

Specimen — illustrative example

Corbin Freight Systems 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.

AI Risk Management Standard

Corbin Freight Systems

Document type	standard	Version	1.0 Draft
Owner	Director of Safety and Compliance	Customer decision role	Chief Operating Officer
Effective date	Upon customer release	Review cycle	Annual
Framework basis	RiskWoven AI practical best practices		
Jurisdiction	Ontario and Quebec, Canada		
Prepared for	Corbin Freight Systems	Industry	Freight and logistics
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 standard establishes the mandatory controls for assessing, testing, reviewing and monitoring AI-related risk at Corbin Freight Systems. It implements the risk management

requirements of the AI Governance and Accountability Policy and applies to every AI system used in Corbin Freight operations, whether developed internally, procured from a vendor or embedded in a third-party service.

2. Scope

This standard applies to:

- a) All AI systems that process Corbin Freight data or influence Corbin Freight decisions, including the in-cab driver behaviour detection system, the route-planning model and any future AI capability.
- b) All personnel who propose, develop, procure, operate or oversee AI systems.
- c) All third-party AI services assessed under the Third-Party AI Review Procedure.

The standard does not replace the Privacy and Personal Information Policy, the Information Security Policy or the collective agreement. Where those instruments impose a stricter requirement, the stricter requirement governs.

3. Definitions

3.1 AI risk: The possibility that an AI system causes harm to individuals, to Corbin Freight operations, to regulatory standing or to public trust. Harm includes physical safety consequences, privacy violations, unfair treatment of employees, inaccurate outputs that affect decisions and reputational damage.

3.2 Impact: The severity of harm if a risk materialises. This standard assesses impact on two axes held separately: road safety impact and employee impact. The higher of the two ratings governs the overall impact rating.

3.3 Likelihood: The probability that a risk will materialise within the assessment period, considering the frequency of the activity, the effectiveness of existing controls and relevant incident history.

3.4 Evaluation: A structured assessment of an AI system against the criteria in this standard, producing a documented risk rating, a set of required controls and a review decision.

3.5 Drift: A change in an AI system's behaviour or performance over time, whether caused by changes in input data, model updates, environmental factors or degradation of underlying

assumptions.

3.6 Residual risk: The risk that remains after all required controls are in place and operating effectively. Residual risk is accepted, transferred or further mitigated; it is never ignored.

4. Roles and Responsibilities

4.1 Director of Safety and Compliance owns this standard, maintains the AI risk register and ensures evaluations are completed on schedule.

4.2 Chief Operating Officer holds review authority for high-risk AI systems and for any exception to this standard.

4.3 System Owner is the named individual accountable for each AI system. The System Owner initiates evaluations, implements required controls and reports monitoring results.

4.4 Safety Supervisor reviews triggered driver behaviour events before any event is recorded against a driver, as required by Section 8.5.

4.5 Privacy Lead advises on privacy risk and confirms alignment with the Privacy and Personal Information Policy.

4.6 Information Security Lead advises on security risk and confirms alignment with the Information Security Policy and the Data Classification and Handling Standard.

5. AI System Documentation Requirements

Before an AI system enters production use, the System Owner must document the following in the AI risk register:

5.1 Intended purpose: A plain-language statement of what the system does and the business objective it serves. For the in-cab behaviour detection system, this includes detecting distraction, following distance and seatbelt use to support coaching conversations.

5.2 Affected people: The individuals whose data the system processes or whose circumstances the system influences. For driver-facing systems, this includes all drivers operating vehicles equipped with the technology.

5.3 Benefits: The expected positive outcomes, stated in terms a reviewer can later verify. For the behaviour detection system, this includes reduced collision risk and structured coaching

input.

5.4 Limitations: Known constraints on the system's accuracy, applicability or reliability. This includes environmental conditions that degrade detection, categories of behaviour the model does not detect and any population for whom performance differs.

5.5 Foreseeable misuse: Uses the system was not designed for but could plausibly be put to, and the harm that would result. For the behaviour detection system, foreseeable misuse includes browsing footage without a triggered event, using scores for compensation or termination decisions and exporting footage for vendor model training.

5.6 Data inputs and outputs: The categories of data the system ingests, the outputs it produces and the downstream systems or decisions those outputs feed. For the behaviour detection system, inputs include driver video and vehicle telemetry; outputs include behaviour events and a driver behaviour score.

6. Risk Assessment Requirements

6.1 Every AI system must undergo a documented risk evaluation before production use and on the reassessment triggers in Section 11.

6.2 The evaluation must assess risk across the following domains:

- a) Data risk: The sensitivity of data processed, the adequacy of data quality controls and the consequences of data loss, corruption or unauthorised access. Driver video and behaviour events are classified as the most sensitive category at Corbin Freight.
- b) Privacy risk: The collection, use and disclosure of personal information, alignment with the Privacy and Personal Information Policy and compliance with applicable Ontario and Quebec privacy law. The Privacy Lead must confirm this assessment.
- c) Security risk: Threats to confidentiality, integrity and availability, alignment with the Information Security Policy and the Data Classification and Handling Standard. The Information Security Lead must confirm this assessment.
- d) Fairness risk: The potential for the system to treat individuals or groups inequitably, including differential accuracy across driver populations and the use of outputs in employment-related decisions.

e) Accuracy risk: The consequences of incorrect outputs, the system's known error rates and the adequacy of mechanisms to detect and correct errors.

f) Transparency risk: The ability of affected individuals and reviewers to understand how the system reaches its outputs, and the adequacy of notice provided to affected individuals.

g) Human-oversight risk: The adequacy of human review before consequential decisions, the ability of human reviewers to override or correct system outputs and the risk that human reviewers defer inappropriately to system outputs.

6.3 For each domain, the evaluation must rate likelihood and impact. Impact is rated on two axes: road safety and employee impact. The higher of the two governs the overall impact rating for that domain.

6.4 The overall risk rating for the system is the highest domain rating. A system that is low risk on six domains and high risk on one domain is a high-risk system.

6.5 Risk ratings use a three-level scale: Low, Medium, High. Corbin Freight Systems must define the criteria that distinguish each level; the following are offered as a starting point and are not derived from a cited framework:

- High: Harm is severe or irreversible, likelihood is more than remote, or the system influences safety-critical or employment-consequential decisions.
- Medium: Harm is material but recoverable, likelihood is moderate, and human review can catch most errors before consequence.
- Low: Harm is minor, likelihood is low, and the system does not influence safety or employment decisions.

6.6 The evaluation must identify required controls for each material risk and state the residual risk that remains after those controls are in place.

7. Acceptance Criteria and Pre-Production Testing

7.1 Before an AI system is reviewed for production use, the System Owner must define acceptance criteria that are specific, measurable and recorded in the AI risk register.

7.2 Acceptance criteria must address, at minimum:

- a) Accuracy: The minimum acceptable accuracy, precision, recall or other performance metric for the system's primary function, measured on a test set representative of Corbin Freight's operating environment.
- b) Fairness: Evidence that performance does not differ materially across relevant subgroups of affected individuals. For driver-facing systems, this includes analysis by driver tenure, route type and vehicle configuration where data permits.
- c) Robustness: Evidence that the system performs acceptably under foreseeable variations in input quality, environmental conditions and edge cases.
- d) Security: Completion of a security assessment aligned with the Information Security Policy.
- e) Privacy: Completion of a privacy impact assessment where required by the Privacy and Personal Information Policy.
- f) Human-oversight readiness: Confirmation that the human review process required by Section 8 is documented, staffed and tested.

7.3 The System Owner must conduct or commission testing sufficient to demonstrate that acceptance criteria are met. Test results, including failures and how they were addressed, must be recorded.

7.4 A system that does not meet its acceptance criteria may not proceed to production use unless the Chief Operating Officer grants a documented exception under Section 13.

8. Human Oversight Controls

8.1 Every AI system that influences decisions about individuals must have a documented human oversight process proportionate to the risk rating.

8.2 For high-risk systems, a qualified human reviewer must review the system's output before any consequential action is taken. The reviewer must have the authority, information and time to override or correct the output.

8.3 For medium-risk systems, human review may occur on a sample basis or exception basis, provided the sampling rate and exception triggers are documented and the review is completed within a timeframe set by Corbin Freight Systems.

8.4 For low-risk systems, human review may be limited to periodic audit of outputs, provided the audit frequency is documented.

8.5 Driver behaviour detection system: A Safety Supervisor must review every triggered event before the event is recorded against a driver. No disciplinary step may be taken on a model output alone. The driver behaviour score may not be used for compensation, promotion or termination decisions. These requirements implement the collective agreement and the AI Acceptable Use Policy.

8.6 Footage access: Driver video may be reviewed only on a triggered event. Browsing footage without a trigger is prohibited. Every footage retrieval must be logged with the identity of the retriever and the trigger that justified access.

8.7 The System Owner must monitor human override rates. A sustained override rate above a threshold set by Corbin Freight Systems triggers a reassessment under Section 11. Corbin Freight Systems has not yet set this threshold; 15 percent is offered as a starting point and is not derived from a cited framework.

9. Review and Recording of Residual Risk

9.1 When the evaluation is complete and acceptance criteria are met, the System Owner must prepare a review record that includes:

- a) The system name, version and intended purpose.
- b) The overall risk rating and the rating for each domain.
- c) The required controls and evidence that each is in place.
- d) The residual risk that remains after controls, stated in terms a reviewer can understand.
- e) The monitoring requirements from Section 10.

f) The next scheduled reassessment date.

9.2 Review authority is determined by the overall risk rating:

- High-risk systems: Chief Operating Officer.
- Medium-risk systems: Director of Safety and Compliance.
- Low-risk systems: System Owner, with notification to the Director of Safety and Compliance.

9.3 The reviewer must record their decision, the date and any conditions attached. A conditional review must state the conditions, the deadline for meeting them and the consequence of missing the deadline.

9.4 A system may not enter production use until the review record is complete and the reviewer with appropriate authority has recorded their decision.

9.5 The AI risk register must retain the review record for the retention period specified in the Records Retention and Disposal Policy.

10. Ongoing Monitoring Requirements

10.1 Every AI system in production must have a documented monitoring plan proportionate to its risk rating.

10.2 The monitoring plan must specify:

a) The metrics to be tracked, including accuracy, error rates, drift indicators and human override rates.

b) The data sources for each metric.

c) The frequency of measurement. Corbin Freight Systems must set monitoring frequencies; the following are offered as starting points and are not derived from a cited framework:

- High-risk systems: Monthly metric review.
- Medium-risk systems: Quarterly metric review.
- Low-risk systems: Semi-annual metric review.

d) The thresholds that trigger escalation or reassessment.

e) The individual responsible for conducting the monitoring and the individual who receives the results.

10.3 For the driver behaviour detection system, monitoring must include:

- a) Event accuracy: The rate at which Safety Supervisors confirm or reject triggered events.
- b) Detection consistency: Analysis of whether detection rates differ materially across driver populations, route types or environmental conditions.
- c) Footage access compliance: Review of footage retrieval logs to confirm every retrieval has a documented trigger.
- d) Data residency: Confirmation that no footage has left Canada and no footage has been provided for vendor model training.

10.4 Monitoring results must be recorded. Results that breach a threshold must be escalated to the Director of Safety and Compliance within a timeframe set by Corbin Freight Systems.

10.5 The Director of Safety and Compliance must report monitoring status to the Chief Operating Officer on a cycle set by Corbin Freight Systems; quarterly is offered as a starting point.

11. Reassessment Triggers

11.1 A full reassessment under Section 6 is required when any of the following occurs:

- a) Material change: A change to the system's model, training data, input sources, output uses or affected population that could alter the risk profile.
- b) Incident: An incident involving the system that is reportable under the AI Incident Response Procedure, the Security Incident Response Procedure or the Privacy Breach Response Procedure.
- c) Performance degradation: Monitoring results that breach a threshold defined in the monitoring plan, or a sustained human override rate above the threshold in Section 8.7.
- d) New obligation: A change in law, regulation, collective agreement or contractual commitment that affects the system's compliance posture.

e) Scheduled reassessment: The reassessment date recorded in the review record. Corbin Freight Systems conducts annual reviews; the next reassessment must occur no later than 12 months after the previous review decision.

11.2 The System Owner must initiate the reassessment within a timeframe set by Corbin Freight Systems after the trigger is identified. Corbin Freight Systems has not yet set this timeframe; 30 calendar days is offered as a starting point.

11.3 If a reassessment cannot be completed within the required timeframe, the System Owner must notify the Director of Safety and Compliance and document the reason and the revised completion date.

11.4 A system that fails reassessment must be suspended from production use or granted an exception under Section 13.

12. Metrics and Reporting

12.1 The Director of Safety and Compliance must track and report the following metrics:

- a) High-risk assessments reviewed before use: The percentage of high-risk AI systems that received Chief Operating Officer review before entering production.
- b) Monitoring tests completed on schedule: The percentage of scheduled monitoring reviews completed by their due date.
- c) Required reviews completed on time: The percentage of scheduled reassessments completed by their due date.
- d) Exceptions past expiry: The number of exceptions granted under Section 13 that have passed their expiry date without resolution.
- e) Material control failures and overdue corrective actions: The number of control failures identified through monitoring or incident and the number of corrective actions that remain open past their due date.

12.2 Metrics must be reported to the Chief Operating Officer on a cycle set by Corbin Freight Systems; quarterly is offered as a starting point.

12.3 Metrics must be retained for the period specified in the Records Retention and Disposal Policy.

13. Exceptions

13.1 An exception to any requirement in this standard may be granted only by the Chief Operating Officer.

13.2 An exception request must document:

- a) The specific requirement to be excepted.
- b) The business justification.
- c) The risk accepted by granting the exception.
- d) The compensating controls, if any.
- e) The proposed expiry date. Exceptions must have a defined duration; indefinite exceptions are not permitted.

13.3 The Chief Operating Officer must record the decision, the conditions and the expiry date.

13.4 The Director of Safety and Compliance must track all open exceptions and report any that have passed their expiry date in the metrics under Section 12.

13.5 An exception that has passed its expiry date without renewal or resolution is a control failure and must be escalated to the Chief Operating Officer.

14. Collective Agreement and Union Notification

14.1 Driver video and derived behaviour events are subject to the collective agreement. This standard does not modify collective agreement obligations.

14.2 The union must be notified of any change to the detection categories used by the driver behaviour detection system before the change is deployed.

14.3 The Director of Safety and Compliance must maintain a record of union notifications and confirmations.

15. Data Residency and Vendor Restrictions

15.1 Driver video and behaviour events must remain within Canada at all times. No footage may be transferred outside Canada for any purpose.

15.2 No driver video or behaviour event data may be provided to any vendor for the purpose of training a vendor model.

15.3 The System Owner must confirm compliance with these requirements as part of the monitoring in Section 10.

15.4 A violation of Section 15.1 or 15.2 is a reportable incident under the AI Incident Response Procedure and the Privacy Breach Response Procedure.

16. Record Retention

16.1 AI risk evaluations, review records, monitoring results and exception records must be retained for the period specified in the Records Retention and Disposal Policy.

16.2 Footage retrieval logs must be retained for a period set by Corbin Freight Systems; 2 years is recommended as a starting point.

16.3 Unreviewed driver video is overwritten on a rolling 30-day cycle. Video associated with a triggered event that has been reviewed and recorded follows the retention period for safety records in the Records Retention and Disposal Policy.

16.4 Technical logs from the telematics platform and AWS must be searchable for a period set by Corbin Freight Systems; 90 days is recommended as a starting point.

17. Related Documents

This standard implements and must be read with:

- AI Governance and Accountability Policy
- AI Acceptable Use Policy
- Privacy and Personal Information Policy
- Information Security Policy
- Data Classification and Handling Standard
- Third-Party Risk Management Policy
- Third-Party AI Review Procedure

- AI Incident Response Procedure
- Security Incident Response Procedure
- Privacy Breach Response Procedure
- Records Retention and Disposal Policy

18. Review and Maintenance

18.1 The Director of Safety and Compliance owns this standard and is responsible for its maintenance.

18.2 This standard must be reviewed annually or when a material change in law, regulation, technology or organisational structure affects its requirements.

18.3 Amendments require review 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	The information supplied does not include verified framework text. All requirements in this standard are derived from RiskWoven AI practical best practices and the organisation's stated practices, not from a cited external framework. No control identifiers are available to cite.	Entire document
gap	The organisation has not defined the specific criteria that distinguish Low, Medium and High risk ratings. Section 6.5 offers a starting point that must be confirmed or replaced by Corbin Freight Systems.	Section 6.5
gap	The organisation has not set the human override rate threshold that triggers reassessment. Section 8.7 offers 15 percent as a starting point.	Section 8.7
gap	The organisation has not set monitoring frequencies. Section 10.2(c) offers monthly, quarterly and semi-annual as starting points by risk level.	Section 10.2
gap	The organisation has not set the timeframe for initiating reassessment after a trigger. Section 11.2 offers 30 calendar days as a starting point.	Section 11.2
gap	The organisation has not set the escalation timeframe for monitoring breaches. Section 10.4 requires this to be defined.	Section 10.4

gap	The organisation has not set the reporting cycle for metrics and monitoring status. Sections 10.5 and 12.2 offer quarterly as a starting point.	Sections 10.5, 12.2
gap	The retention period for AI risk evaluations, review records and exception records is deferred to the Records Retention and Disposal Policy. Corbin Freight Systems must confirm that policy specifies a period for these record types.	Section 16.1
gap	The footage retrieval log retention period and technical log searchability period in Sections 16.2 and 16.4 are recommendations only. Corbin Freight Systems must set these as organisation-defined parameters.	Sections 16.2, 16.4
vague	The standard references 'applicable Ontario and Quebec privacy law' without naming specific statutes. Corbin Freight Systems' legal advisors should confirm which provincial and federal privacy legislation applies to driver video and employee data in the freight and logistics context.	Section 6.2(b)
gap	The standard references the collective agreement but does not have access to its text. Corbin Freight Systems must verify that Sections 8.5, 8.6 and 14 align with the actual collective agreement provisions.	Sections 8.5, 8.6, 14

Information the organization must supply

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

- Specific criteria distinguishing Low, Medium and High risk ratings (Section 6.5 offers a starting point).
- Human override rate threshold that triggers reassessment (Section 8.7 offers 15 percent as a starting point).
- Monitoring frequencies for high, medium and low-risk systems (Section 10.2(c) offers monthly, quarterly and semi-annual as starting points).
- Timeframe for initiating reassessment after a trigger is identified (Section 11.2 offers 30 calendar days as a starting point).
- Escalation timeframe for monitoring results that breach a threshold (Section 10.4).
- Reporting cycle for metrics and monitoring status to the Chief Operating Officer (Sections 10.5 and 12.2 offer quarterly as a starting point).
- Confirmation that the Records Retention and Disposal Policy specifies retention periods for AI risk evaluations, review records and exception records.
- Organisation-defined footage retrieval log retention period (Section 16.2 recommends 2 years as a starting point).

- Organisation-defined technical log searchability period (Section 16.4 recommends 90 days as a starting point).
- Legal confirmation of which provincial and federal privacy legislation applies to driver video and employee data.
- Verification that Sections 8.5, 8.6 and 14 align with the actual collective agreement provisions regarding driver monitoring and union notification.

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