PRACTITIONER REFERENCE

The 20-Domain Control Universe

Framework Linkage, Explained — Provision-by-Provision Detail & Worked Examples

---

This companion guide expands each of the 20 governance domains from the “AI Governance Audit — End-to-End Methodology & Process” deck. For every domain, each linked EU AI Act article, ISO/IEC 42001 clause, NIST AI RMF function and OECD principle — plus two national crosswalks, Canada (AI for All, Bill C-36, OSFI Guideline E-23) and India (RBI FREE-AI Framework and Draft Guidance on Model Risk Management, 2026) — is explained as its own short paragraph, followed by a worked example broken into the 5C finding elements (Condition, Criteria, Cause, Consequence, Corrective action). Examples are fictional, illustrative composites in the style of the deck’s “Meridian Bank” scenario.

EU AI Act	ISO/IEC 42001	NIST AI RMF	OECD Principles	Canada	India (RBI)
Binding EU law	AI management system	Risk framework	Values baseline	Strategy + law + regulation	Framework + draft MRM rule

Presented by Arindam Pal — AI Governance · Audit · Assurance

PART IV SUPPLEMENT · NATIONAL FRAMEWORK CROSSWALK

Canada’s AI Governance Framework

“A strategy to lead, a law to protect, and a regulation to govern risk.” — how this guide integrates Canada’s three-instrument model into the 20-domain control universe.

Instrument	Role	Issuer / Date	Focus
AI for All	The Strategy — to lead	ISED / Government of Canada Launched Jun 4, 2026	National 5-year strategy; $3.5B+ investment; six pillars incl. CAISI, sovereign compute, literacy.
Bill C-36 (PPCDA)	The Law — to protect	Parliament of Canada Introduced Jun 15, 2026	Enforceable privacy rights, consent, deletion, automated-decision transparency, surveillance-pricing ban.
OSFI Guideline E-23	The Regulation — to govern risk	OSFI Final Sep 11, 2025 · Effective May 1, 2027	Binding model risk management for all FRFIs — full lifecycle, AI/ML-specific risks, vendor models.

HOW THIS GUIDE USES THE CANADA CROSSWALK

Each domain page carries a Canada crosswalk tag alongside the EU AI Act, ISO/IEC 42001, NIST AI RMF and OECD references, and a corresponding short paragraph in “What each provision requires.” Most domains map to OSFI Guideline E-23, Canada’s binding model risk management standard for federally regulated financial institutions (FRFIs) — full lifecycle governance, board/senior-management accountability, named AI/ML-specific risks, third-party vendor accountability, and risk-based proportionality.

Domains touching personal data, consent, pricing fairness, or a customer’s right to an explanation draw instead — or additionally — on Bill C-36, which establishes privacy as a fundamental right, mandates automated decision-making transparency, and bans discriminatory surveillance pricing, enforced by the Digital Safety and Data Protection Commission with penalties up to $25M or 5% of global revenue. Domains touching oversight capacity, model evaluation, or agentic/GenAI systems also draw on AI for All’s CAISI expansion and its 2026–2031 strategic horizon.

WHY ALL THREE, TOGETHER

Without AI for All…	the regulatory instruments lack a policy rationale, and E-23 loses the economic context that motivates genuine investment in governance capacity.
Without Bill C-36…	citizens have no enforceable protection as AI-driven decisions multiply — a national strategy without enforceable law is aspiration without accountability.
Without E-23…	systemic financial risk from AI model failure goes ungoverned — a privacy law without a sectoral risk framework leaves high-risk AI ungoverned in critical infrastructure.

Sources: Canada.ca, Parliament of Canada, OSFI (as of June 2026). This crosswalk is a companion mapping prepared for audit purposes and is not legal advice.

PART IV SUPPLEMENT · NATIONAL FRAMEWORK CROSSWALK

India’s AI Governance Framework — RBI

From a principles-based blueprint to a binding model-risk rulebook — how this guide integrates RBI’s evolving AI governance regime into the 20-domain control universe.

Instrument	Role	Issuer / Date	Focus
FREE-AI Framework	The Blueprint — to enable, responsibly	RBI Committee (const. Dec 2024) Report released Aug 13, 2025	7 Sutras, 6 pillars, 26 recommendations balancing AI innovation with consumer & systemic safeguards.
Draft Guidance on Model Risk Management, 2026	The Regulation — to govern model risk	RBI, Dept. of Regulation Released Jun 24, 2026	Board-owned MRMF, 3 lines of defence, model tiering, and a dedicated AI/ML chapter for all Regulated Entities (REs).

HOW THIS GUIDE USES THE INDIA (RBI) CROSSWALK

Each domain page now also carries an India tag, referencing whichever of the two RBI instruments is most relevant: the FREE-AI Framework (Aug 2025) — a principles-based report built on seven “Sutras” (Trust, People First, Innovation, Fairness, Accountability, Explainability, Resilience) and six pillars (Infrastructure, Policy, Capacity, Governance, Protection, Assurance) — and the Draft Guidance on Regulatory Principles for Model Risk Management, 2026, released for public consultation on June 24, 2026 (comments closed July 24, 2026; final guidance and effective date not yet notified as of this guide’s publication).

The Draft MRM Guidance applies to all RBI-regulated entities (REs) — commercial, small finance, payments and co-operative banks, NBFCs, HFCs, All India Financial Institutions, ARCs and credit information companies — and covers any model, including AI/ML, whether built internally, bought from a vendor, or a mix. It requires a Board-approved Model Risk Management Framework (MRMF), a three-lines-of-defence structure, risk-based model tiering, and a dedicated AI chapter naming seven risk dimensions (explainability, hallucinations, bias, overfitting, spurious correlations, output variability, data risks) alongside kill-switch, human-oversight and customer-disclosure mandates — arguably the most prescriptive AI-specific technical requirements of any framework in this guide.

WHAT MAKES THE RBI APPROACH DISTINCTIVE

Kill-switch mandate	An explicit, named requirement to be able to override, suspend or deactivate any AI model immediately — stated more concretely than the EU AI Act’s Art. 14 “stop” function.
10-year retention	Decommissioned models must be retained for 10 years, roughly 20x the EU AI Act’s 6-month minimum log-retention baseline.
No vendor safe-harbour	REs are told plainly they cannot rely on a vendor’s safety certificate — independent validation of third-party AI is mandatory, not best practice.
Still in draft	Unlike E-23 (already final), the RBI Draft MRM Guidance remains a consultation document — institutions should treat its provisions as a strong signal of coming obligations, not yet binding law.

Sources: RBI FREE-AI Committee Report (Aug 2025); RBI Draft Guidance on Regulatory Principles for Model Risk Management, 2026 (Press Release 2026-2027/528, Jun 24, 2026), as of Aug 2026. This crosswalk is a companion mapping prepared for audit purposes and is not legal advice; the Draft MRM Guidance is not yet finalised and its provisions may change before issuance.

DOMAIN 01 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Governance & Accountability

EU AI Act: Arts. 4, 17, 26, 27 | ISO/IEC 42001: Cl. 4–10 (5.1–5.3) | NIST AI RMF: GOVERN | OECD: Accountability (1.5) | Canada: OSFI E-23 (Board Oversight) + AI for All (CAISI) | India: RBI Draft MRM Guidance 2026 (Board-Approved MRMF)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 4	Requires organisations to ensure staff and others operating AI systems have sufficient "AI literacy" — the people running the system must understand it well enough to use it responsibly.
EU AI Act — Arts. 17, 26, 27	Art. 17 requires providers of high-risk systems to run a quality management system. Arts. 26–27 push deployer-side duties — human-oversight assignment and, for certain deployers, a fundamental-rights impact assessment — onto the bank as the entity actually using the model in production.
ISO/IEC 42001 — Cl. 4–10	Requires context-of-the-organisation analysis, leadership commitment, resourcing, and a documented AI management system (AIMS) subject to internal audit and management review — much like an existing ISO 27001 or SOX control environment.
NIST AI RMF — GOVERN	The umbrella function: it asks whether policies, roles and culture exist before any technical testing starts. A bank that tests bias metrics on one model without board-level ownership of AI risk has not actually reduced its exposure.
Canada — OSFI E-23 & AI for All	OSFI Guideline E-23 requires board-level risk committees to govern model risk and senior management to run enterprise-wide model risk management proportional to size and complexity; AI for All's Pillar 1 backs this with $50M to expand the Canadian AI Safety Institute (CAISI) for research, model evaluations and monitoring.
India — RBI Draft MRM Guidance, 2026	Requires every regulated entity to adopt a Board-approved Model Risk Management Framework (MRMF) with explicit Board, Risk Management Committee and senior-management accountability, operated through a strict three-lines-of-defence structure (model owners, independent validation, internal audit) — echoing FREE-AI's Governance pillar, which calls for clear accountability on the part of deploying entities.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	At a mid-size retail bank, the audit requested the AI governance policy and interviewed the digital channels team about three live GenAI chatbot deployments.
Condition:	The AI governance policy existed but had not been reviewed or re-approved by the board in over 18 months, and no named individual held Art. 17-style accountability for the three chatbots.
Criteria:	EU AI Act Art. 26 deployer obligations and ISO 42001 Cl. 5.3 (assignment of roles and authorities).
Cause:	The governance policy predates the GenAI rollout and was never updated when the chatbots were launched by the digital channels team without model-risk sign-off.
Consequence:	No one can attest to conformity if a regulator asks; accountability for three live customer-facing systems is effectively absent.
Corrective action:	Appoint an accountable executive for GenAI and refresh the governance charter within 90 days. Rated High.

DOMAIN 02 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Inventory & Classification

EU AI Act: Arts. 9, 17, 18; Annex IV | ISO/IEC 42001: Cl. 6, 8 | NIST AI RMF: MAP, GOVERN | OECD: Accountability (1.5) | Canada: OSFI E-23 (Expanded Model Definition) | India: RBI Draft MRM Guidance 2026 (Model Inventory & Tiering)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 9	A risk-management system must start from identifying and analysing known and foreseeable risks — impossible without a complete inventory of every AI system in use.
EU AI Act — Arts. 17–18; Annex IV	Require providers of high-risk systems to maintain detailed technical documentation per system, effectively forcing a system-by-system record covering credit scorecards, fraud models, GenAI copilots and embedded vendor AI.
ISO/IEC 42001 — Cl. 6, 8	Planning (Cl. 6) and operational control (Cl. 8) require the AIMS to identify all AI systems within scope and classify each by risk tier.
NIST AI RMF — MAP	Is explicitly about establishing context and cataloguing use cases before risk can be measured or managed — the Act's risk tiers (unacceptable, high-risk, limited-risk, minimal-risk) map onto this same cataloguing exercise.
Canada — OSFI E-23	E-23's expanded model definition captures any theoretical, empirical, statistical or AI/ML method that generates predictions, recommendations or decisions — every model must be inventoried and classified regardless of its approval category or methodology, closing the "it's just a spreadsheet" loophole.
India — RBI Draft MRM Guidance, 2026	Mandates a comprehensive inventory of every model — active, inactive, under-development and retired — broadly defined to include AI/ML systems, scoring algorithms, rule engines and even material spreadsheets that influence lending or pricing decisions, each classified into a risk tier reviewed at least annually.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	At fictional "Meridian Bank," the audit reconciled the official AI inventory (41 systems) against cloud API billing data and procurement records.
Condition:	Six additional systems were found in active use that were absent from the inventory, including a marketing team's GenAI tool used to draft loan-offer copy.
Criteria:	EU AI Act Art. 9 risk-tiering requirement, which cannot be applied to systems that are never registered.
Cause:	No central gate exists requiring new AI procurement or SaaS sign-up to pass through the AI inventory process before use.
Consequence:	Unknown whether any of the six systems touch credit decisions, which would make them high-risk under Annex III with no compensating control in place.
Corrective action:	Freeze new AI procurement outside the central inventory process; run a 30-day catch-up classification sprint. Rated Critical.

DOMAIN 03 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Risk Management

EU AI Act: Art. 9 | ISO/IEC 42001: Cl. 6.1, 8.2 | NIST AI RMF: MAP, MANAGE | OECD: Robustness (1.4) | Canada: OSFI E-23 (Lifecycle & Proportionality) | India: RBI Draft MRM Guidance 2026 (Risk-Based Tiering)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 9	Requires providers and deployers of high-risk AI to establish, implement, document and maintain a risk-management system across the entire lifecycle — identifying risks from both intended use and reasonably foreseeable misuse, then mitigating and testing residual risk.
ISO/IEC 42001 — Cl. 6.1, 8.2	Cl. 6.1 requires actions addressing risks and opportunities at the AIMS level; Cl. 8.2 requires an AI-system-specific risk assessment before deployment and at defined intervals thereafter.
NIST AI RMF — MAP, MANAGE	MAP requires context and risk sources (data risk, model risk, deployment risk, societal risk) to be identified up front; MANAGE requires those risks to be prioritised, treated and monitored over time — model risk management extended to cover AI-specific failure modes like prompt injection.
Canada — OSFI E-23	Requires full lifecycle governance — design, independent validation, controlled deployment, monitoring and structured decommissioning — with governance intensity scaled under a risk-based proportionality principle to the model's inherent risk, complexity and systemic impact.
India — RBI Draft MRM Guidance, 2026	Proposes a risk-based tiering approach classifying each model by business importance, customer impact, complexity, explainability and regulatory significance, with high-risk models requiring Board Risk Committee approval and materially closer monitoring — tiering must be reviewed annually or on significant change.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	The audit pulled the risk assessment on file for a commercial-lending AI decision-support tool.
Condition:	The document was a copy-pasted risk assessment for an unrelated fraud-detection model, with only the system name changed — no unique consideration of disparate-impact risk on protected classes.
Criteria:	EU AI Act Art. 9(2), which requires risks "reasonably foreseeable" for that specific system to be assessed.
Cause:	The risk-assessment template lacks mandatory system-specific fields, and no reviewer caught the duplication before approval.
Consequence:	Material lending-bias risk may be entirely unassessed for a live credit-decisioning system.
Corrective action:	Rebuild the risk assessment from scratch with mandatory second-line reviewer sign-off before the next credit cycle. Rated High.

DOMAIN 04 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Data Governance

EU AI Act: Art. 10 | ISO/IEC 42001: Cl. 8; Annex B | NIST AI RMF: MAP, MEASURE | OECD: Transparency (1.3) | Canada: Bill C-36 (Consent; Cross-Border Transfers) | India: RBI FREE-AI (Data Risks; DPDP Act 2023)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 10	Sets detailed data-governance requirements for high-risk systems: training/validation/test data must be governed for design choices, collection, preparation (labelling, cleaning, enrichment), suitability, and examined for possible biases likely to cause discrimination, with gaps identified.
ISO/IEC 42001 — Cl. 8; Annex B	Annex B provides detailed control guidance on data quality and provenance for AI systems, tied into the organisation's broader data-management system under Cl. 8.
NIST AI RMF — MAP, MEASURE	MAP asks whether data lineage and context are understood; MEASURE requires data-quality metrics to actually be computed and tracked — not merely asserted in a model document.
Canada — Bill C-36 (PPCDA)	Requires meaningful consent through plain-language explanations of data collection, use and disclosure, and mandates robust risk assessments before personal data used to train or run a model leaves Canada in a cross-border transfer.
India — RBI FREE-AI Framework	Names data risk as one of the AI-specific risk dimensions institutions must manage, and directs entities to avoid over-collection of data and comply with the Digital Personal Data Protection Act 2023 alongside RBI's own IT and outsourcing guidelines when sourcing and preparing model training data.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	A bank's SME credit-risk model used "postal code" and "industry sector" as input features; the audit re-performed a proxy-variable check.
Condition:	Postal code was found to act as a strong proxy for a protected characteristic in a subset of urban branches; no data-governance documentation had flagged or tested for this.
Criteria:	EU AI Act Art. 10(2)(f), which explicitly requires examination for possible proxy biases in the data.
Cause:	The data-governance sign-off process does not include a mandatory proxy-variable test as part of feature approval.
Consequence:	The model may be systematically disadvantaging customers in specific urban postal areas without detection.
Corrective action:	Formal proxy-variable review across all customer-facing credit models; compensating fairness constraint or feature removal pending remediation. Rated High.

DOMAIN 05 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Bias & Fairness

EU AI Act: Arts. 9, 10, 13, 14, 15 | ISO/IEC 42001: Cl. 6, 8, 9 | NIST AI RMF: MAP, MEASURE, MANAGE | OECD: Human-centred values (1.2) | Canada: Bill C-36 (Surveillance Pricing Ban) + OSFI E-23 (Bias) | India: RBI FREE-AI (Fairness Sutra) + Draft MRM (Bias Risk)

WHAT EACH PROVISION REQUIRES

EU AI Act — Arts. 9, 10	Art. 9's risk-management system must explicitly evaluate discrimination risk; Art. 10's data-governance duties require bias examination in training data before the model is built.
EU AI Act — Arts. 13, 14, 15	Arts. 13–14 (transparency, human oversight) ensure a human can understand and intervene on a disparate outcome; Art. 15 requires accuracy and robustness that regulators read to include consistency across subgroups, not just aggregate accuracy.
ISO/IEC 42001 — Cl. 6, 8, 9	Folds fairness into planning (Cl. 6), operational controls (Cl. 8) and performance evaluation (Cl. 9) — fairness is tested continuously, not just at model sign-off.
NIST AI RMF / OECD	NIST's MEASURE requires quantitative subgroup testing, mitigated under MANAGE; the OECD's human-centred values principle anchors fairness as a values-level expectation throughout the lifecycle.
Canada — Bill C-36 & OSFI E-23	Bill C-36 introduces a surveillance-pricing ban prohibiting manipulative or discriminatory data-driven pricing, and requires disclosure whenever a significant decision is algorithmic; E-23 separately names bias among the AI/ML-specific risks FRFIs must govern.
India — RBI FREE-AI & Draft MRM Guidance	FREE-AI's "Fairness" Sutra and Protection pillar call for consumer safeguards and bias mitigation across AI-driven decisions; the Draft MRM Guidance separately names bias/discrimination as one of seven AI risk dimensions requiring active testing before and after deployment.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	For an unsecured personal-loan approval model, the audit re-ran an adverse-impact ratio test across protected age bands on a held-out sample.
Condition:	Approval rates for one age band were roughly 15 percentage points lower than the reference group — well outside the bank's own 5-point fairness tolerance — yet no fairness sign-off existed on file at all.
Criteria:	EU AI Act Art. 9 discrimination-risk evaluation and Art. 15 consistent accuracy requirement.
Cause:	Subgroup fairness testing is not a mandatory gate in the model-development lifecycle before production go-live.
Consequence:	A live model is producing a materially disparate lending outcome for an entire protected age band with no monitoring.
Corrective action:	Immediate enhanced human review of declines in the affected band; full fairness re-assessment; make subgroup testing a permanent mandatory gate. Rated Critical.

DOMAIN 06 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Model Development & Documentation

EU AI Act: Art. 11; Annex IV | ISO/IEC 42001: Cl. 7.5, 8 | NIST AI RMF: GOVERN, MAP | OECD: Transparency (1.3) | Canada: OSFI E-23 (Design & Documentation) | India: RBI Draft MRM Guidance 2026 (Model Development)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 11; Annex IV	Sets an extensive documentation standard for high-risk systems: system description and intended purpose, architecture and key design choices, data requirements, human-oversight measures, and validation/testing procedures — updated whenever the system is substantially modified.
ISO/IEC 42001 — Cl. 7.5, 8	Cl. 7.5 requires documentation to be controlled — versioned, reviewed, protected from unauthorised change; Cl. 8 requires the processes that produced the model to themselves be documented and repeatable.
NIST AI RMF — GOVERN, MAP	GOVERN treats documentation as a governance artefact demonstrating accountability; MAP treats understanding a system's design and limitations as a prerequisite to correctly assessing its risk.
Canada — OSFI E-23	Full lifecycle governance begins at the design stage, requiring documented model design decisions before independent validation and deployment — the same substantiation discipline applies uniformly to a bank's theoretical, empirical, statistical or AI/ML models.
India — RBI Draft MRM Guidance, 2026	Requires model development to start from a clearly defined objective and problem statement, with the model's interface to core banking, liquidity, ALM or other risk systems documented, and outcomes required to be "consistent, unbiased, explainable and verifiable" as part of the validation framework.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	The audit reviewed the technical documentation pack for a fraud-scoring model and conducted a code walkthrough with the development team.
Condition:	Documentation described a gradient-boosted tree architecture, but the production model had been silently replaced eight months earlier with a neural-network variant; documentation was never updated.
Criteria:	Art. 11 and Annex IV(1) currency requirements for technical documentation.
Cause:	No change-control gate requires documentation sign-off before a modified model is redeployed to production.
Consequence:	Any conformity assessment relying on the old documentation would be invalid; the "substantial modification" trigger under the Act was missed entirely.
Corrective action:	Rebuild documentation to match the live model; introduce a mandatory documentation-refresh gate in the MLOps pipeline. Rated High.

DOMAIN 07 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Model Validation

EU AI Act: Arts. 9, 15 | ISO/IEC 42001: Cl. 8, 9.1 | NIST AI RMF: MEASURE | OECD: Robustness (1.4) | Canada: OSFI E-23 (Independent Validation) | India: RBI Draft MRM Guidance 2026 (Independent Validation)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 9	Requires testing procedures suitable to achieve the intended purpose and to identify appropriate risk-management measures — the basis for independent validation of every high-risk model.
EU AI Act — Art. 15	Sets a baseline that high-risk systems achieve appropriate accuracy, robustness and cybersecurity consistently throughout their lifecycle — not just at initial launch.
ISO/IEC 42001 — Cl. 8, 9.1	Cl. 8 requires operational planning and control of validation activities; Cl. 9.1 requires the organisation to determine what is measured, by what method, and at what frequency — validation cannot be a one-off event.
NIST AI RMF — MEASURE	Dedicated to quantitative and qualitative assessment of AI system performance and trustworthiness, using appropriate, repeatable methods.
Canada — OSFI E-23	Independent validation is an explicit, named stage of the model lifecycle — separate from design and deployment — and applies uniformly to AI/ML models alongside traditional statistical and empirical models used for underwriting, pricing or claims.
India — RBI Draft MRM Guidance, 2026	Requires independent vetting and ongoing validation of every model — including third-party and vendor models — as the second line of defence, distinct from the team that built or owns the model; RBI also reserves the right to engage external experts to independently validate deployed models.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	For a mortgage-affordability model, the audit independently re-performed key validation tests using a more recent out-of-time sample than the bank's own validation report.
Condition:	Discriminatory power (Gini) had degraded 20% since the last validation, which was 14 months old; the bank's policy requires annual review but no re-validation had been triggered.
Criteria:	Art. 15's "consistently throughout lifecycle" requirement and internal validation policy.
Cause:	No automated trigger links validation due-dates to actual live performance monitoring.
Consequence:	The model may now be systematically over- or under-approving borrowers without anyone aware of the degradation.
Corrective action:	Immediate re-validation; a system-generated validation calendar tied to the model inventory so due dates cannot silently lapse. Rated High.

DOMAIN 08 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Explainability & Transparency

EU AI Act: Arts. 13, 14, 50, 86 | ISO/IEC 42001: Cl. 7.4, 8 | NIST AI RMF: MAP, GOVERN | OECD: Transparency (1.3) | Canada: Bill C-36 (Automated Decision Transparency) | India: RBI Draft MRM Guidance 2026 (Explainability Thresholds)

WHAT EACH PROVISION REQUIRES

EU AI Act — Arts. 13, 14	Art. 13 requires systems designed for sufficient operational transparency so deployers can interpret and use output appropriately; Art. 14 requires effective human oversight, impossible without some explainability.
EU AI Act — Art. 50	Introduces GenAI-specific transparency duties: people must be informed they are interacting with AI, and AI-generated content must in many cases be marked as such.
EU AI Act — Art. 86	Grants individuals subject to a high-risk-system decision with legal or similarly significant effects a right to an explanation of the AI system's role and the main elements of the decision.
ISO/IEC 42001 — Cl. 7.4, 8	Requires the organisation to have defined how, when and to whom explanations are communicated, both internally and to customers.
Canada — Bill C-36 (PPCDA)	Requires automated decision-making transparency: organisations must disclose to individuals when a significant decision about them is made by an algorithm, giving Bill C-36 direct overlap with E-23's own explainability requirement for AI/ML models.
India — RBI Draft MRM Guidance, 2026	Sets explicit explainability thresholds within its dedicated AI chapter, naming explainability as one of seven AI risk dimensions FRFIs must actively manage — directly mirroring FREE-AI's "Explainability" Sutra that no material financial decision should remain a black box to customers or supervisors.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	For an auto-insurance pricing model, the audit sampled 25 customers who received a premium increase and requested the explanation given to each.
Condition:	In six cases the stated reason ("claims history") did not match the model's top SHAP-value feature, which was actually a telematics-derived driving-behaviour score.
Criteria:	Art. 86 right to explanation and Art. 13 transparency requirement.
Cause:	Explanation templates were hard-coded years before the current model version and were never linked to live SHAP output.
Consequence:	Customers are receiving explanations that are misleading rather than merely generic, raising complaint and reputational risk.
Corrective action:	Auto-generate explanations directly from live model output; review historical cases with customer communications team. Rated High.

DOMAIN 09 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

GenAI Output Reliability

EU AI Act: Arts. 9, 14, 15, 50 | ISO/IEC 42001: Cl. 8, 9 | NIST AI RMF: MEASURE, MANAGE | OECD: Robustness (1.4) | Canada: OSFI E-23 (Adversarial/Poisoning) + AI for All (CAISI) | India: RBI Draft MRM Guidance 2026 (Hallucination Controls)

WHAT EACH PROVISION REQUIRES

EU AI Act — Arts. 9, 14, 15	The same backbone articles as classical AI — risk management, human oversight, accuracy/robustness — applied to GenAI-specific test types: factuality checks, RAG source-citation accuracy, refusal-rate testing, and jailbreak red-teaming.
EU AI Act — Art. 50	GenAI-specific transparency duties — disclosure of AI interaction and labelling of synthetic content where required — apply on top of the accuracy requirements.
ISO/IEC 42001 — Cl. 8, 9	Requires operational controls and performance monitoring adapted to the system type, including generative-specific failure modes.
NIST AI RMF — MEASURE, MANAGE	Both functions explicitly call out generative AI considerations — confabulation, toxic or biased content generation, and information-integrity risks.
Canada — OSFI E-23 & AI for All	E-23 names adversarial manipulation and data poisoning among the AI/ML-specific risks FRFIs must govern, which extends naturally to generative-model reliability; CAISI's expanded mandate under AI for All funds independent model evaluations relevant to GenAI systems.
India — RBI Draft MRM Guidance, 2026	Names hallucinations and output variability among the seven AI risk dimensions requiring active testing and defence, and mandates red-teaming of AI/ML and generative models before deployment — the closest Indian analogue to the EU AI Act's GenAI reliability requirements.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	The audit red-teamed a customer-facing GenAI "virtual assistant" used for mortgage FAQs with 40 adversarial test prompts.
Condition:	In 4 of 40 cases the assistant fabricated a specific interest rate and repayment term that did not exist in any bank product, presented with full confidence and no disclaimer.
Criteria:	Art. 15 accuracy requirement and Art. 50 transparency requirement.
Cause:	No retrieval-grounding (RAG) constraint ties responses strictly to an approved product-rate document; no confidence-based fallback to a human agent.
Consequence:	Potential mis-selling and consumer-protection exposure from customers relying on fabricated financial terms.
Corrective action:	Implement grounding with citation, human fallback threshold, and mandatory disclaimers; re-test before re-enabling. Rated Critical.

DOMAIN 10 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Drift & Monitoring

EU AI Act: Arts. 15, 17, 72 | ISO/IEC 42001: Cl. 9.1, 10 | NIST AI RMF: MANAGE | OECD: Robustness, Accountability (1.4, 1.5) | Canada: OSFI E-23 (Monitoring Stage) | India: RBI Draft MRM Guidance 2026 (Drift Monitoring)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 15	Requires accuracy and robustness maintained "consistently throughout the lifecycle," which as a practical matter requires ongoing monitoring, not a point-in-time check.
EU AI Act — Arts. 17, 72	Art. 17's quality management system requires post-market monitoring procedures; Art. 72 imposes an explicit post-market monitoring obligation with a documented plan proportionate to risk.
ISO/IEC 42001 — Cl. 9.1, 10	Cl. 9.1 requires monitoring to be planned (what, how, when); Cl. 10 requires corrective action when monitoring reveals nonconformity.
NIST AI RMF — MANAGE	The ongoing-risk-treatment function, covering deployed-system monitoring and response over time.
Canada — OSFI E-23	Monitoring is a distinct, mandatory stage of E-23's full lifecycle governance requirement, sitting between controlled deployment and structured decommissioning — a model cannot be validated once and then left unmonitored for the rest of its working life.
India — RBI Draft MRM Guidance, 2026	Requires active testing and defence against data drift as a named AI risk dimension, incorporated into an ongoing monitoring and reporting framework that includes a defined role for internal audit — model risk tiers must be reassessed whenever significant drift or change occurs.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	A bank's transaction-fraud model had a population-stability-index (PSI) monitoring dashboard tracked monthly.
Condition:	Drift exceeded the 0.25 "significant shift" threshold for three consecutive months, but no ticket, escalation, or model-owner action was logged against any of the alerts.
Criteria:	Art. 72 post-market monitoring obligation and ISO 42001 Cl. 10.
Cause:	The monitoring tool and incident-management system were never integrated, so alerts did not generate tickets.
Consequence:	Fraud-detection accuracy may have silently degraded for an entire quarter with no one aware.
Corrective action:	Integrate drift alerting with the incident-management system so every breach auto-generates a tracked ticket with an SLA. Rated High.

DOMAIN 11 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Privacy & Data Protection

EU AI Act: Art. 10 (+ GDPR) | ISO/IEC 42001: Cl. 4.2, 8 | NIST AI RMF: MAP, GOVERN | OECD: Human-centred values (1.2) | Canada: Bill C-36 (Core Privacy Rights) | India: RBI FREE-AI (Data Risks; DPDP Act 2023)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 10 (+ GDPR)	Data-governance requirements interlock with GDPR's purpose limitation and minimisation principles; examining data for bias may itself require processing special-category or proxy data needing a GDPR Art. 9 legal basis.
ISO/IEC 42001 — Cl. 4.2, 8	Cl. 4.2 requires understanding the needs of interested parties including data subjects and regulators; Cl. 8 requires operational controls embedding privacy-by-design into the AI lifecycle.
NIST AI RMF — MAP, GOVERN	Both functions flag privacy as a cross-cutting characteristic to be assessed alongside fairness and security, not bolted on afterward.
Canada — Bill C-36 (PPCDA)	The Act's core purpose: privacy as a fundamental right (a first for federal private-sector law), a right to deletion and data mobility between organisations, and heightened protections for children's data across all digital environments.
India — RBI FREE-AI Framework	Directs regulated entities to avoid over-collection of personal data and to comply with the Digital Personal Data Protection Act 2023 and RBI's IT and outsourcing guidelines — the closest Indian analogue to Bill C-36 or GDPR-style data-minimisation and lawful-basis requirements for AI training data.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	A bank's customer-service GenAI copilot had access to a knowledge base of unredacted customer complaint narratives, including vulnerable-customer health information.
Condition:	No Data Protection Impact Assessment (DPIA) had been completed for this AI-assisted retrieval use case; the legal basis on file covered only original complaint handling.
Criteria:	EU AI Act Art. 10 and GDPR Arts. 5, 9 and 35.
Cause:	No privacy gate exists in the AI-onboarding process for new data sources connected to a GenAI system.
Consequence:	Potential GDPR breach and vulnerable-customer harm from special-category data exposed to an AI system without safeguards.
Corrective action:	Immediate redaction/access restriction, retrospective DPIA, and a mandatory privacy-review gate for any new AI data source. Rated Critical.

DOMAIN 12 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Cybersecurity & Robustness

EU AI Act: Art. 15 | ISO/IEC 42001: Cl. 6, 8 (+ ISO 27001) | NIST AI RMF: MEASURE, MANAGE | OECD: Robustness (1.4) | Canada: OSFI E-23 (AI Cybersecurity Exposures) | India: RBI Draft MRM Guidance 2026 (Adversarial/Cyber Risk)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 15	Requires high-risk AI systems to be resilient against attempts to alter their use, output or performance by exploiting vulnerabilities, explicitly including adversarial examples and data poisoning.
ISO/IEC 42001 — Cl. 6, 8 (+ ISO 27001)	Requires risk treatment and operational controls tailored to AI, integrated with an existing ISO 27001 information-security management system rather than built as a parallel one.
NIST AI RMF — MEASURE, MANAGE	MEASURE requires adversarial testing and robustness metrics to actually be computed; MANAGE requires treatment plans and incident response tailored to AI-specific attack types.
Canada — OSFI E-23	AI cybersecurity exposures and adversarial manipulation are named explicitly among the AI/ML-specific risks institutions must govern, alongside the more familiar data-poisoning risk to training pipelines.
India — RBI Draft MRM Guidance, 2026	Requires active testing and defence against adversarial cyberattacks, overfitting and spurious correlations as named AI risk dimensions — robustness testing is treated as a mandatory pre-deployment and ongoing control, not a one-off penetration test of surrounding infrastructure.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	The audit requested evidence of adversarial robustness testing for an anti-money-laundering (AML) transaction-monitoring model.
Condition:	The security team had penetration-tested the surrounding infrastructure (APIs, servers) but had never tested whether an actor could structure transactions to stay just under the model's detection threshold.
Criteria:	Art. 15 resilience requirement against exploitation of system vulnerabilities.
Cause:	Security-testing scope is defined by the infrastructure team without AI-specific input from model risk.
Consequence:	The model may have exploitable blind spots already known to sophisticated launderers.
Corrective action:	Commission model-level adversarial and evasion testing; formally extend cyber-testing scope to include AI-specific attack vectors. Rated High.

DOMAIN 13 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Human Oversight

EU AI Act: Arts. 14, 26 | ISO/IEC 42001: Cl. 5.3, 8 | NIST AI RMF: GOVERN | OECD: Human-centred values (1.2) | Canada: OSFI E-23 (Board & Senior Management) | India: RBI Draft MRM Guidance 2026 (Kill-Switch & HITL)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 14	Requires high-risk systems designed for effective human oversight: a qualified person must understand the system's capacities and limitations, correctly interpret output, and be able to override or stop it via a functioning "stop" capability.
EU AI Act — Art. 26	Places the corresponding duty on deployers to assign oversight to individuals with the competence, training and — critically — the time and authority to exercise it meaningfully.
ISO/IEC 42001 — Cl. 5.3, 8	Cl. 5.3 requires oversight roles to be formally assigned; Cl. 8 requires the operational process to build in real intervention points, not just after-the-fact notification.
Canada — OSFI E-23	Board-level risk committees must govern model risk, and senior management must run enterprise-wide model risk management proportional to the institution's size, complexity and systemic risk — oversight cannot be delegated below a genuinely accountable layer.
India — RBI Draft MRM Guidance, 2026	Mandates anti-automation-bias controls: human-in-the-loop (HITL) review, a human override capability, and an emergency "kill-switch" able to take a malfunctioning model offline immediately — among the most concrete human-oversight requirements of any national framework surveyed in this guide.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	A commercial underwriting team was designated as the "human oversight" layer for an AI-assisted risk-pricing tool; the audit interviewed underwriters about their review workload.
Condition:	Each underwriter was expected to review roughly 80 AI-generated quotes per day — under two minutes per case — and the override rate was effectively zero.
Criteria:	Art. 14(4) and Art. 26(2), which require meaningful, resourced oversight, not a nominal review step.
Cause:	The oversight design did not account for realistic caseload capacity when the tool was deployed.
Consequence:	The control is illusory — the model is effectively making unsupervised pricing decisions.
Corrective action:	Redesign the workflow with risk-based sampling for full review plus lighter-touch exception handling; report override-rate KPIs to governance. Rated High.

DOMAIN 14 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Third-Party & Vendor AI

EU AI Act: Arts. 25, 26, 27 | ISO/IEC 42001: Cl. 8, 9 | NIST AI RMF: GOVERN (Govern 6) | OECD: Accountability (1.5) | Canada: OSFI E-23 (Third-Party Accountability; B-10) | India: RBI Draft MRM Guidance 2026 (Third-Party Accountability)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 25	Clarifies when a deployer or distributor can itself become a "provider" — e.g. by substantially modifying a vendor system — which matters for banks fine-tuning a vendor's foundation model.
EU AI Act — Arts. 26–27	Place deployer-side due-diligence, human-oversight and (for certain uses) fundamental-rights-impact-assessment obligations on the bank regardless of who built the underlying model.
ISO/IEC 42001 — Cl. 8, 9	Requires supplier and third-party AI to be subject to the same operational control and performance-evaluation regime as internally built systems.
Canada — OSFI E-23	Explicitly brings vendor AI/ML models into scope: contracts with third-party providers must enforce MRM-consistent validation and reporting, cross-referenced with Guideline B-10 on third-party risk management.
India — RBI Draft MRM Guidance, 2026	States plainly that regulated entities cannot rely on a vendor's safety certificate — they remain fully accountable for third-party AI tools and must independently validate them, with outsourcing contracts updated to guarantee documentation access, audit rights and exit arrangements.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	A bank embedded a third-party AI-driven document-verification tool into account opening; the audit reviewed the vendor due-diligence file.
Condition:	The vendor claimed "99.9% accuracy across all demographics," but the due-diligence file contained no independent validation and no vendor subgroup performance breakdown.
Criteria:	Art. 26's deployer due-diligence duty over third-party AI.
Cause:	Procurement lacks a mandatory model-risk and fairness due-diligence gate for AI vendors.
Consequence:	Undetected bias or accuracy shortfalls could disproportionately affect certain customer groups at onboarding.
Corrective action:	Obtain independent validation or vendor subgroup data; insert audit-rights clauses at renewal; add an AI vendor-risk gate to procurement. Rated High.

DOMAIN 15 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

GenAI & Agentic Governance

EU AI Act: Arts. 50, 53, 55, 56 | ISO/IEC 42001: Cl. 6, 8 | NIST AI RMF: GOVERN, MANAGE | OECD: Transparency, Accountability (1.3, 1.5) | Canada: AI for All (CAISI) + OSFI E-23 (AI/ML Risks) | India: RBI Draft MRM Guidance 2026 (Dedicated AI Chapter)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 50	GenAI-specific transparency duties: disclosure of AI interaction and labelling of synthetic/deepfake content.
EU AI Act — Arts. 53, 55, 56	Set obligations for providers of general-purpose AI (GPAI) models, including technical documentation and, for higher-capability models, systemic-risk assessment and codes of practice — relevant when banks deeply integrate large foundation models.
ISO/IEC 42001 — Cl. 6, 8	Requires the AIMS to explicitly scope what actions an autonomous "agentic" system may take without human confirmation versus what requires it.
Canada — AI for All & OSFI E-23	CAISI's expanded $50M mandate funds research, model evaluations and monitoring relevant to advanced and agentic systems, while E-23's AI/ML-specific risk categories (adversarial manipulation, explainability) apply without carve-out to autonomous or agentic deployments.
India — RBI Draft MRM Guidance, 2026	Includes a dedicated chapter setting explainability thresholds, hallucination and bias controls, mandatory red-teaming, kill-switches and human oversight for AI/ML and generative systems specifically — India's first detailed regulatory treatment of GenAI and, by extension, agentic AI deployments in finance.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	The audit tested an internal "AI ops agent" designed to process routine payment-reconciliation exceptions, via a live walkthrough rather than documentation review alone.
Condition:	A configuration error had granted the agent write access to initiate a category of corrective payment entries autonomously, with no transaction-value cap or real-time human notification.
Criteria:	Art. 14 human oversight applied to agentic contexts, and internal agentic-AI policy.
Cause:	Permission configuration was not independently reviewed against the intended design before go-live.
Consequence:	Potential for unauthorised or erroneous financial transactions at scale with no real-time visibility.
Corrective action:	Immediately revoke autonomous write access; require human confirmation for any transaction-initiating action; mandate a pre-go-live permissions review. Rated Critical.

DOMAIN 16 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Record-Keeping & Logging

EU AI Act: Arts. 12, 19, 26 | ISO/IEC 42001: Cl. 7.5, 9.1 | NIST AI RMF: GOVERN, MANAGE | OECD: Accountability (1.5) | Canada: Bill C-36 (Disclosure Trail) | India: RBI Draft MRM Guidance 2026 (10-Year Retention)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 12	Requires high-risk AI systems to technically allow automatic recording of events ("logs") over the system's lifetime, at a traceability level appropriate to its intended purpose.
EU AI Act — Arts. 19, 26	Art. 19 requires providers to retain system-generated logs for an appropriate period (at least six months, often longer under other financial-services record rules); Art. 26 requires deployers to keep logs under their control for an appropriate period.
ISO/IEC 42001 — Cl. 7.5, 9.1	Requires logs to be retained, protected and actually usable for evaluation — not just generated and forgotten.
Canada — Bill C-36 (PPCDA)	The automated decision-making transparency provision effectively requires organisations to be able to produce the disclosure trail behind a significant algorithmic decision — the record-keeping evidentiary base that makes the transparency right meaningful rather than aspirational.
India — RBI Draft MRM Guidance, 2026	Requires decommissioned models to be retained, with documentation, for 10 years — a materially longer retention period than the EU AI Act's minimum six months — alongside FREE-AI's recommendation for logging and record retention to enable auditability across the model lifecycle.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	For a credit-card fraud-blocking model, the audit selected ten disputed transactions and asked the bank to reconstruct the full decision trail for each.
Condition:	In three cases the logs showed only the final block/allow decision, with no record of which model version scored the transaction or the underlying risk score.
Criteria:	Art. 12 traceability requirement and Art. 19 log-retention duty.
Cause:	A platform migration eight months earlier did not carry the logging schema forward, breaking backward compatibility.
Consequence:	Inability to defend contested fraud-block decisions or respond fully to a regulator's request for records.
Corrective action:	Restore full-fidelity logging immediately; add a backward-compatibility check as a mandatory step in future migrations. Rated High.

DOMAIN 17 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Incident Management

EU AI Act: Arts. 72, 73 | ISO/IEC 42001: Cl. 8, 10.2 | NIST AI RMF: MANAGE | OECD: Accountability (1.5) | Canada: OSFI E-23 (Supervisory Escalation) | India: RBI FREE-AI (Incident Reporting Mechanism)

WHAT EACH PROVISION REQUIRES

EU AI Act — Art. 72	The post-market monitoring obligation feeds directly into incident detection — systems must be actively watched, not just built and left alone.
EU AI Act — Art. 73	Requires providers of high-risk AI to report serious incidents to the relevant market surveillance authority without undue delay, within a defined window from becoming aware (or from when they reasonably ought to have known).
ISO/IEC 42001 — Cl. 8, 10.2	Cl. 8 requires operational controls for incident detection; Cl. 10.2 requires the organisation to react to nonconformity, evaluate root cause, and update risk assessments accordingly.
Canada — OSFI E-23	Non-compliance triggers supervisory escalation, remedial plans and capital adequacy adjustments — binding, auditable consequences under federal prudential oversight that turn an unmanaged AI incident into a direct capital and supervisory issue.
India — RBI FREE-AI Framework	Recommends a dedicated AI incident reporting mechanism (an illustrative form is annexed to the FREE-AI report) and directs entities to incorporate AI into existing incident-reporting frameworks while specifically monitoring for model drift as a trigger for escalation.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	The audit reviewed a logged GenAI incident where a customer-service chatbot gave a customer incorrect information about an overdraft fee waiver, which the customer relied on.
Condition:	The incident sat untriaged for 11 days, no severity classification was applied, and the Art. 73 reportability assessment was never actually performed.
Criteria:	Art. 73's "without undue delay" reporting requirement and the internal incident-management SLA.
Cause:	AI incidents are not distinctly tagged in the general IT incident system, so they get lost in a high-volume queue.
Consequence:	A possible missed regulatory reporting obligation for a serious incident.
Corrective action:	Create a distinct AI-incident category with a dedicated triage SLA and a mandatory Art. 73 reportability checklist. Rated High.

DOMAIN 18 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Compliance & Conformity

EU AI Act: Arts. 16–27, 43, 47, 49 | ISO/IEC 42001: Cl. 9.2 | NIST AI RMF: GOVERN | OECD: Accountability (1.5) | Canada: OSFI E-23 (Binding Obligations) + Bill C-36 (DSDPC) | India: RBI Draft MRM Guidance 2026 (Binding on Finalisation)

WHAT EACH PROVISION REQUIRES

EU AI Act — Arts. 16–27	Collectively set out the full suite of provider and deployer obligations — risk management, data governance, documentation, logging, transparency, human oversight, accuracy/robustness, quality management, deployer due diligence.
EU AI Act — Art. 43	Sets out conformity-assessment procedures a high-risk system must pass before being placed on the market or put into service.
EU AI Act — Arts. 47, 49	Art. 47 requires an EU declaration of conformity; Art. 49 requires CE marking and registration in the EU database for high-risk systems, before deployment.
Canada — OSFI E-23 & Bill C-36	E-23 imposes binding, auditable obligations under federal prudential oversight from May 2027; Bill C-36 is enforced by the new Digital Safety and Data Protection Commission, with penalties up to $25M or 5% of global revenue for the most serious breaches.
India — RBI Draft MRM Guidance, 2026	On finalisation, will bind all 11 categories of RBI-regulated entities and formally supersede Chapter 3 of the 2002 Guidance Note on Credit Risk Management — comments on the June 2026 draft closed 24 July 2026, with the final circular and effective date still pending as of this guide's publication.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	For an AI-driven employee-screening tool used in the bank's own hiring process (high-risk under Annex III), the audit requested the full conformity file.
Condition:	Technical documentation and a risk assessment existed, but no declaration of conformity had been drawn up and the system had never been registered in the required database.
Criteria:	Arts. 43, 47 and 49 conformity-assessment, declaration and registration duties.
Cause:	The AI Act compliance programme was scoped only to customer-facing financial-services use cases, missing internal HR AI.
Consequence:	The system is technically non-conformant and exposed to direct regulatory action.
Corrective action:	Complete the conformity package retrospectively; expand the compliance programme's scope to all Annex III use cases. Rated High.

DOMAIN 19 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Internal Audit & Assurance

EU AI Act: Arts. 16–27; QMS | ISO/IEC 42001: Cl. 9.2, 10 | NIST AI RMF: GOVERN | OECD: Accountability (1.5) | Canada: OSFI E-23 (Risk-Based Proportionality) | India: RBI Draft MRM Guidance 2026 (Third Line of Defence)

WHAT EACH PROVISION REQUIRES

EU AI Act — QMS (Arts. 16–27)	Requires providers, and in substance mature deployers, to operate a quality management system with a systematic approach to compliance — which internal audit is the natural mechanism to test.
ISO/IEC 42001 — Cl. 9.2, 10	Requires internal audits at planned intervals to determine whether the AIMS conforms to its own requirements and is effectively implemented, with Cl. 10 requiring results to drive genuine corrective action.
NIST AI RMF — GOVERN	Explicitly calls out independent audit and assurance as a governance mechanism distinct from first- and second-line self-assessment.
Canada — OSFI E-23	Risk-based proportionality means governance intensity — and therefore the evidence an internal audit function must gather — scales with a model's inherent risk, complexity and systemic impact, giving auditors a regulator-endorsed basis for risk-ranking their AI audit universe.
India — RBI Draft MRM Guidance, 2026	Assigns internal audit the explicit third-line role in the mandated three-lines-of-defence structure, and FREE-AI's Assurance pillar separately calls for independent model validation, periodic audits and updated supervisory/audit tools calibrated to AI-specific risks.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	The audit reviewed the internal audit function's AI-specific coverage plan and staff competency records.
Condition:	Internal audit had performed one AI-related review in three years — a general IT-controls review of the MLOps platform — with no auditor holding AI/ML-specific training and no risk-based AI audit universe covering the bank's 40+ systems.
Criteria:	ISO 42001 Cl. 9.2 and QMS expectations under the AI Act.
Cause:	Internal audit's risk-based planning process has not been updated to reflect the growth of the bank's AI estate.
Consequence:	The third line cannot provide credible independent assurance over a fast-growing risk.
Corrective action:	Build a dedicated, risk-ranked AI internal-audit universe; invest in AI/ML audit skills through training or co-sourcing. Rated High.

DOMAIN 20 OF 20 · FRAMEWORK CROSSWALK (INCL. CANADA & INDIA)

Continual Improvement

EU AI Act: Ongoing compliance | ISO/IEC 42001: Cl. 9.3, 10 | NIST AI RMF: MANAGE | OECD: Responsible stewardship (1.1) | Canada: AI for All (2026–2031 Plan) + OSFI E-23 (Renewal) | India: RBI FREE-AI (Standing Committee; AI Institute)

WHAT EACH PROVISION REQUIRES

EU AI Act — Ongoing compliance	Obligations phase in over a multi-year timeline and guidance keeps evolving, so "ongoing compliance" requires a mechanism to track and absorb regulatory change, not a one-off gap assessment.
ISO/IEC 42001 — Cl. 9.3, 10	Cl. 9.3 requires top management to conduct management reviews of the AIMS at planned intervals; Cl. 10 requires continual improvement of the AIMS's suitability, adequacy and effectiveness.
NIST AI RMF — MANAGE	Framed as an iterative loop: risks are monitored, treated, and the treatment itself is reassessed as context changes.
OECD — Responsible stewardship	Sets continual diligence as a values-level expectation, not a box-ticking exercise performed once.
Canada — AI for All & OSFI E-23	AI for All is a five-year plan (2026–2031) with phased targets requiring periodic recalibration, while E-23's lifecycle governance explicitly includes structured decommissioning and renewal — both instruments assume AI governance is a continuing programme, not a one-time certification.
India — RBI FREE-AI Framework	Recommends a permanent, multi-stakeholder Standing Committee to continuously monitor AI evolution and reassess regulatory frameworks (Recommendation 8), plus a dedicated AI institute to build long-term capacity (Recommendation 11) — treating AI governance as a standing programme rather than a fixed rulebook.

WORKED EXAMPLE — LINKED TO THE PROVISIONS ABOVE (5C FORMAT)

Scenario:	The audit compared the current AI governance policy against the prior year's internal audit report and its finding-closure tracker.
Condition:	Five of seven prior findings were marked "closed," but none had produced any visible change to policy, training or system controls — closure evidence was a management attestation email, not demonstrable remediation.
Criteria:	ISO 42001 Cl. 10 continual-improvement requirement.
Cause:	The findings-closure process accepts management attestation without independent verification of the underlying control change.
Consequence:	The same root causes are likely to recur and resurface in future incidents or audits.
Corrective action:	Require documented, verifiable evidence before any finding is closed; introduce an annual management review cross-referencing prior findings against current controls. Rated Medium.