Crisil
Integral IQ

Navigating OSFI's Revised E-23 Implications, challenges and mitigation strategies

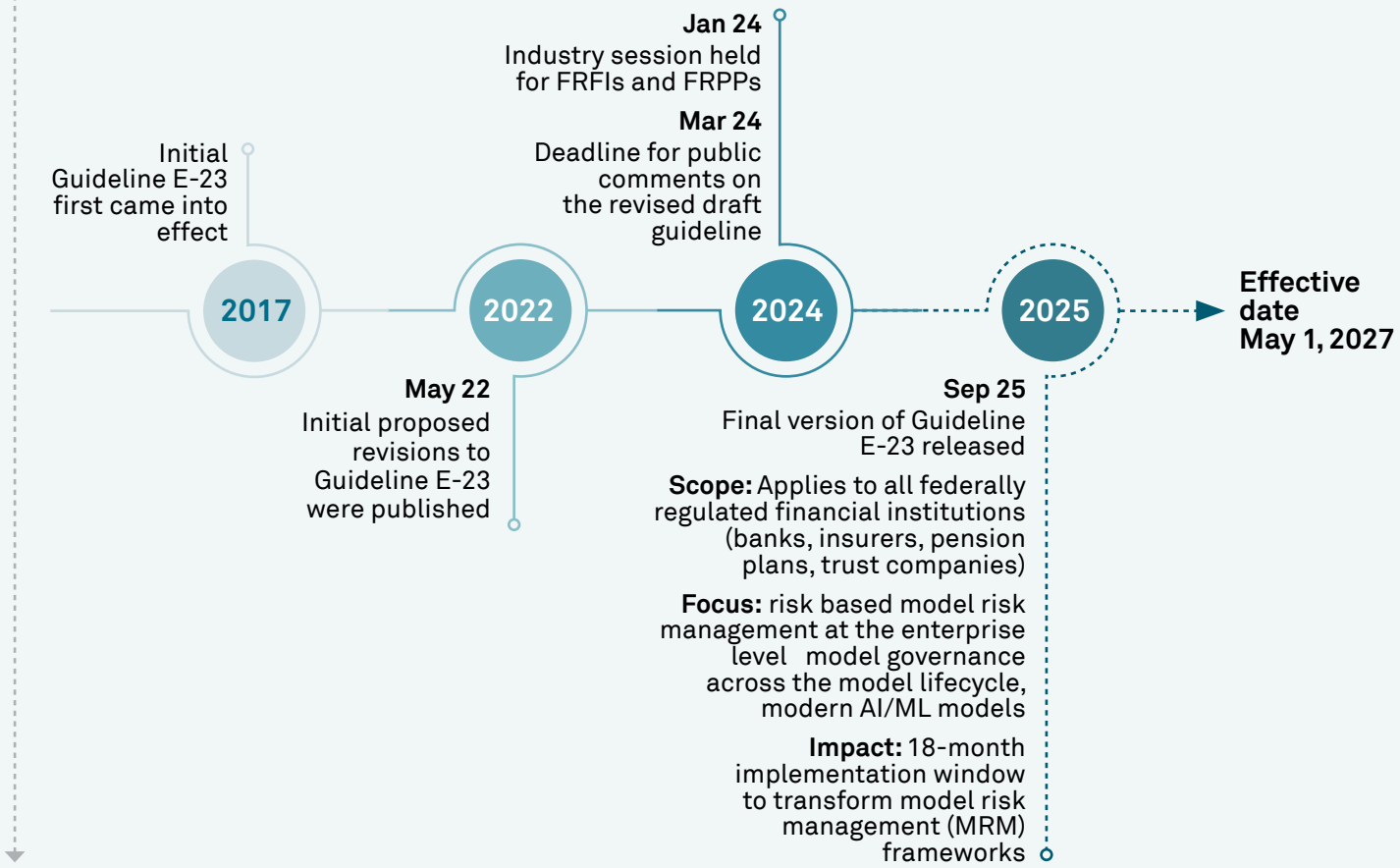
OSFI's revised E-23 guidelines introduce significant changes for Federally Regulated Financial Institutions (FRFIs) in Canada. E-23 calls for an enterprise-wide perspective and a governance framework that aligns oversight with each model's risk rating. It mandates robust controls across the model lifecycle, including design, data, development, independent review, deployment, change management, monitoring, and retirement. The scope also covers artificial intelligence (AI) and machine learning (ML) models, especially those impacting business decisions or day-to-day operations.

E-23 recognizes that eliminating model risk entirely is not feasible. Institutions must understand inherent model risks, apply proportionate oversight, and report residual risks to senior leadership.

by S&P Global

E-23 timeline and background

Background: E-23 has served as the foundational supervisory benchmark for overall model risk management for Canadian financial institutions, since its original release in 2017. The 2027 revision modernizes it with accentuated focus on managing model risk at an enterprise level, model risk rating, model governance and bias, explainability and transparency guidelines around modern Artificial Intelligence and Machine learning models.



1 Recent changes and regulatory expectations

OSFI's E-23 signals that Canadian FRFI s should maintain enterprise-wide oversight of model risk, rather than allowing individual analytics teams to manage it in isolation. Institutions are expected to set up a risk-based oversight framework that matches the governance intensity to real-world stakes. It also makes clear that modern AI/ML models fall under E-23's scope, particularly when models affect operations or customers.

2 Comparison with SR11-7

SR11-7 (US Federal Reserve/OCC) guidelines established the foundational framework for model risk management emphasizing robust model development, independent validation, governance and controls within banking institutions in the US. OSFI's E-23 builds on similar principles but adopts a more modern enterprise-wide perspective, with greater emphasis on risk-tiering , adopting a flexible principles-based approach and oversight of emerging techniques such as AI and Machine learning models. In practice, multinational institutions[2] that have already implemented a mature SR11-7 aligned model risk framework typically require only incremental enhancements to meet E-23 expectations rather than a comprehensive redesign of their model risk program. The table below presents a comparison of SR11-7 and E-23 across key dimensions.

[2]Foreign entities operating on a branch basis in Canada

Comparison between SR11-7 and OSFI E-23

Dimension	OSFI E-23	SR11-7
Scope	Applies to all Federally regulated financial institutions (FRFIs), including banks, insurers, and branches	Applies to banking organizations supervised by Fed/ OCC, scaled to size/complexity
Definition of model	An application of theoretical, empirical, judgmental assumptions or statistical techniques, including AI/ML methods, which processes input data to generate results.	A quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. Includes quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.
Model risk rating	Explicit requirement for model risk rating methodology and use of inherent and residual risk	No explicit model risk rating methodology guidelines, though risk based concepts are implicit
AI/ML explicitness	Directly addresses AI/ML complexity, bias, explainability, and transparency	Predates large scale AI/ML use; AI is covered only generically as models
Integration with other guidelines	Explicitly tied to B-10 (third party), B-13 (tech/cyber), E-21 (operational resilience) and corporate governance expectations	SR11-7 references broader risk management but with fewer explicit linkages to operational/cyber risk frameworks
Lifecycle detail and decommissioning	More explicit on tracking lifecycle status, performance status, modifications, and decommissioning, including keeping decommissioned models in inventory	Lifecycle expectations are described but with less explicit detail on decommissioning and status tagging
Supervisory posture & timing	Effective date of May 1, 2027, for all FRFIs	Standing guidance without a single compliance deadline; expectations enforced through ongoing supervision

3 Key challenges and impact on FRFI's MRM function

a. Enterprise-wide focus

E-23 fundamentally changes the accountability model. Senior management is now expected to maintain enterprise-wide oversight of model risk, rather than allowing individual analytics teams to manage it in isolation. The second major shift is comprehensive lifecycle coverage. E-23 requires institutions to treat models as ongoing assets, with controls and documentation covering rationale, data quality, development standards, independent review, deployment with change control, monitoring with thresholds and escalation, and formal retirement. Decommissioned models must also be retained on record for a defined period.

To address these gaps, a fundamental shift in mindset is necessary; Institutions should adopt a portfolio view of model risk, with clearly defined processes and capabilities for measuring, managing, monitoring and reporting on model risk at different model segments and enterprise levels

b. Inventory gaps

Most FRFIs maintain a model list but lack an accurate and controlled enterprise system of record. Common items missing from the inventory include high-impact spreadsheets, embedded decision engines within vendor platforms (primarily related to AML and fraud analytics), pricing calculators, and models developed in foreign head offices but used in Canada. In addition to missing models, many institutions also lack essential data fields, such as model dependencies, data sources, approved use, and limitations, for models already uploaded in the inventory.

To address these gaps, institutions should assign a Model Steward, typically from the model governance function, and conduct a structured enterprise-level review to identify which items require full life cycle governance. Depending on the inventory system's capability to track model meta data as required by E-23, potential upgrades may also be necessary.

c. Risk rating struggles

E-23 requires each model to be assigned an inherent risk tier using measurable criteria that combine quantitative factors, such as portfolio size and operational impact, with qualitative factors, including use case, complexity, data reliability, and customer or regulatory exposure. However, a common issue arises when a scoring model is developed that does not influence actual processes.

To mitigate this, institutions should establish well-defined and governed processes for model risk rating. The resulting inherent risk should determine review frequency, documentation requirements, approval authority, monitoring cadence, and re-rating triggers. When models with negligible inherent risk are exempted from full model life cycle governance requirements, there must be a robust process to approve and track such exemptions.

d. AI/ML blind spots

With the widespread adoption of AI/ML systems across various use cases, and the fact that many AI/ML models are embedded within third-party "black box" vendor systems, institutions need to reconsider their AI-specific risk and governance mechanisms.

To mitigate these risks, AI models require specialized validation techniques focused on examining bias, transparency, and explainability. Autonomous systems require evaluation and early warning indicators for of concept and data drift as part of ongoing monitoring. Generative AI models embedded in applications (e.g., document summarization or report writing) require application-specific evaluation rather than general benchmark assessments. Customer-facing applications, like chatbots, require techniques such as adversarial testing to ensure confidential information is not leaked.

e. Governance fragmentation

E-23 specifies that MRM requires appropriate reporting structures, relevant skills, and a multidisciplinary team, including risk, IT, and legal or ethics as needed. To achieve this, institutions should establish a consistent, enterprise-wide governance framework that aligns policies, standards, and oversight across business lines.

To mitigate risks arising from shared ownership of model components, the governance framework should also include clearly defined roles and responsibilities for model owners, users, developers, validators, and auditors, ensuring consistent application of model life cycle controls. Importantly, the framework must be sufficiently flexible to accommodate evolving technologies, different model types (especially crucial given the "black box" and autonomous nature of many AI/ML models), varying levels of model risk, and organizational changes. This enables more effective and coordinated management of model risk across the organization.

f. Deployment Risk Assessments

Before deployment, institutions should assess non-model risks that could affect model confidentiality, integrity, availability, and resilience. Key areas include cybersecurity, technology vulnerabilities, third-party dependencies, and other operational risks.

To address these risks, organizations should complete initial risk assessments and update them after significant changes. Organizations must also confirm that controls such as secure configuration, access management, vulnerability remediation, and incident response are in place to ensure resilience.

How we can help

We offer comprehensive services to support FRFIs in meeting the revised Guideline E-23, including:

Our team brings extensive industry knowledge and regulatory expertise, positioning us as a trusted partner for Canadian FRFIs. While Guideline E-23 is complex, we can help streamline your compliance efforts. Please contact us to discuss how we can support your team's preparation.

Crisil Integral IQ analytical contacts

Srinivasan Muthukrishnan
Head of Quantitative Solutions, Americas
srinivasan.muthukrishnan@crisil.com

Bhushan Chopde
Model Risk Practice Partner, Americas
bhushan.chopde@crisil.com

Garvit Dave
Model Risk Practice Partner, Americas
garvit.dave@crisil.com

About Crisil Integral IQ (formerly Global Research & Risk Solutions)

Crisil Integral IQ delivers solutions and actionable intelligence to top financial institutions, driving strategic transformation, risk optimization, and operational excellence. Our offerings across research, risk, lending, analytics and operations have empowered clients to navigate complex markets, mitigate risks and unlock new opportunities. Our domain expertise, innovative solutions, future-ready technologies such as AI and data science give clients the confidence to accelerate growth and achieve sustainable competitive advantage. Our globally diverse workforce operates in the Americas, Asia-Pacific, Europe, Australia and the Middle East.

For more information, visit IntegralIQ.Crisil.com

About Crisil

Crisil is a global, insights-driven analytics company. Our extraordinary domain expertise and analytical rigour help clients make mission-critical decisions with confidence.

Large and highly respected firms partner with us for the most reliable opinions on risk in India, and for uncovering powerful insights and turning risks into opportunities globally. We are integral to multiplying their opportunities and success.

Headquartered in India, Crisil is majority owned by S&P Global.

Founded in 1987 as India's first credit rating agency, our expertise today extends across businesses: Crisil Ratings, Crisil Intelligence, Crisil Coalition Greenwich and Crisil Integral IQ.

Crisil's global workforce operates in the Americas, Asia-Pacific, Europe, Australia and the Middle East, setting the standards by which industries are measured.

For more information, visit www.Crisil.com

Connect with us: LinkedIn | Twitter

Crisil Privacy

Crisil respects your privacy. We may use your personal information, such as your name, location, contact number and email id to fulfil your request, service your account and to provide you with additional information from Crisil. For further information on Crisil's privacy policy please visit https://www.crisil.com/content/crisilcom/en/home/crisil-privacy-notice.html.