GOVERNED TEMPLATE RENDERING REFERENCE: COMPLIANCE CONTROL MATRIX DEFAULT V2 (DRAFT)

definition f438bd65…cc0f

COMPLIANCE CONTROL MATRIX · PROJECT ARTIFACT

SPECIRA

Compliance Control Matrix: Dispatch Modernization

Meridian Field Services: instructional example, not project evidence

DRAFT · WATERMARK POLICY: DRAFT_ONLY

template compliance_matrix v2 · pack: specira_default_delivery

the matrix links obligation to proof · the siblings implement

§1 Applicable Regulations

mandatory | 1 decision | 1 evidence rule

validators: applicable_regulation_set_has_named_determiner_and_rationale · regimes_classed_mandatory_or_elected · exclusions_carry_rationale

Scoping is a decision, not a lookup: a lawyer-adjacent judgment with a named determiner. Over- and under-inclusion both create exposure, so the ruled-out list is part of the decision.

Determined by: outside counsel with N. Duval, July 8; sponsor informed (applicability memo[1]).

Regime	Class	Why it applies (this footprint)
Federal private-sector privacy law	MANDATORY	Personal data of employees in a federally regulated transport-adjacent fleet; counsel's memo attached
Provincial employment standards (monitoring notice)	MANDATORY	Staff monitoring at the Ontario workplace
Collective agreement: monitoring clauses	MANDATORY	Binding by contract force at the represented hub

Regime	Class	Why it applies (this footprint)
Enterprise customer contract: security schedule	`elected`	Clause 14 retention, clause 18 audit rights; contract-driven
SOC 2-shaped shared control set	`elected`	One control set serves the privacy law, the contract schedule, and future procurement at once (the middle-layer rationale)

Excluded, with rationale: payment-card standards (no cardholder data anywhere in scope, per entities[2]); health-privacy regimes (the classification register's special-category column says none, per PII register[3]). **Re-scoping triggers**: a new jurisdiction hub, a new data class entering the register, a customer segment with its own regime.

§2 Control Mapping

mandatory · 1 decision · 1 evidence rule

validators: every_control_cites_implementing_mechanism_by_id · no_duplicate_control_across_mapped_regulations · every_control_names_evidence_artifact_and_cadence · every_gap_has_remediation_owner_and_date

One shared control set: many obligations cite one control. Mechanisms are citations; a control that re-described SR-004 would drift the day SR-004 changed.

Control	Cited by (clauses)	Mechanism (by id)	Evidence · cadence	Mode
CTL-01 `access control`	Privacy-law safeguards · schedule 18.2: *one control, two obligations*	permission model[4] · SR-004[5]	Quarterly access-review export	`continuous` : role-change audi events (audit events[4])
CTL-02 `retention & disposal`	Privacy-law limitation · clause 14	retention rules[3] (cited, never restated)	Disposal-job log · monthly	`periodic`
CTL-03 `monitoring notice`	Employment standards · collective agreement	The dispatcher-facing notice	Published notice + acknowledgments	`periodic`

Control	Cited by (clauses)	Mechanism (by id)	Evidence · cadence	Mode
		(consent model[3])		
`CTL-04` encryption	Privacy safeguards · schedule 18.4	SR-024, SR-025[5]	Platform configuration export	`continuous` : the drift check (environments[6]
`CTL-05` audit trail	Schedule 18.6 · privacy-law accountability	SR-030, SR-031[5] · audit events[4]	Append-only audit stream · 2-y retention per retention rules[3]	`continuous`

Gap	Remediation	Owner	Target
`CTL-03 partial`	Union co-signature review of the notice (RSK-07[7])	N. Duval	`Aug 8, 2026`

§3 Audit Requirements

mandatory · 1 decision · 1 evidence rule

validators: audit_window_and_access_plan_stated · evidence_exists_before_audit_window_not_promised · findings_route_to_existing_trackers

Audit-ready means the evidence exists before the request list lands, into a folder that is already full.

Fact	Value
Basis	Enterprise contract schedule 18: annual customer audit, Type-II-shaped
Observation window	`Six months ending Sep 30`
Fieldwork	`Two weeks, October`
Access	Named customer auditor: audit stream (read-only), access-review exports, three control owners for walkthroughs; **production data access denied by design**; evidence exports substitute (agreed with the customer July 10)
Findings route	Into the §2 gap table and, where material, the risk register by id (governance[7]); no new tracker for audit season

§4 Open Questions

mandatory 1 decision

Question	Owner	Answer by	Blocks
Does the SOC 2-shaped elected control set formalize into an actual Type II engagement for enterprise sales next fiscal year? (Commercial decision with audit-cost implications.)	The sponsor with N. Duval	Nov 1, 2026	Nothing in the current matrix

Refs References & Package Contents

In this export package

package [1] Counsel's applicability memo ./compliance/applicability-memo.pdf

In the Specira workspace

specira [2] Data model: entities (no cardholder data) app.specira.ai/projects/dispatch-modernization/artifacts/data-model

specira [3] Data classification: PII register, retention rules, consent model app.specira.ai/projects/dispatch-modernization/artifacts/data-classification

specira [4] Auth & authz policy: permission model, audit events app.specira.ai/projects/dispatch-modernization/artifacts/auth-authz-policy

specira [5] Security requirements: SR-004, SR-024, SR-025, SR-030, SR-031 app.specira.ai/projects/dispatch-modernization/artifacts/security-requirements

specira [6] Infrastructure & deployment: the drift check app.specira.ai/projects/dispatch-modernization/artifacts/infrastructure-deployment#environments

specira [7] Risk register: RSK-07; governance rules app.specira.ai/projects/dispatch-modernization/artifacts/risk-register

Generated by Specira · template compliance_matrix v2 (draft) · pack specira_default_delivery lineage f438bd65…cc0f · page 1 of 4