Supervisory Toolkit for AI Use in Capital Markets: Standalone Toolkit

EXTRACT FROM FINAL REPORT

The Board of the
International Organization of Securities Commissions

OR/07/2026 May 2026

This document is an extract of the full IOSCO report *Supervisory Toolkit for AI Use in Capital Markets*. It supports IOSCO member authorities in their respective oversight of the use of Artificial Intelligence (AI) based systems by entities subject to their regulation and supervision through a toolkit that provides supervisors with practical, non-binding, non-prescriptive supervisory tools, applicable across regulatory models. This report is the result of a multi-phased approach by IOSCO through its Fintech Task Force (FTF) to assist IOSCO members as they consider regulatory and supervisory responses to AI technologies used in capital markets. This approach is based on a shared understanding of the risks such technologies may pose to investor protection, market integrity, and financial stability.

Through extracting the toolkit from the full report into this standalone document, IOSCO aims to provide supervisors with a practical reference that can be readily utilized during supervisory activities, including on-site examinations and inspections. By consolidating the tools in a single, accessible format, this document is designed to serve as a hands-on resource that supervisors can refer to when assessing supervised firms' use of AI systems. The full report provides broader context on AI-related technological developments, risk analysis, and the principles of risk-based supervision that underpin this toolkit.

These tools are non-binding and non-prescriptive and are instead intended to be practical and applicable across different regulatory models. They are not meant to be exhaustive but provide supervisors with a structured starting point and a flexible framework to identify risks and tailor their oversight approaches to the specific characteristics and contexts of AI deployment within their markets.

Table 2: Areas of supervisory consideration

Area	IOSCO 2021 Report Measures (see Box 3 above)	Potential Supervisory Concerns	Supporting Evidence for Review
AI Governance & Oversight (see Table 3 for more detailed considerations)	Measures 1 and 3	• Lack of Board and senior management oversight or accountability; inadequate reporting to Board and senior management. • Lack of documented internal AI governance and risk management framework and broader AI policies and procedures, including IT and data governance framework. • No AI inventory or classification to identify AI use cases. • Insufficient approval processes. • Inadequate training and ongoing education for Board, senior management and staff exercising control functions. • Lack of understanding and knowledge of AI system design. • Lack of clear and documented roles and responsibilities for developers, deployers, and users.	• AI governance policies & procedures. • AI risk management framework. • AI inventory/registry, including technical documentation/description of AI systems. • Governance committee documents. • Organization charts. • Training programs, materials, and records relating to AI systems and usage. • Human oversight, policies & procedures in place for appropriate and proportionate human intervention/interruption in the operation of the AI system. • Documentation of staff qualifications, including relevant certifications, competency assessments, and continuing education plans.

Area	IOSCO 2021 Report Measures (see Box 3 above)	Potential Supervisory Concerns	Supporting Evidence for Review
Model Risk Management (see Table 3 for more detailed considerations)	Measures 2, 3 and 6	• Inadequate model testing, including back testing, stress testing, testing for bias and model drift, and underlying data testing. • Inadequate ongoing performance monitoring. • No independent validation of model performance. • No alert mechanisms for anomaly detection. • No methodology for AI system suspension where anomalies are detected.	• Model validation and testing policies & procedures and reports, including pre-deployment, post-deployment and ongoing validation, monitoring and testing, including documentation and logs. • Model performance monitoring policies & procedures and reporting, including performance and bias. • Model change management policies & procedures and logs. • Independent AI model validation and testing reports. • Model performance anomaly detection alerts and processes.
Investment Advice & Suitability (see Table 5 for more detailed considerations)	Measure 6	• Lack of suitability of AI-generated recommendations. • Failure to consider investor circumstances. • Inadequate human oversight. • Bias in AI systems, including logic and prompts. • Conversational interface advertising (i.e., embedded sponsored content within an AI-driven advisory conversation). • Claims that are misleading or overstate AI capabilities ("AI-Washing").	• Client profile and input data. • Suitability policies and procedures addressing client profile, including risk tolerance and investment objectives. • Policies and procedures addressing the availability of product or service offerings for investment recommendations by any AI system. • AI recommendation logs, including outputs and supporting data. • Human review and override documentation.

Area	IOSCO 2021 Report Measures (see Box 3 above)	Potential Supervisory Concerns	Supporting Evidence for Review
			• Conflict identification and management policies & procedures. • Investor complaints. • Client disclosures.
Market Risks (see Table 3 for more detailed considerations)	Measure 2	• AI use amplifying market volatility. • Flash crashes from AI-driven trading. • Herding behavior/correlation /collusion. • Liquidity issues. • Other sources of systemic risk.	• Market risk policies & procedures. • Stress testing policies & procedures. • Circuit breaker or kill switch policies & procedures. • Volatility and liquidity management plans. • Emergency policies & procedures.
System Reliability & Business Continuity Planning	Measures 2 and 6	• AI system failures. • No backup or recovery procedures. • Single points of failure. • Inadequate business continuity. • Service disruptions.	• Operational resilience framework, encompassing both business and cybersecurity aspects. • Business continuity and disaster recovery planning and testing, including plans for AI service disruptions and system outages. • Backup and recovery policies & procedures, including safeguards to protect client records and other sensitive information. • System availability and performance monitoring, including related reporting and service level agreement compliance.

Area	IOSCO 2021 Report Measures (see Box 3 above)	Potential Supervisory Concerns	Supporting Evidence for Review
Cybersecurity & Data Privacy/Protection	Not covered explicitly in 2021 AI Report.	• AI system attacks/breaches. • Client data exposure or exfiltration. • Model theft or manipulation (poisoning). • Inadequate access controls. • Other data leakage. • Use of AI for advanced cyberattack, i.e., social engineering, deepfakes, identity theft.	• Cybersecurity policies & procedures and standards, including where relevant the cloud infrastructure associated with AI systems used. • Penetration test framework. • Identity and access management controls for AI systems and data. • Incident response policies & procedures. • Privacy impact and data privacy assessments. • Security audit reports, logs, and penetration test results. • Continuous training of users.
Outsourcing & Third-Party Dependencies (see Table 4 for more detailed considerations)	Measures 3 and 4	• Third-party AI vendor risks, including data access and privacy risks, and cybersecurity risks. • Inadequate due diligence. • Poor contract terms. • Inadequate monitoring of the third-party Provider. • Vendor concentration and dependency risk. • Service provider failures.	• Vendor selection, due diligence (including the level of knowledge, expertise and experience on AI systems), and contract terms, including notice and exit provisions, service level requirements, and data protection obligations. • Ongoing monitoring and oversight procedures, including performance metrics, issue escalation policies, and remedies for poor performance. • Third-party validation and assessments of AI systems, including the identification of cross-market

Area	IOSCO 2021 Report Measures (see Box 3 above)	Potential Supervisory Concerns	Supporting Evidence for Review
		• Lack of technical skills involved in procurement process. • Inappropriate cross-jurisdictional data transfer.	dependencies and potential single points of failures affecting multiple entities. • Where contract terms are general/not tailored to the firm, an assessment of the risks associated with using the firm's services and the firm's own processes to manage those risks.
Disclosure & Transparency (see Table 5 for more detailed considerations)	Measure 5	• Inadequate AI disclosure to investors. • Claims that are misleading or overstate AI capabilities (AI-Washing). • Hidden AI system usage for investor facing services. • Lack of transparency about limitations. • Insufficient disclosure of use of third-party AI services. • Over-reliance on third-party providers' disclosures.	• Client agreements, including account information, acknowledgements, and marketing materials relating to AI usage. • Disclosures outlining material risks and impacts on investors. • Disclosure of incidents where adoption of AI systems has raised regulatory, ethical or legal issues. • Client communications relating to AI usage, including policies & procedures for monitoring such communications for accuracy. • Policies & procedures for reviewing and updating client disclosures to ensure AI-related disclosures are accurate and up-to-date.
Recordkeeping & Audit Trail (see Table 6 for more	Not covered explicitly in 2021 AI Report.	• Inadequate AI system records. • Lack of explainability of AI logic.	• Recordkeeping policies & procedures for AI systems and data, including data with a third-party or external provider.

Area	IOSCO 2021 Report Measures (see Box 3 above)	Potential Supervisory Concerns	Supporting Evidence for Review
detailed considerations)		• Missing audit trails or logs. • Insufficient communication with supervisors through required regulatory reporting. • Insufficient documentation. • Lack of AI system oversight throughout the lifecycle.	• AI inventories. • Recordkeeping of AI-generated outcomes and how AI systems generate outputs. • Compliance policies & procedures for adherence to laws, regulations, and internal standards. • AI system decision and usage logs and audit trail documentation, including inputs, outputs, and AI system logic. • Regulatory filings and supporting documentation. • Incident reporting.

Table 3: Evaluating governance and risk management of AI use

Area	Considerations	Examples of Questions	Information Sources
1. Oversight from Board or Governing Body	• Does the Board set strategic objectives and risk appetite for AI use, and does it set AI policies and procedures? • Does the Board receive regular management information on areas such as the design, implementation, and use of AI systems, governance and risk management, and measures to address investor protection and market integrity?	• Has the Board defined an AI strategy and risk appetite and communicated that within the organization? • How does the Board ensure it possesses sufficient understanding of AI risks and opportunities and how does it promote a corporate culture that prioritizes ethical, fair, and responsible AI use across the organization? • How does the Board ensure that AI risks, where material, are explicitly addressed within the firm's overall risk appetite and management framework, including the setting of appropriate qualitative statements and quantitative measures or limits? • How does the Board ensure that the firm's approach, risk management framework, roles and responsibilities, capabilities and culture for risk management of AI use are regularly reviewed to keep pace with newer AI developments, as well as changes in the firm's risk profile and business strategies? • Does the Board approve the risk management framework, the operational resilience framework, and the outsourcing due diligence framework, and related material modifications? • How does the Board ensure that clear accountability mechanisms are in place when it comes to AI and its risks? • What processes are in place for the Board to independently review and challenge management's assessment of AI system risks, including validation results, AI incident investigations, and the adequacy of mitigation actions? • What reporting is provided to the Board on the use of AI models or systems? How frequently is this provided?	• The firm's AI strategy, risk appetite, AI policies and procedures or broader governance and risk management framework. • Board minutes, management information packs, board reports, key performance indicators. • Evidence of board training on AI governance and risk management.

Area	Considerations	Examples of Questions	Information Sources

2. Senior Management Responsibilities	• Is accountability for AI assigned appropriately to senior management?
	• Is senior management responsible for ensuring the effective implementation of AI-related governance and risk management policies and procedures, and regularly reviewing their effectiveness?
		• Describe the firm's framework for human oversight of AI systems, including clear allocation of roles and responsibilities, decision rights, and escalation paths for AI-driven outcomes.
		• Describe the processes, and senior management's roles and responsibilities within these processes, for the following:
		  ○ Introduction and implementation of AI systems.
		  ○ Coordination and accountability for AI-related risk management across the firm.
		  ○ Review of the use of the AI system for compliance with legal and regulatory requirements.
		  ○ Internal escalation process for managing material AI risks and exceptions, such as incidents or breaches of risk thresholds, and ensuring appropriate and timely actions are taken.
		  ○ Updating the Board on material AI risk issues in a timely manner.
		  ○ Ensuring the necessary competence of personnel and allocating adequate resources (such as human, technological, financial resources) for effective AI risk management, including appropriate training and capacity building.
		  ○ Establishing controls over use of AI by staff, including third-party tools or AI systems used without prior authorization.
		  ○ Establishing adequate controls around third-party vendors.
			• The firm's AI policies and procedures or broader governance and risk management framework
			• Evidence of risks that have been escalated to senior management and/or the Board
			• Organizational charts and role/responsibility assignment matrices that delineate roles/responsibilities

3. AI risk management systems, policies and procedures	• Does the firm implement a formal AI risk management framework, and how does this risk	• What is the firm's stated risk appetite for AI systems (including GenAI and Agentic systems)? Where is risk appetite formalized within the firm internal documentation? • How does the firm maintain a complete AI inventory, including vendor information, usage, risks and goals of each AI system or model, and govern their use according to the assessed risk appetite?	• The firm's AI policies and procedures or broader governance and risk

Area	Considerations	Examples of Questions	Information Sources
	management framework incorporate considerations of the key sources of risk in AI systems, e.g., hallucination risk, explainability and transparency, conflict of interests and bias? • Does the firm determine appropriate human-oversight configurations, define intervention thresholds, support contestability and redress where appropriate, and guard against automation bias? • Does the firm operate end-to-end AI system lifecycle controls (from	• Does the firm have an assessment methodology to evaluate the risk materiality of an AI use case, system or model based on the nature of its business? Is this risk assessment done on a regular basis? Has an impact assessment been undertaken? • Has the firm developed indicators to monitor performance, and has the Board/senior management approved their use? • For a material AI use case, what human oversight measures are in place? Who can intervene or override and how quickly? How often do the interventions/overrides take place? How does the firm back-test if such overrides are appropriate? • What policies and procedures are in place to identify, address or mitigate material conflicts of interest in the use of AI systems? • How does the firm monitor for and guard against automation bias, including through training, awareness information programs and/or controls that encourage critical assessment of AI outputs by staff? • How is AI risk management integrated into the firm's overall risk management framework? • Explain in detail the governance of the AI system lifecycle for a high-impact AI use case, from ideation to retirement. • Does an Internal Audit function conduct reviews concerning the use of AI within the organization?	management framework • Lifecycle standard operating procedures, system development standards, validation/test plans and go-live approvals. • Internal audit reporting

Area	Considerations	Examples of Questions	Information Sources
	ideation to retirement)?		
4. Data governance	• Does the firm, through its policies and procedures ensure data used for AI systems is accurate, complete, representative, timely and relevant for the intended purpose? • Does the firm conduct appropriate data collection, preparation, and maintenance in the use of AI systems?	• How does the firm ensure the quality, representativeness, and appropriateness of data used in AI systems, including steps taken to identify and mitigate potential biases? • What governance structures exist around data ownership and accountability? • How does the firm ensure transparency and traceability of data used in AI systems? • What processes does the firm have in place to ensure that the use of personal or sensitive data in AI systems complies with applicable regulations? • How is data and system access provided AI systems to protect material non-public information and respect information barriers? • How does the firm validate the suitability of external or third-party data sources, and what due-diligence processes are in place? • How does the firm monitor and manage data degradation? • What mechanisms are in place to detect and remediate data incidents, including inaccuracies, loss, corruption, or unauthorized access?	• The firm's data governance framework, data management policy, or enterprise-wide data strategy • Records of data quality assessments, profiling exercises, and remediation logs
5. Risk management of Advanced AI systems	• Does the firm clarify and understand distinctions among different forms of AI within its internal risk management and	• Does the firm distinguish between different AI systems (GenAI, Agentic AI, traditional AI/ML systems, etc.)? If so, has the firm evidenced that it accounts for relevant differences in its approach depending on the specific functionality, risk profile, and governance needs of the AI system being used? Is the added value of complex systems, in terms of their enhanced capabilities, compared to simpler AI systems, analyzed?	• Specific risk management frameworks and processes for advanced AI systems (including model

Area	Considerations	Examples of Questions	Information Sources
	operational resilience documentation, particularly for higher risk advanced AI systems, and manage and oversee those systems commensurate with the risk involved?	• Describe the assessment process and criteria used by the firm for determining which type of AI method is suited for a specific use case. • Before implementing new AI systems, what steps are carried out by the firm to ensure they are ready for deployment, including the principal regulator's consultation (where applicable)? • Describe how the AI system lifecycle is managed, including use of training data, monitoring performance, validation, testing and risk management. • What are the current AI use cases? How are unique risks related to specific use cases (e.g., hallucinations, bias) recorded and assessed?	validation, testing, and monitoring; guardrails and harnesses; training, etc.).

6. AI model validation, testing and monitoring	• Does the firm conduct relevant evaluation and testing that is proportionate to the assessed risk materiality of the AI use case, system or mode?
	• Does the firm identify and assess evolving AI-specific risks such as model drift, adversarial attacks, data poisoning or
		• How are AI-specific risks (including data quality, data management, algorithmic bias, model explainability, and operational resilience) systematically identified, assessed, monitored, and managed within the firm's risk management framework?
		  ○ What is the frequency of testing and oversight over the AI model? What reporting is provided regarding the AI model?
		  ○ Have you integrated preventative and post-event measures against hallucination risk?
		  ○ Have you determined the extent of transparency and explainability required of an AI use case, system or model according to its assessed risk materiality, and established the relevant controls accordingly?
		  ○ Have you defined what the firm considers "fair" outcomes and have appropriate controls to identify and mitigate harmful biases and discriminatory outcomes across the AI lifecycle, calibrated to its assessed risk materiality?
			• Validation, testing, and monitoring exercise results of AI systems (incl. resilience and red team testing)
			• Monitoring dashboards (performance/fairness/drift), alert thresholds, rollback plans,

Area	Considerations	Examples of Questions	Information Sources
	new regulatory requirements?	○ Are key performance indicators of the AI model implemented and monitored? • How is efficient collaboration ensured between all relevant stakeholders in the AI lifecycle, i.e., reviews from model engineers, system operators, data scientists, business experts and senior management? • Is AI also deployed to govern or monitor AI products and, if so, how? How do firms evaluate the value of such use cases and how do firms retain control over the process?	usage and change logs.
7. Controls and human oversight of AI systems	• Does the firm have policies and procedures in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems beyond senior management?	• How is human oversight implemented for AI systems and how does the firm evidence its effectiveness? For Agentic AI, also consider: • What are the specific risks associated with the data and systems the agent has access to, scope of actions the agent can take, the potential for the agent to share information and to whom, the reversibility of those actions, and the agent's level of autonomy? • What are the specific controls for agents? How does the firm limit the scope of impact of agents (e.g., by designing appropriate boundaries at the planning stage)? • Is there sufficient clarity in the roles and responsibilities of both agents and humans throughout the overall lifecycle? Are there adaptations to appropriate human oversight to address automation bias associated with increasingly capable agents? • What new / additional technical controls and processes are in place for agentic components (e.g., pre-deployment and post-deployment testing, gradual rollouts, continuous monitoring? • How are end users informed of the agent's range of actions, access to data, and the user's own responsibilities?	• Second and third line of defense reviews (incl. Legal and Compliance) of AI systems (pre- and post-deployment) • External reviews of AI systems (e.g., system of controls reviews, audit controls, data controls)

Area	Considerations	Examples of Questions	Information Sources
8. Training and AI literacy	• Does the firm deliver role-specific training across relevant stakeholders (e.g., Board, senior management developers, validators, front-office, compliance) and promote AI literacy?	• How does the firm ensure it has the necessary knowledge, staff training/capacity, resources and compliance measures in place for AI systems, particularly regarding privacy and data security? • How does the firm ensure relevant staff can explain, challenge and escalate AI outcomes in their domain? • How does the firm assess and document the qualifications, expertise and ongoing training of individuals responsible for AI policy development, implementation, controls and monitoring to ensure they remain competent as AI technologies — and regulatory expectations — evolve?	• Mapping of AI related tasks with AI system owners, validators, and product owners, with training plans and competency assessments. • Training material, attendance, certifications and competency assessments for employees involved in all stages of the AI-system's lifecycle.

Table 4: Evaluating third-party and outsourcing risks

Area	Considerations	Examples of Questions	Information Sources
1. Assessment of Risk-Proportionate Controls	• Does the firm have policies and procedures around onboarding, and development and deployment controls for third-party AI use, and are they adequate for the risk materiality of the use case, system or model? • Do policies and procedures cover whether testing of third-party AI products and services uses the firm's own data and use cases and do processes exist to receive notifications and assess the impact of third-party AI updates or changes? • Does the firm undertake appropriate compensatory testing (i.e., additional testing to address gaps, weaknesses or limitations in testing or disclosures from the third party)?	• How does the firm select Third-Party AI service providers? What due diligence does it undertake? • Does the firm keep a register of third-party contracts and usage focusing on AI-related providers? • Demonstrate how the firm's control framework scales with the risk materiality of different third-party AI applications. • What testing has the firm conducted using actual data, and how does the firm address informational gaps when providers don't disclose sufficient technical details? • Explain in detail the firm's process for evaluating and managing updates from third-party AI providers.	• Contractual terms and conditions relating to third-party vendors and their AI use. • Risk materiality classifications for all third-party AI use cases with corresponding control frameworks. • Evidence of testing protocols using the firm's own data and specific use case scenarios. • Documentation of compensatory testing addressing gaps from inadequate third-party disclosures. • Formal review schedules and update notification processes for third-party AI systems, presence of received notifications or checks in line with the firm's process. • Results of AI usage surveys, third-party registers and incident reports.

Area	Considerations	Examples of Questions	Information Sources
2. Transparency Measures	• Does the firm assess the level of transparency it receives from third-party AI providers on how key risks (data, model, technology, and cybersecurity) are addressed during development and deployment? • Where third-party transparency measures are not sufficient, has the firm employed compensatory measures such as additional testing, greater human oversight, or appropriate disclosures to users?	• How does the firm assess whether a third-party provider's transparency level meets established expectations? • What specific compensatory measures has the firm implemented where third-party AI lacks required transparency, and how does the firm validate their effectiveness?	• Evidence of regular review/updates to transparency expectations for third-party AI providers. • Records of transparency assessments conducted on third-party AI providers, documenting evaluation of their disclosures on data governance, system development, technology infrastructure, and cybersecurity controls. • Documentation of compensatory measures including additional testing, enhanced human oversight, and user disclosures.
3. Fairness Due Diligence Assessment	• Does the firm exercise due diligence regarding the fairness practices of third-party AI providers, recognising that the firm remains accountable for the fairness outcomes of third-party AI used within the organisation?	• How does the firm verify that third-party AI providers have appropriate risk management practices in place? • How does the firm conduct due diligence on third-party providers' fairness practices, and what evidence does it require? • Given that the firm remains accountable for fairness outcomes, how does the firm monitor and validate that third-party AI produces fair results across different client segments?	• Due diligence documentation on third-party AI providers' fairness practices and methodologies. • Evidence of ongoing monitoring for discriminatory outcomes from third-party AI systems. • Accountability frameworks demonstrating how the firm maintains responsibility for fairness of the outcomes.

Area	Considerations	Examples of Questions	Information Sources
4. Supply Chain Risk Assessment	• Does the firm ensure that key third-party and open-source AI models, datasets, and dependencies have undergone supply chain risk assessments and validation, including reviews of model provenance, training data integrity, and other known vulnerabilities?	• Explain in detail the firm's supply chain risk assessment for your most critical third-party AI systems, including model provenance and training data integrity. • How does the firm validate and monitor known vulnerabilities in its third-party and open-source AI dependencies?	• Third-Party risk management policy requirements in relation to AI related risks and subcontracting. • Documentation of supply chain risk assessments for key AI models, datasets and dependencies. • Documentation of model provenance reviews, training data integrity checks, and vulnerability assessments. • Evidence of validation processes (including testing processes) for both third-party and open-source AI components.
5. Concentration Risk	• Does the firm assess potential concentration risks arising from over-reliance on key third-party AI providers? • Does this assessment consider both direct dependencies (e.g., a single AI model or vendor) and indirect dependencies (e.g., reliance on shared infrastructure or cloud providers)?	• What analysis have you conducted on concentration risks from the firm's third-party AI providers, including indirect dependencies? • What specific steps is the firm taking to reduce over-reliance on key providers, and what are the target timelines?	• Analysis of direct and indirect concentration risks from key third-party AI providers. • Diversification strategies and implementation roadmaps. • Regular concentration risk monitoring and internal and regulatory reporting mechanisms.

Area	Considerations	Examples of Questions	Information Sources
6. Contingency Planning	• Does the firm have robust contingency plans to address potential failures, unexpected behaviour of third-party AI, or discontinuing of support by vendors, particularly for third-party AI used in high-risk materiality use cases, systems or models?	• If the firm's primary AI vendor discontinued support with minimal notice, what specific steps would the firm take and how long would full functionality restoration take? • Provide evidence of the firm's contingency plan testing for high-risk third-party AI applications. • What backup systems or alternative providers does the firm have validated and ready for deployment? • How does the firm assess potential negative consequences in case of discontinuity, i.e., data loss/alteration/leakage?	• Robust contingency plans specifically addressing third-party AI failures and unexpected behavior, including exit plans for normal and stressed exit scenarios. • Vendor discontinuation and vendor-switching response procedures with defined recovery timeframes. • Evidence of contingency plan testing, particularly for high-risk materiality use cases.
7. Legal Framework and Accountability	• Does the firm have legal agreements to facilitate clear expectations and responsibilities, including clauses pertaining to performance guarantees, data protection, the right to audit, notification when AI is introduced, or seeking the firm's agreement before incorporating AI?	• What contractual rights does the firm have to audit third-party AI providers, and how frequently does the firm exercise these rights? • How do the firm's legal agreements provide for notification and approval before AI is introduced or modified in products and services it uses?	• Updated legal agreements with clear performance guarantees and data protection clauses. • Contractual provisions for audit rights, AI introduction notifications, and approval processes. • Documentation showing how agreements facilitate clear expectations and responsibilities.

Area	Considerations	Examples of Questions	Information Sources
8. Capability Development	• Does the firm build awareness and develop capabilities of staff involved in procurement, development, deployment, and use of third-party AI systems?	• What specific capabilities has the firm developed in the firm's procurement, risk, and business teams for managing third-party AI systems (or products)? • How does the firm ensure staff awareness and competence keeps pace with your expanding use of third-party AI systems?	• Training programs and competency frameworks for staff involved in third-party AI procurement and management. • Evidence of appropriately timely and updated awareness-building initiatives across relevant business functions. • Capability assessment results and development plans.
9. Use of Complex AI Products	• Does the firm conduct enhanced assessments when using more complex or novel third-party AI products and services that the firm may have less experience with?	• For the firm's most complex third-party AI implementations, explain in detail its enhanced assessment process and additional safeguards. • How does the firm determine when a third-party AI product requires more detailed assessment, and what additional measures does the firm apply?	• Enhanced assessment protocols for complex third-party AI products and services. • Documentation of additional due diligence measures for unfamiliar or sophisticated AI systems (or products). • Evidence of expert involvement and extended evaluation periods for complex implementations.

Table 5: Evaluating disclosure of AI use

Area	Considerations	Examples of Questions	Information Sources
1. Disclosure of AI use in products and services to end-users	• Does the firm transparently inform clients when they are interacting with AI systems (e.g., chatbots, robo-advisors, or decision support tools)? • Does the disclosure clearly explain how AI systems work, including material information about their performance, limitations, and suitability?	• How does the firm ensure clients know when AI is generating responses or analysis? • Provide examples of how outputs are marked as AI-generated or synthetic. • How does the firm communicate AI decision logic and the firm's application of outputs in client communications or disclosures? • What internal controls exist to validate claims about AI sophistication, performance, or level of integration before they appear in disclosure documents? • How does the firm disclose material AI-related risks (e.g., hallucination risk, third-party dependencies, bias, cybersecurity incidents)? • How often is disclosure occurring (at a single point in time vs. whenever a client interacts with an AI system)? • How does the firm ensure that disclosure about AI use is accurate, evidence-based, and not promotional in tone (i.e., does not constitute AI-washing)?	• Client-facing materials (websites, apps, account agreements) stating whether AI was involved in the process, evidence of machine-readable labels or markings on AI-generated content, and consent language in privacy policies or service agreements specifying AI use. • Substantiation records for claims made in disclosures.
2. AI governance and strategy disclosures	• Does the firm publish disclosures on board/senior management oversight, governance and risk management	• Does the firm publicly describe the Board's/Senior Management's role in overseeing AI systems? • Which senior managers are accountable for AI governance and risk management, as stated in the firm's public disclosures?	• Public reports documents such as annual reports or prospectuses describing use of AI in operations, internal controls, risks, and public

Area	Considerations	Examples of Questions	Information Sources
	frameworks, and roles and responsibilities for AI?	• What internal review process does the firm use to validate marketing, investor, or governance disclosures relating to AI performance, system sophistication, or automation levels?	incident reports; regulatory breach disclosures. • Client facing documents and disclosures regarding the oversight of AI use by the firm. • Board/senior management reporting on risk disclosures referencing AI-enabled systems, accuracy issues, bias management, or fraud, summaries of data, architecture, performance, limitations, and bias metrics for each AI system.
3. Disclosure and consent	• Where AI systems, whether proprietary or run by a third-party, impact client rights, account access, or privacy, is the firm informing clients and seeking explicit consent or allow opting out?	• How does the firm inform clients and obtain consent when AI affects their products, the investment objective or strategy, pricing, or data rights or privacy? Where applicable, how does the firm obtain client consent? • Provide examples of where the firm offers explicit opt-in or opt-out for AI-driven decisions. • What contest or redress mechanisms does the firm have in place for clients to be able to challenge decisions/outcomes where AI has been used? • Where there is material reliance on third-party tools, do firms disclose such dependencies, including associated risks, rather than deferring transparency to technology vendors?	• Records evidencing opt-in/out mechanisms from AI services/products for clients potentially impacted by AI systems. • Client facing documents and disclosures regarding the use of AI systems, including client data used, use of AI systems on services provided to the client.

Area	Considerations	Examples of Questions	Information Sources
4. Identifying misleading claims	• Are AI related claims materially inaccurate, false, vague, or misleading, whether in filings, reports, marketing materials, websites, and social media? • Is the firm able to fairly and accurately substantiate its AI-related claims?	• How does the firm ensure that public statements about your AI are accurate, evidence-based, and not overstated? • Does the firm benchmark your AI systems' performance when making public claims? If so, what evidence underpins such claims? • How does the firm ensure that statements about proprietary AI tools accurately reflect the extent of third-party or vendor reliance? • How does the firm monitor and correct outdated public descriptions of the firm's AI use (e.g., if a system is scaled back, retired, or replaced)? • What governance mechanisms exist to detect and address potential AI-washing identified by clients, investors, employees, or external parties?	• Board/senior management reporting on risk disclosures referencing AI-enabled systems, accuracy issues, bias management, or fraud, summaries of data, architecture, performance, limitations, and bias metrics for each AI system. • Policies and procedures to review the use of AI-related claims in marketing materials, client documents, public statements; include documentation evidencing review of AI claims or statements.

Table 6: Evaluating the recordkeeping and reporting of AI use

Area	Considerations	Examples of Questions	Information Sources
1. Documentation of AI Lifecycle Oversight	• Does the firm maintain comprehensive documentation covering all stages of an AI system's lifecycle, including, e.g., design and planning; data collection and processing; architecture/model choice, model building, training, testing and validation; deployment, operation, modification and monitoring; algorithms used; and decommissioning plan?	• What mechanisms ensure comprehensive traceability and auditable recordkeeping for AI-driven decisions? • Does the firm use different tools for traceability and audit depending on the AI systems type (e.g., ML or LLM based)? • How does the firm record and track modifications to AI systems over time? Does the firm maintain a copy of the models used and modified during the time (model versioning)? • What processes ensure lifecycle documentation remains current and complete both for proprietary AI systems and third-party AI systems?	• Documentation and logs across the AI system lifecycle. • Records of AI model choices per use case, or for proprietary models, model architecture choices and rationale. • Change management records for AI system updates.
2. Documentation of Business Objectives Related to AI	• Does the firm clearly document the business objectives behind AI adoption, including expected benefits, risk considerations, and alignment with strategic goals?	• What business objectives does this AI system support, and how are they documented? • How does the firm ensure AI objectives align with your overall risk management framework?	• Business case documents for AI projects, including any board-approved papers referencing AI objectives.
3. Documentation of AI-Generated Outcomes	• Does the firm maintain records of AI-generated outcomes, focusing on investor or market impacting use cases?	• What processes are taken to review and document AI outputs on a periodic basis?	• Documentation and logs of validation, testing, and monitoring procedures, internal reports, and

Area	Considerations	Examples of Questions	Information Sources
		• What audit trail does the firm maintain for AI-system outcomes in investor or market impacting use cases? • What processes ensure traceability between AI outputs and final actions taken? • How does the firm document and retain evidence of AI-generated outcomes? • How does the firm document and retain evidence of human oversight or intervention in decisions made by AI systems, particularly in investor or market impacting AI applications?	documentation of algorithms and decision pathways used in AI systems.
4. Documentation of Explainability of AI Outputs	• Does the firm maintain records that explain how AI systems generate outputs, including decision-making logic and reasoning?	• To what extent can the firm meaningfully explain the outcomes of the AI systems? How are these explanations tailored for different stakeholders (end-users, Board and senior management, supervisors)? • How does the firm ensure explanations are accurate, fair, and free from bias taking into account the explainability techniques used to enhance human understanding of the Ai systems? • How does the firm document the logic behind AI-generated decisions? • What records demonstrate the firm's ability to explain AI outputs to stakeholders? • What evidence does the firm maintain to show that explanations of AI outputs are accessible and understandable to non-technical stakeholders, such as retail investors?	• Internal guidelines for interpreting AI outputs and audit trails showing human validation of AI outputs.

Area	Considerations	Examples of Questions	Information Sources
		• Does the firm use different tools for tracing explainability and interpretability?	
5. Records on Incidents relating to AI products or services	• Does the firm have policies and procedures for recording and reporting incidents that note whether these incidents included the use of AI systems? • Does the firm keep records of operational failures, misconduct, or security breaches, and maintain detailed records of AI-related incidents, including root cause analysis and remediation actions?	• Are incident logs and monitoring records maintained in a manner that enables effective supervisory review and supports accountability for AI system outcomes? • Does the firm periodically review and update its incident management policies and procedures to reflect lessons learned from past AI-related incidents and evolving regulatory expectations? • What thresholds does the firm maintain for an AI-related incident to be reportable? • Does the firm's business continuity procedures consider a response plan to incidents (e.g., identification of an incident, steps taken to address and remediate, any escalation procedures or steps, documentation of an incident)?	• Policy for recording and reporting AI-related incidents. • Records of AI-related incidents over the past 12 months. • Records of remediation.
6. Reporting	• Does the firm comply with relevant jurisdictional reporting requirements, to provide the supervisory authority with appropriately frequent, timely and high-quality reporting across the areas listed above?	• What reporting processes are in place to ensure timely and high-quality reporting on AI in line with relevant reporting requirements? • What constitutes an AI-related reportable incident within the firm? Does the firm define this in its internal rules or guidelines? • What reporting mechanisms cover third-party or external data dependencies? • How does the firm notify supervisors of significant AI failures, biases, cybersecurity events, data breaches, or incorrect outputs?	• Incident management policies, including those specific to AI. • Templates for incident reporting to authorities. • Incident documents and logs with timestamps and impact assessments, including root cause analysis reports for AI failures.

Area	Considerations	Examples of Questions	Information Sources
		• What criteria determine whether an AI system requires mandatory notification or prior approval?	

Table 7: Key indicators for supervisory oversight of AI use

Indicator	Purpose
AI adoption	
Proportion of supervised firms that use AI technologies	This provides an overview to the supervisory authority of how widespread AI use is across supervised firms and use cases. Through understanding AI use across sectors of firms, supervisors can analyse AI adoption patterns.
Proportion of use cases in development vs those deployed in production	This distinguishes between experimental projects and active systems affecting business outcomes, to assess current vs. emerging risk exposure. Supervisors could classify firm usage in three categories: (i) using AI in production, (ii) experimenting with AI and (iii) not using AI, to facilitate monitoring of: • Conversion rate of experimentation to production deployments. • Growth rate of production use cases. Adoption rate of AI based on firms moving from not using AI to experimenting with AI to using AI in production.
AI technologies Research and Development (R&D) spending	• By understanding the amount invested in AI technologies R&D over past years or forecast for future years, supervisors can understand the likely growth trajectory in AI use in supervised firms, as well as its relative priority to a particular firm.
Number of AI-related patents/patent applications by a firm or sector	Similar to R&D spending, this metric can provide an indication of internal research and investment focused on AI and whether proprietary AI systems are being prioritized by a particular firm or sector.
Nature and use cases of AI systems	
Detailed inventory of the AI use cases and AI system type in development and deployment	By categorizing AI systems by use case and system type, supervisors can understand how AI is being used across firms in a spectrum of use cases.
AI system-related attributes	Information concerning core attributes of an AI system, including specific underlying models, technical specifications, and linkages to products/services can promote an understanding of how an AI system is used and its potential risks.

Indicator	Purpose
Third party dependencies and concentrations	Supervisors may also wish to consider information on the proportion of AI systems and use cases of those systems that are supported through third party AI service providers vs internally developed. Supervisors may also want to understand across firms the level of dependency on and concentration in specific third-party providers for specific AI systems, as well as the dependencies on and concentrations in those third-party providers for the firm as a whole (e.g., what other systems or services the third-party provides to the firm).
AI system performance	
Frequency and severity of incidents in AI systems	Information tracking failures, errors, outages, cyber incidents, data breaches, instances of frauds/misconduct and malfunctions in AI systems can identify reliability and safety concerns, including their business impact, duration, and affected investors/end users.
Model performance validation and monitoring metrics	Information concerning a firm's ability to identify and track key performance indicators such as prediction accuracy, error rates, and model drift and degradation over time can enable early identification of underperforming systems.
Examples of sector specific metrics[1]	
Broker-dealers	Incidents or alerts of AI-driven mis-selling or unsuitable recommendations requiring human intervention. Bias or fairness indicators in recommendation or communication tools. Input/output correlation metrics, checking whether small changes in input lead to disproportionately large, erratic, or unexplained changes in system output.
Asset Managers	Accuracy or consistency of AI-supported valuations relative to market benchmarks. Incidents or alerts of AI-driven mis-selling or unsuitable recommendations.

[1] These are examples of indicators that may help monitor specific risks of AI use cases in each sector from the 2025 AI Report but are not exhaustive, nor are they intended to be prescriptive.

Indicator	Purpose
	Indicators of mandate or portfolio-construction drift attributable to AI-generated outputs. Level and frequency of human intervention in AI-driven investment process. Accuracy or consistency of risk profiling of clients, and suitability of AI-supported asset allocation and investment recommendation relative to client profiles in the context of robo-advisers.
Exchanges and Other Financial Market Intermediaries	Market quality measures (e.g., bid-ask spreads, price impact) where AI-driven systems influence order routing or matching. Effectiveness of AI-driven surveillance systems in detecting market manipulation, insider trading, and other misconduct. Market volatility or instability patterns associated with AI-driven trading systems. Accuracy or consistency of AI-supported models for financial risk management by market infrastructure providers. Trade matching and settlement failures arising from AI automation in processes.

Data sources

To support oversight of financial institutions and collection and analysis of the indicators highlighted above, supervisors may consider a variety of data sources, tools, and techniques. As highlighted in the FSB 2025 report[2] and corroborated by the Survey responses, data is most often collected through:

- Supervisory reporting and data collection during examination and inspection: Data collected through supervisory reporting, examination, and inspection can include AI-related data where feasible. Such data, especially when collected on a regular basis, can enable quantitative and qualitative analysis of AI use by supervised firms.

- Regular and structured outreach and engagement with firms through supervisory engagement: Direct engagement with firms can enhance understanding of how AI systems are being used in financial products

[2] FSB 2025 report.

and services and where risks may emerge, while at the same time reinforcing regulatory requirements and expectations.

- Surveys of market participants: While surveys are used infrequently by supervisory authorities, according to the Survey results, sector-wide surveys can promote effective monitoring, covering AI inventories, third-party dependencies and concentrations, and AI-related investments, with survey designs that remain consistent yet adaptable, timely, and forward-looking to capture emerging developments.

- Research on publicly available information: Public reports (e.g., annual reports, press releases, company disclosures, industry, and sector reports) can provide information ahead of more focused engagement.

- Real-time monitoring tools used by supervisors: Only a few authorities reported employing real-time capabilities, including systems to analyze trading behavior through AI-powered detection tools. Real-time monitoring implies a cost-benefit assessment, but cross-border information sharing can help reduce the costs and frictions in developing such capabilities.

- AI tools: While most IOSCO members responding to the Survey indicated that they are not currently using AI systems to support their monitoring activities, a few do use AI systems for analyzing data from routine monitoring or public filings, to detect outliers, anomalies, or to scan available data for relevant information. Analyses reportedly are carried out by using both commercial and internally developed tools.

- Enhanced information sharing among national or cross-border authorities: Such information sharing can help to minimize duplication and improve coverage and comparability.

- Sandboxes, innovation hubs, and other initiatives: Some IOSCO members are using other ways to gather information on AI use in firms, including through engagement and outreach to industry, market participants, and others.[3]

[3] For instance the UK FCA has launched its AI Lab initiative and live AI testing service: FCA set to launch live AI testing service | FCA.