA and determine backup and replication requirements.

Continuity plan: A documented set of actions, roles, resources and decision criteria that enables Halden Precision Manufacturing to maintain or restore a critical service within its RTO and RPO. A continuity plan covers people, facilities, technology, information and suppliers relevant to that service.

5. Critical Services and Recovery Objectives

The Chief Operating Officer has reviewed and recorded the following recovery objectives. These figures are binding on all continuity plans and exercises until the Chief Operating Officer records a revised review.

Critical service	RTO	RPO	Primary fallback
------------------	-----	-----	------------------

Production line control	4 hours	1 hour	Manual operation per documented fallback procedure
Quality records system	24 hours	4 hours	Manual inspection records per documented fallback procedure
Reporting and analytics	5 business days	24 hours	Deferred reporting; manual data collection

Manual inspection is the documented fallback for the vision system. The Controls Engineer is responsible for maintaining the manual fallback procedure and for confirming at each annual exercise that production staff can execute it without system support.

The Plant Operations Manager must initiate a BIA review whenever a new service is proposed for the critical services list, whenever an existing service's business impact changes materially, or whenever a continuity exercise reveals that a current objective cannot be met. The Chief Operating Officer must review and record any change to the table above before it takes effect.

6. Business Impact Analysis

The Plant Operations Manager must conduct a BIA covering all services that may qualify as critical. The BIA must:

- Identify each service, its dependencies (people, facilities, technology, information and suppliers) and the consequences of disruption at defined time intervals;
- Determine the maximum tolerable period of disruption for each service;
- Propose RTO and RPO values for Chief Operating Officer review;
- Identify single points of failure and interdependencies, including dependencies on critical suppliers;
- Inform the continuity strategies required by Section 7.

The BIA must be reviewed on the annual cycle defined in Section 10 and whenever a material change occurs to a critical service or its dependencies. The BIA review record must be retained in accordance with the Records Retention and Disposal Policy.

7. Continuity Strategies and Plans

7.1 Requirement to plan

Every critical service listed in Section 5 must have a current, tested continuity plan. A plan that has not been exercised within the required cycle is not considered current.

7.2 Plan content

Each continuity plan must address:

- **People:** Named roles and their alternates for each shift, including on-call coverage for controls support outside shift hours. The plan must remain executable when key individuals are unavailable.
- **Facilities:** The actions required if the primary facility is inaccessible, including any alternative work locations or production arrangements.
- **Technology:** Step-by-step recovery actions for each technology component within the service, including the activation of fallback systems. For production line control, this includes the manual inspection fallback and the conditions under which the Controls Engineer activates it.
- **Information:** Backup and restoration procedures consistent with the RPO for each service. Backup arrangements must align with the Data Classification and Handling Standard.
- **Suppliers:** Actions required when a critical supplier cannot deliver. Plans must reflect the support response times, notification obligations and source or escrow arrangements required under the Third-Party Risk Management Policy for the vision system vendor, the controls integrator and the maintenance analytics provider.

7.3 Activation and escalation

Each plan must state the conditions that trigger activation, the role responsible for declaring activation, and the escalation path to the Chief Operating Officer. Plans must be consistent with the Security Incident Response Procedure and the AI Incident Response Procedure where a disruption has a security or AI dimension.

7.4 Availability during disruption

Continuity plans must be accessible when the systems they protect are unavailable. The Plant Operations Manager is responsible for ensuring that current plan versions are held in a location and format that remains accessible during the disruption scenarios the plans address.

8. Supplier Continuity Requirements

Critical suppliers — the vision system vendor, the controls integrator and the maintenance analytics provider — must demonstrate continuity capability as a condition of their engagement and at each contract renewal. The Plant Operations Manager, with Chief Operating Officer review, must confirm that each critical supplier's continuity arrangements are consistent with the RTOs and RPOs in Section 5.

Contract terms for critical suppliers must include defined support response times, notification of model or software changes, and source code or escrow arrangements for line-critical software, consistent with the Third-Party Risk Management Policy. Where a critical supplier's continuity capability is found to be inadequate, the Plant Operations Manager must escalate to the Chief Operating Officer and record a corrective action.

The Third-Party Risk Management Policy governs the broader supplier risk framework. This policy states only the continuity-specific obligations.

9. Exercises and Testing

9.1 Exercise requirement

Every continuity plan for a critical service must be exercised on a cycle set by the Plant Operations Manager and reviewed by the Chief Operating Officer. Halden Precision Manufacturing has set this cycle as annual; this is an organisational decision and is not derived from an external framework requirement. The exercise cycle must be risk-based: services with higher business impact or greater dependency complexity may warrant more frequent exercises, and the Plant Operations Manager must document the rationale for the cycle assigned to each plan.

9.2 Exercise types

Exercises may include tabletop walkthroughs, component tests or full activation tests. The exercise type must be appropriate to the risk level of the service. At least one exercise per cycle for production line control must test the manual inspection fallback under realistic conditions.

9.3 Exercise records

The Plant Operations Manager must record the date, type, participants, scenario, findings and corrective actions for every exercise. Records must be retained in accordance with the Records Retention and Disposal Policy.

9.4 Corrective actions

Every material weakness identified in an exercise must have a corrective action with a named owner and a target completion date. The Plant Operations Manager must track open corrective actions and report overdue items to the Chief Operating Officer. A material weakness is one that would prevent a critical service from meeting its RTO or RPO, or that would leave personnel unable to execute the plan safely.

9.5 Metrics

The Plant Operations Manager must report the following metrics to the Chief Operating Officer on the annual review cycle and at any time the Chief Operating Officer requests:

- Number of critical services with a current, exercised continuity plan;
- Number of exercises completed on schedule versus planned;
- Percentage of required plan reviews completed on time;
- Number of reviewed exceptions that have passed their expiry date;
- Number of material control failures identified and number of overdue corrective actions.

10. Plan Maintenance and Review

10.1 Annual review

The Plant Operations Manager must review all continuity plans and the BIA annually. The Quality Manager must participate in the review of plans affecting the quality records system. The Chief Operating Officer must review and record the outcome of the annual review before any revised plans take effect.

10.2 Triggered review

The Plant Operations Manager must initiate an unscheduled review of any affected plan when:

- A critical service, its dependencies or its supplier arrangements change materially;

- An exercise identifies a material weakness;
- A real disruption occurs and the plan is activated;
- A critical supplier notifies Halden Precision Manufacturing of a change to its systems, software or support model.

A triggered review must be completed and the Chief Operating Officer's review recorded within a timeframe set by the Plant Operations Manager at the time of the trigger. Halden Precision Manufacturing must set this timeframe; 30 days from the triggering event is offered as a starting point and is not derived from an external framework requirement.

10.3 Version control

Every plan must carry a version number, the date of the last review, and the name of the reviewer. Superseded versions must be retained in accordance with the Records Retention and Disposal Policy.

11. Exceptions

A request to operate outside a requirement of this policy must be submitted to the Plant Operations Manager with a written justification, an assessment of the residual risk, and a proposed expiry date. The Chief Operating Officer must review and record every exception before it takes effect. No exception is open-ended: every exception must carry an expiry date. The Plant Operations Manager must track all open exceptions and report any exception that has passed its expiry date to the Chief Operating Officer as an overdue item in the metrics reported under Section 9.5.

12. Relationship to Other Policies and Procedures

This policy operates alongside the following instruments in Halden Precision Manufacturing's governance framework:

- **Information Security Policy:** Governs the security controls that protect the systems and data on which critical services depend.
- **Third-Party Risk Management Policy:** Governs the broader framework for managing critical supplier risk, including contract requirements and ongoing monitoring.
- **Records Retention and Disposal Policy:** Governs the retention periods for BIA records, continuity plans, exercise records and exception records produced under this

policy.

- **Privacy and Personal Information Policy:** Governs the handling of personal information that may be involved in continuity activities.
- **Data Classification and Handling Standard:** Governs backup and handling requirements for information assets by classification level.
- **Security Incident Response Procedure and AI Incident Response Procedure:** Govern the response to disruptions with a security or AI dimension; continuity plans must be consistent with those procedures.
- **AI Risk Management Standard and AI Governance and Accountability Policy:** Govern AI-specific risks relevant to the vision system and maintenance analytics provider.

This policy does not restate the requirements of those instruments. Where a continuity obligation requires action under a sibling instrument, the Plant Operations Manager is responsible for ensuring the two are aligned.

13. Compliance and Consequences

Compliance with this policy is mandatory for all employees and contractors within scope. The Plant Operations Manager is responsible for monitoring compliance and reporting material failures to the Chief Operating Officer. Failure to maintain a current continuity plan, failure to exercise plans on schedule, and failure to act on material weaknesses are each reportable failures under this policy. Individuals who do not follow continuity arrangements when activated may be subject to Halden Precision Manufacturing's disciplinary process.

14. Governing Law

This policy is governed by the laws of Ontario, Canada. Halden Precision Manufacturing's legal reviewers must confirm which applicable Ontario and federal legislation imposes continuity, notification or record-keeping obligations relevant to precision manufacturing operations, and must ensure this policy and its supporting plans remain consistent with those obligations. The information supplied for this document does not specify the applicable statutes, and no statutory requirements have been stated in this policy as a result.

15. Document Control

Field	Detail
Document title	Business Continuity Policy
Document type	Policy
Owner	Plant Operations Manager
Review authority	Chief Operating Officer
Reviewer	Quality Manager
Review cycle	Annual
Version	1.0
Review date	To be set on first Chief Operating Officer review

Owner review items

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

Type	Detail	Where
gap	The organisation's physical locations are not specified. Section 7.2 requires facility continuity plans, but no alternative facility or work location has been identified. The Plant Operations Manager must supply this information before the facility continuity plans can be completed.	Section 7.2 — Facilities
gap	No applicable Ontario or federal statutes governing business continuity, notification or record-keeping for precision manufacturing operations were supplied. The document does not name any statute. Legal reviewers should confirm which instruments apply — candidates may include applicable Ontario occupational health and safety legislation, federal or provincial environmental requirements, and any sector-specific regulation — but this advisory is for legal review only and no statutory content has been incorporated.	Section 14 — Governing Law
gap	The triggered-review completion timeframe (30 days) is an organisational parameter offered as a starting point. Halden Precision Manufacturing must set and record this value before the policy takes effect.	Section 10.2 — Triggered review
gap	The exercise cycle is stated as annual, consistent with the customer's answer. The policy requires the Plant Operations Manager to document a risk-based rationale for the cycle assigned to each plan. That rationale does not yet exist and must be produced as part of the first BIA review.	Section 9.1 — Exercise requirement
gap	The Records Retention and Disposal Policy governs retention periods for BIA records, continuity plans, exercise records and exception records. This document does not state retention periods because the text of that sibling policy was not supplied. The Plant Operations Manager must confirm that the Records Retention and Disposal Policy covers these record classes and, if not, must initiate an update to that policy.	Sections 6, 9.3, 10.3
vague	The customer's answers do not specify alternative production arrangements or named alternate personnel for each shift. Section 7.2 (facilities) and Section 7.2 (people) require these to be named in the continuity plans. The Plant Operations Manager must supply this detail at the plan level.	Section 7.2 — People and Facilities
gap	The AI Risk Management Standard and AI Governance and Accountability Policy are referenced as governing AI-specific risks for the vision system and maintenance analytics provider. This document has not asserted what those instruments require, as their text was not supplied. The Plant Operations Manager must confirm that the continuity plans for the vision system and maintenance analytics provider are consistent with those instruments.	Section 12 — Relationship to Other Policies and Procedures

Information the organization must supply

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

- The physical location or locations of Halden Precision Manufacturing's facilities, and any identified alternative facilities or work locations, so that the facility continuity plans required by Section 7.2 can be completed.
- Legal review confirming which Ontario and federal statutes impose continuity, notification or record-keeping obligations on Halden Precision Manufacturing's precision manufacturing operations, so that Section 14 can be updated with accurate statutory references if required.
- A decision on the triggered-review completion timeframe in Section 10.2. Thirty days from the triggering event is offered as a starting point and is not a framework requirement. The Chief Operating Officer must review and record the chosen value before the policy takes effect.
- Named alternate personnel for each production shift and for on-call controls support, to be recorded in the continuity plans for production line control and the quality records system.
- Confirmation that the Records Retention and Disposal Policy covers BIA records, continuity plans, exercise records and exception records. If it does not, an update to that policy must be initiated.
- A risk-based rationale for the exercise cycle assigned to each critical service plan, to be documented by the Plant Operations Manager as part of the first BIA review.
- Confirmation that the continuity plans for the vision system vendor and the maintenance analytics provider are consistent with the AI Risk Management Standard and the AI Governance and Accountability Policy.
- The version number and first review date to be entered in the Document Control table in Section 15 once the Chief Operating Officer has completed the initial review.

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.