

# Information



**Effective Date:** TBD  
**Identifier:** No. AU0137INF

## Proposed Guidance for Operational Risk Management Framework in Rating and Underwriting of Automobile Insurance

### Table of contents

Purpose .....	2
Scope .....	2
Rationale and Background .....	3
Principles .....	4
Operational risk management framework .....	5
Application to other existing obligations .....	12
Effective date and future review .....	12
About this guidance .....	12
Appendix 1: Model risk management .....	13

## Purpose

This Guidance is intended to articulate foundational and sound practices for operational risk management (ORM) in the rating and underwriting of automobile insurance.

Application of this Guidance will promote just, reasonable, and accurate rates charged to consumers. It will also support fair treatment for consumers engaged in the underwriting process.

The level of implementation/adoption of this Guidance should be interpreted with a proportionality principle commensurate with the nature (including business model), size, complexity and risk profile of the insurer.

**Note for Consultation:**  
**Strategy for Reforming Regulation of Auto Insurance Rates and Underwriting**

FSRA's proposed priorities for 2022-23<sup>1</sup> include the implementation of a strategy for reforming the regulation of auto insurance rates and underwriting. The purpose of this Guidance aligns with the target outcomes of FSRA's overall priority, particularly fair treatment of consumers through FSRA guidance and a new supervisory framework for rate regulation.

## Scope

This Guidance affects insurance companies writing automobile insurance in Ontario.<sup>2</sup>

---

<sup>1</sup> [FSRA 2022-23 Statement of Priorities \(fsrao.ca\)](https://fsrao.ca)

<sup>2</sup> FSRA acknowledges how the outlined foundational and sound practices may be applied across different products/business lines, or implemented at the enterprise-level by P&C insurers.

## Rationale and background

Through targeted consultations with auto insurers and analysis of information collected during the review of rate filings, FSRA has identified gaps in operational risk management and model governance practices in the industry.

Examples include:

- Lack of robust three lines of defence, governance and control throughout the model lifecycle (e.g. missing independent second line for model review or model approval function), which may lead to customers being priced inaccurately
- Lack of process to understand the impact to individual customers from the use of models, including machine learning models, which may lead to unfair discrimination and constitute a contravention of Regulation 7/00 *Unfair or Deceptive Acts or Practices* (“**UDAP Regulation**”)
- Lack of operational risk management process to identify, mitigate and report underwriting and/or rating errors<sup>3</sup>, which may lead to undetected errors and incorrect premiums charged to consumers

FSRA has identified sound operational risk management practices through jurisdictional scans and stakeholder consultation<sup>4</sup> as a mechanism to address the gaps.

Identifying and promoting sound operational risk management practices achieves FSRA’s statutory objects,<sup>5</sup> including:

---

<sup>3</sup> FSRA is developing a Guidance to set out regulatory requirements and compliance expectations to auto insurers regarding the regulatory reporting and resolution of rating and underwriting errors.

<sup>4</sup> Sound Operational risk management practices identified in this Guidance are consistent with those promulgated by the Committee of Sponsoring Organizations ([COSO](#)) and International Organization for Standardization ([ISO](#)) and with guidelines set out by Office of the Superintendent of Financial institutions ([OSFI](#)) (namely B-10). Model risk management practices outlined in appendix 1 are consistent with OSFI guidelines E-23 and E-25.

<sup>5</sup> FSRA Objects (see section 3): <https://www.ontario.ca/laws/statute/16f37#BK4>

- to contribute to public confidence in the regulated sectors
- to monitor and evaluate developments and trends in the regulated sectors
- to promote high standards of business conduct
- to protect the rights and interests of consumers
- to foster strong, sustainable, competitive and innovative financial services sectors

## Improved compliance

FSRA anticipates that adopting the ORM framework will assist insurers in complying with applicable *Insurance Act* and *Automobile Insurance Rate Stabilization Act* requirements, including by avoiding unintended contraventions of s. 439 of the *Insurance Act* as it relates to paragraphs (3) and (11) of s. 1 and paragraph (5) of s. 2(1) of the UDAP Regulation.<sup>6</sup>

## Principles

FSRA's [Rate Regulation Principles](#) are foundational to its approach to auto insurance rate regulation and have been central to the design of this guidance. In developing a principles-based and outcomes focused approach to managing operational risk in rating and underwriting, FSRA was guided by all six principles with a particular emphasis on *Consumer Focus*.

---

<sup>6</sup> Paragraph (3) of s. 1 of the UDAP Regulation prescribes as an unfair or deceptive act or practice, “any unfair discrimination in any rate or schedule of rates between risks in Ontario of essentially the same physical hazards in the same territorial classification.”

Paragraph (11) of s. 1 of the UDAP Regulation prescribes as an unfair or deceptive act or practice, “when rating a person or a vehicle as an insurance risk for the purpose of determining the premium payable for a policy of automobile insurance, misclassifying the person or vehicle under the risk classification system used by the insurer or that the insurer is required by law to use.”

Paragraph (5) of s. 2(1) of the UDAP Regulation prescribes as an unfair or deceptive act or practice, “When [an insurer, officer, employee or agent of an insurer or a broker] applies any information or other factor in a prohibited manner on receiving a request for a quotation for automobile insurance, a request for an application to apply for automobile insurance, an application for automobile insurance or in connection with an offer to renew an existing contract of automobile insurance.”

# Operational risk management framework

## Operational risk defined and other terminology

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. FSRA's concerns about operational risk are driven by the negative consumer outcomes and breaches of applicable law that can occur if operational risk, including model risk, is not well managed. For these types of risks, the focus is on ensuring appropriate governance and controls are in place to identify and manage risks, rather than managing every activity in detail. It is FSRA's view that rating and underwriting activities are subject to operational risks that can be managed in a similar manner.

As such, for the purposes of this Guidance:

- The term "ORM" refers specifically to operational risk management for auto insurance rating and underwriting activities.
- The term "ORM framework" refers to the policies, procedures, and any related documents that outline how the company manages its operational risk in its auto insurance rating and underwriting activities.
- The term "Senior Management" refers to the insurer's Senior Management, including the Chief Executive Officer, the Chief Financial Officer, the Chief Risk Officer, Chief Compliance Officer, the Executives responsible for rating and underwriting, and any other employee formally identified by the insurer's Board of Directors.

## The operational risk management cycle

Managing operational risk in an insurer's processes generally follows a consistent cycle, termed here as the ORM cycle. This section outlines the ORM cycle and associated steps observed by FSRA that should be taken to manage an operational risk in rating/underwriting, including specific considerations.

- 1) Risk identification:** An insurer's ORM framework should outline how it will ensure that operational risks are identified in a timely manner. The specific tools used to identify operational risk will depend on a range of relevant factors, particularly the nature

(including business model), size, complexity and risk profile of the insurer – examples of identification tools include surveys, workshops, registers, and questionnaires.

- 2) Risk assessment:** An insurer's ORM framework should outline how it will assess the materiality of identified operational risks in a consistent manner. The insurer should be able to articulate its inherent and residual risk, where inherent risk is defined as the risk level prior to accounting for existing controls or risk responses and residual risk is defined as the risk level after taking into account existing controls/responses.
- 3) Risk prioritization and mitigation:** Based on the risk level identified through the assessment process, the insurer can rank any new risk against its pre-existing risks for prioritization purposes and, therefore, can determine how the risk should be managed (e.g. accept, reduce, share, avoid). The insurer's ORM framework should outline the processes and controls by which risks are prioritized and managed.
- 4) Risk monitoring and reporting:** An insurer's ORM framework should outline how it will monitor risks being managed, how it will report risk levels to relevant stakeholders, and how it will address risks that fall outside acceptable levels. When a risk falls outside acceptable levels, the insurer's ORM framework should outline how action plans will be established to bring risks within acceptable levels, including appropriate escalations – if needed, to the Senior Management and Board of Directors.

The ORM Cycle should occur on an on-going basis for existing processes and on an ad-hoc basis as required for new product introductions, projects or changes contemplated to existing products and processes. On a periodic basis, the insurer should also review all high-risk areas (even those that are appropriately mitigated within acceptable levels) in order to have a full understanding of all the significant risks.

## Operational risk management foundational practices

FSRA has observed that, for the ORM cycle to be applied effectively to address the risks in rating/underwriting, the ORM Framework should, at a minimum, include the following foundational practices:

- 1) define an operational risk appetite specific for rating and underwriting of automobile insurance
- 2) clearly define roles and responsibilities with robust accountability mechanisms
- 3) have data governance in place
- 4) maintain ORM frameworks on an on-going basis

Each of these foundational practices are outlined below.

### **1) Defining operational risk appetite for rating and underwriting**

To ensure that operational risks are managed in a consistent manner throughout the organization over time, insurers should develop and maintain a comprehensive risk appetite statement for operational risks in rating and underwriting of automobile insurance. The risk appetite is a statement or series of statements that describes the entity's attitude towards risk taking. More specifically, it articulates the nature and types of operational risk that the insurer is willing or expected to assume in order to achieve its business objectives.

The operational risk appetite statement should be succinct, clear, and include a measurable component (limits/thresholds). The purpose of having a measurable component is to indicate the level of operational risk that is considered acceptable within the insurer. The limits/thresholds may also serve to indicate the level at which operational risk events, near misses, or cumulative patterns, are considered necessary for escalation to Senior Management (in some cases, separate reporting thresholds may be established).

In formulating a risk appetite statement, insurers may consider elements such as: changes in the external environment; material changes in business or activity volumes; the quality of the control environment; the effectiveness of risk management or mitigation strategies; the insurer's operational risk event experience; and the frequency, volume or nature of risk appetite limit/threshold breaches.

In the case of insurers with lower operational risk profiles, risk appetite can be evidenced by the use of reporting/escalation thresholds for material operational risk events.

### **2) Clearly defined roles, responsibilities, and accountability mechanisms**

For an operational risk management framework to be effective, it is essential that all participating stakeholders and their respective responsibilities are clearly documented and defined, and that adequate accountability mechanisms are established. In order to achieve these outcomes, an appropriate governance structure and a Three Lines of Defence model, explained below, should be implemented.

### **Governance structure**

To instill a strong, organization-wide risk management culture, the Board of Directors and Senior Management should play an active role. As the stakeholder ultimately responsible for the activities of an insurer, the Board of Directors should therefore also have responsibility for the insurer's ORM framework.

This includes ensuring it has a sound understanding of the insurer's operational risks and whether the ORM framework is operating as expected, including ensuring that independent risk management functions exist and are effective.

Senior Management should be responsible for establishing and maintaining the policies and processes that operationalize the ORM framework, embedding appropriate accountability mechanisms, such as the Three Lines of Defence model discussed below, throughout the organization. Issues should be escalated to the Board of Directors and Senior Management when necessary.

### **Three lines of defence**

Appropriate accountability in the management of operational risk is essential. A "three lines of defence" structure is one way to achieve such accountability. For illustrative purposes, the roles and responsibilities of each of the three lines are described below. In determining what is considered an appropriately robust structure, insurers may consider factors such as size, ownership structure, complexity of operations, corporate strategy, and risk profile.

#### **First line of defence**

The business line – the first line of defence – has ownership of risk whereby it acknowledges and manages the inherent and residual operational risk that it incurs in conducting its activities. The first line of defence is responsible for the ORM lifecycle as per the insurer's ORM framework,



including following its Risk Appetite, policies / processes, reporting, monitoring, etc. The first line of defence may develop a compliance or quality assurance process to assist it in fulfilling its risk ownership responsibilities.

## Second line of defence

The second line is an independent function that should provide an effective challenge and oversight of first line's activities, ensuring that operational risk is properly managed and within the insurer's risk appetite. Second line's review should include, at a minimum, a review of:

- **Reproducibility:** The second line should be able to understand first line's processes and procedures and independently trace the first line's decision-making. This necessarily implies that first line should have current, accurate, and complete documentation that can be reviewed by the second line.
- **Soundness:** The second line should provide an objective and independent review of whether the first line's management of operational risk is conceptually sound. If the second line considers the first line's management of operational risk inadequate or incomplete, then feedback should be provided on how findings can be remediated.

## Third line of defence

The third line of defence is administered by the internal audit function, providing independent assurance to the Board of Directors and Senior Management on the effectiveness of the insurer's ORM framework with respect to rating and underwriting.

The third line of defence should be separate and independent from both the first and second lines of defence and provide an objective review and testing of the insurer's ORM controls, processes, systems, and of the effectiveness of the first and second line of defence functions.

The third line of defence is best placed to observe and review ORM more generally within the context of the insurer's overall risk management and corporate governance functions. Objective review and testing coverage should be sufficient in scope to verify that the ORM framework has been implemented as intended and is functioning effectively.

### 3) Having data governance in place

Effective decision-making is contingent on the quality of data. An insurer's ORM framework should outline how its data governance practices apply in its ORM practices, ensuring that data used is appropriate, accurate, complete, and timely. This should include items such as:

- **Data quality assessments:** Insurers should identify characteristics that data should possess in order to produce credible estimates and then, based on their criteria, verify their data through fitness for use assessments. Data quality should be monitored on a regular basis to ensure fitness of use.
- **Identification of data problems/opportunities:** Timely identification and resolution of problems, including opportunities for making improvements in data processes, with a goal to increasing the quality of existing and future data.
- **Identification of data limitations:** Insurers should identify all known limitations in their data and consider items such as why, despite limitations, the data is appropriate for use, special monitoring considerations for such data, etc.
- **Data ownership:** In addition to characteristics regarding data, it is critical that each data source used has a designated owner to instill accountability for data quality.

### 4) Maintenance of the operational risk management framework

Maintenance of the ORM framework is important not only from an auditability standpoint but also for business continuity purposes, i.e., to enable sustainable operation in the long-term. The review functions play an essential role in identifying opportunities for improvement in the ORM framework.

Sound practices observed by FSRA include:

- **Training:** Implementing and maintaining an ORM framework will require a thorough understanding from staff of their roles and responsibilities. Insurers should outline in their ORM frameworks the policies/processes used to ensure that staff are adequately trained on an on-going basis. The ORM framework should also outline how it reviews the adequacy of its training processes.

- **Documentation:** Insurers should ensure that they have current, accurate, and complete documentation of their entire ORM framework. This includes items/documents such as a risk registry, risk appetite statements, model risk management policies, model documentation, key decisions, process documentation, interactions between the three lines of defence, use of key risk indicators, etc. Insurers should also ensure they log the materialization of any operational risks or near misses as well as any exercises used to learn from these events, e.g. root cause analysis. Any information relevant to the creation and maintenance of the ORM framework and in decision-making throughout the ORM lifecycle should be documented.
- **Periodic reviews:** Changes in operational, market, or other conditions may render certain policies, processes, or other elements inadequate, thereby requiring revision. An insurer's ORM framework should outline how it would monitor the appropriateness of all elements of its framework and, if deemed necessary, how the insurer would adjust them. This includes but is not limited to training, documentation, risk appetite statement, and governance structures.

## Model risk management

The heavily quantitative nature of models<sup>7</sup> allows them to be managed more precisely than traditional operational risks while also posing additional risks due to their complexity. These risks are particularly pronounced in advanced analytical techniques used in rating and underwriting, such as machine learning and artificial intelligence, and also pose risks in interpretability and explainability. FSRA has outlined how ORM practices may be applied for model risk management in Appendix 1.

---

<sup>7</sup> A model generally refers to a methodology, system, and/or approach that applies mathematical/statistical/actuarial techniques as well as theoretical and (professional) judgmental assumptions (including but not limited to actuarial assumptions) to process input data in order to generate quantitative estimates.

## Application to other existing obligations

Other areas in which these ORM practices may be applied include, but are not limited to:

- **Third-party products and services:** Insurers may decide to use third-party data, use tools created by external parties, or hire a third-party to completely develop products for its own use. Working with third-parties poses additional risks and insurers should take reasonable measures to ensure oversight of use of third-party data or services. Insurers shall retain their regulatory obligations and, therefore, insurers, not vendors, hold ultimate accountability for consumer outcomes.
- **Protection of personal information:** Insurers face various obligations from a confidentiality and privacy standpoint, e.g. the Federal government's *Personal Information Protection and Electronic Documents Act (PIPEDA)* and the proposed *Consumer Privacy Protection Act* through the pending Bill C-11. Applying practices such as a Three Lines of Defence structure can assist insurers in complying with these obligations.

## Effective date and future review

This Guidance became effective on **TBD** and will be reviewed no later than **TBD**.

## About this guidance

This document is consistent with [FSRA's Guidance Framework](#). As Information Guidance, it describes FSRA's views on certain topics without creating new compliance obligations for regulated persons.

## Appendix 1: Model risk management

This appendix outlines foundational and sound practices specific to managing models used in:

- **Ratemaking:** Any model used in the process of estimating future costs associated with the transfer of risk in insurance or other risk-transfer mechanisms.<sup>8</sup> This includes estimation of future costs in total as well as by the underlying levels that comprise the estimate of future cost.
- **Risk classification systems:** Any model used to assign risks to groups based upon the expected future cost or benefit of the coverage or services to be provided.
- **Underwriting:** Any model used to determine whether a risk should be written, renewed, or canceled

### Applying the operational risk management cycle to managing model risk

FSRA has observed how the principles-based nature of ORM practices can be applied effectively in Model Risk Management (MRM). When insurers establish and maintain an effective internal ORM framework, including controls such as the Three Lines of Defence model, this minimizes the risk that models are not developed and implemented in a fair and sound manner.

FSRA acknowledges insurers may already have standalone Model Risk Management frameworks. These practices should be adopted in a proportionality principle, considering materiality of the models, as well as the size and complexity of the insurer.

#### Risk identification

The development of any model should be addressed by the insurer's ORM framework. Insurers should have a model inventory, enabling a comprehensive view of all models being used by the insurer.

---

<sup>8</sup> Definition source: <http://www.actuarialstandardsboard.org/asops/propertycasualty-ratemaking/>

## Risk assessment

For each model identified, the insurer should assess the operational processes/controls in place used to manage model risk. Going through this exercise will allow the insurer to articulate the inherent operational risk in its modeling activities and the quality of risk management applied, from which it can assess the residual operational risk.

When an insurer has strong operational processes/controls in place then it should be able to mitigate the following model risks throughout the modelling process:

- **Inputs:** Data issues such as inaccurate, inappropriate, insufficient, incomplete data, and misuse and/or misunderstanding of data
- **Processing/computation:** Model development issues such as flawed hypotheses and/or assumptions/judgment, inappropriate specifications, coding or calculation errors, unstable models, etc.
- **Outputs:** Model implementation and monitoring issues such as inappropriate, improper or unintended usage, erroneous implementation (e.g. rating errors), misinterpretation of the model results, and inadequate monitoring and/or controls

By understanding whether controls in place are adequate and whether they are being effectively applied, the insurer can then decide how to deal with an identified risk.

## Risk prioritization and mitigation

An insurer can determine how a risk should be managed based on the level of risk determined through assessment. If this process differs for models, then it should be specifically addressed in the insurer's ORM framework.

## Risk monitoring and reporting

Monitoring and reporting processes<sup>9</sup> enable insurers to identify whether the operational risk posed by a model remains within acceptable risk levels and whether the escalation of an issue is necessary, e.g., to the Senior Management and Board of Directors.

## Model risk management foundational practices

FSRA expects Model Risk Management should, at a minimum, include:

- 1) clearly defined model materiality
- 2) three lines of defence being applied throughout the model lifecycle
- 3) model approval function
- 4) process to assess model fairness

### 1) Clearly defined model materiality

The insurer's ORM framework should outline a process to assess and classify the materiality of models, e.g. complexity of model and financial impact, and also outline a governance structure depending on the model materiality. Both quantitative and qualitative measures when possible should be considered.

The degree of governance/control in place for each step of Model Lifecycle should at least be commensurate to the model's materiality.

### 2) Three lines of defence being applied throughout the model lifecycle

Roles of three lines of defence in model risk management include the following:

---

<sup>9</sup> Examples of Key Risk Indicators (KRIs) for model risk monitoring and reporting could include:

- Number of models assessed with high residual risk
- Number of models with significant deterioration in model performance
- Number of models deemed unsuitable for their given purpose by the independent review
- Number of overdue model review
- Number of rating and underwriting errors and their impacts
- Number of overdue reporting of rating and underwriting errors

- The first line of defence (e.g. model owner, developer, user<sup>10</sup>, etc.) is responsible and accountable for managing the model risk
- The second line of defence should be broadly comprised of two core functions:
  - **Independent model review:** This function is responsible for the independent vetting and validation<sup>11</sup> of models, providing conceptual and technical reviews of models developed and maintained, i.e., the full lifecycle of a model is reviewed (from inputs/data to outputs/monitoring).
  - **Model risk management:** This function is responsible for establishing policies that explain the insurer’s Model Risk Management practices and maintaining the model governance framework. Examples include, among others: establishing policies on how model reviews will be prioritized, maintaining an inventory of models, maintaining an inventory of current, accurate, and complete documentation,<sup>12</sup> tracking model findings, etc.
- The third line of defence should perform independent periodic review and/or audit of internal model oversight to assess compliance with established policies and procedures.

Based on the materiality of the model, three lines of defence should be adequately applied in each step of the model lifecycle which generally include **development stage, implementation stage, monitoring/review stage** for new/revised models:

---

<sup>10</sup> Model owner is the first-line unit(s)/individual(s) responsible for the model selection, coordinating model development, initial testing, ongoing monitoring, outcomes analysis, administering changes and documentation. The model owner could also be the model developer who is responsible for designing, developing, evaluating and documenting models or model user who relies on the model’s outputs as a basis for making business decisions.

<sup>11</sup> “Vetting” and “validation” are both review exercises used to determine the appropriateness of a model. To distinguish between both, “vetting” is used to evaluate whether a model is appropriate to place in production whereas “validation” refers to exercises used to ensure that a model in production is still appropriate for use.

<sup>12</sup> For example, decisions and key related information around model approvals and implementation processes should be adequately documented.



- During model development, first line should identify an economic or business rationale for developing a new or revised model and ensure that documentation related to the model development process are comprehensive and address the modelling techniques adopted, and any assumptions/approximations employed, while the second line's review should be sufficiently independent and thorough.
- During implementation, the insurer should ensure the approved model is implemented for its intended purpose and the implemented model reconciles with the intended model. Insurers should perform pre-implementation and post-implementation tests to mitigate the risk of errors.
- During monitoring, the model should be monitored based on emerging data to ensure that it is still appropriate for use. Models should be subject to a periodic review or a review might be initiated in instances where there has been a material event and/or change (e.g., changes in underlying business environment; changes in the size or scope of a business line; deterioration in book of business; changes in mix of business; deterioration in model performance; results of model audits).

### 3) Model approval function

To ensure clarity and accountability in deciding which model is sent for implementation, a Model Approval Function (MAF) should be implemented for the purpose of approving new/revised models for operational use. The MAF may be a senior accountable person or a standalone internal committee or a function incorporated into an existing internal committee – insurers may decide what is appropriate for them. The MAF should review all relevant materials as a basis to make its decision – this includes items such as the model's results, materials from second line's review, documentation, identified findings, etc. The ORM framework should outline how it establishes the MAF.

Models approved for use by the MAF should satisfy all applicable legislative requirements and regulatory Guidance. The MAF should also understand how any other model(s) may have materially influenced the development of an implemented model. The MAF should be presented with not only the model intended for implementation but also details about the other models that influenced the one intended for implementation.

Depending on the size and complexity of the insurer, along with the materiality of the model being reviewed, it may be acceptable for the roles of model reviewer and approver to be combined, provided that there is no potential conflict of interest and independence is maintained. The insurer's policies/processes should outline how it handles this situation.

#### 4) Process to assess model fairness

Insurers should have processes and tools to ensure there is no unfair discrimination in models used for rating and underwriting, throughout the modelling process:

- **Inputs:** Insurers must ensure they are not using any prohibited variables. Other examples of considerations include, among others: processes and controls that ensure the ethical use of data, enable insurers to detect errors and/or bias and mitigate the impacts, where possible.
- **Processing/computation:** The goal of modelling should not be only to maximize predictive performance but to do so subject to a fairness constraint. Examples of considerations include, among others: whether there is alternative specification of the model which has less adverse impact on a customer group but still achieves the level of predictive power/strength of quality.
- **Outputs:** Insurers should ensure they have implemented measures that allow them to assess and track fairness of model outputs. Examples of considerations include, among others: a process/tool to ensure that the model's outputs are aligned with its fairness objectives and other objectives, a process in place to detect unintended model use and unintended harms to individuals or groups during model monitoring and review.

#### Interpretability and explainability of AI/ML models

The complexity and automated nature of artificial intelligence (AI) and machine learning (ML) models can amplify the risk of models being developed in an unfair manner. To mitigate this risk, insurers should establish tools that enable the interpretability and explainability of AI/ML models, which FSRA has defined as follows:

- **Interpretability:** The ability to understand a model's soundness, e.g. understanding its mechanics, the model results, and whether the results meet the model developer's objectives.
- **Explainability:** The ability to convey the model's results and its drivers to stakeholders not involved in the development of the model, e.g. consumers, business partners, etc.

Explainability is particularly important as providing consumers with clear information enables them to make informed decisions, which is consistent with the goals of FSRA's Fair Treatment of Consumers Guidance. FSRA acknowledges that the degree of explanation required may vary by audience.

Insurers should outline in their ORM frameworks the processes/controls used to develop and operationalize these tools ensuring they are used effectively and sustainably for AI/ML models.