Artificial intelligence in compliance and supervision

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland and Germany),
Solicitor (England & Wales and Hong Kong)
Of Counsel, KGP Legal LLC
alexander.ressos@kgplegal.com.sg
www.ressos.com.sg

Transaction monitoring and financial crime

Compliance is one of the most promising and most delicate fields for artificial intelligence. Traditional transaction monitoring systems generate large numbers of alerts, most of which prove unfounded after manual review. Machine-learning models can rank alerts by their likelihood of being genuine, detect patterns across accounts and analyse unstructured information such as news reports. MAS observed that banks commonly use such models in anti-money laundering systems and fraud detection. The regulatory danger is symmetrical. A model that suppresses genuine alerts exposes the bank to breaches of the anti-money laundering rules examined in Part H. A model that cannot explain its result is hard to defend before a supervisor or a court. MAS lists regulatory risk among the main risks of artificial intelligence and gives the example of poor performance in a model used to support anti-money laundering efforts.[1]

The data on which such models depend has also changed. Since 1 April 2024, six major commercial banks have been able to share information on customers who show multiple red flags through COSMIC, a digital platform that MAS launched

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

with them under the Financial Services and Markets (Amendment) Act 2023. Its initial focus is the misuse of legal persons, the misuse of trade finance and proliferation financing.[2] A platform of this kind is a source of structured signals that analytical models can exploit. Its legal framework and its significance for the fight against money laundering are discussed in Part H.

Third-party models and concentration

Most institutions buy their generative models from a small number of global providers. MAS identified three resulting risks: unknown biases from pre-training data, data protection concerns and concentration risk, where many institutions depend on the same underlying models. Banks responded with compensatory testing, contingency plans and revised contracts that provide for performance guarantees, data protection, audit rights and notification when a provider introduces artificial intelligence into an existing service.[3]

The final Guidelines settle the principle. An institution may be unable to compel a third-party provider to adopt robust risk management practices. It nonetheless remains accountable for how third-party AI is used within its organisation and for the possible impact on customers and other stakeholders.[4] The rules on outsourcing and technology risk management, examined in Chapter E.I, apply alongside.

Incidents, monitoring and contingency

The Guidelines define AI incidents as incidents involving a failure, malfunction or poor performance of the underlying system or model. MAS decided against a separate reporting regime for them. Institutions must continue to report incidents under the existing technology risk and business continuity requirements, whatever their root cause. Contingency plans are required for use cases of high risk materiality. Models that update themselves automatically, such as reinforcement-learning systems, call for more stringent monitoring, because their behaviour can evolve during operation without human involvement.[5]

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

For agentic systems, monitoring is to extend to the information flows and decision paths across workflows, including reasoning processes, actions taken and tools used. Such monitoring allows an institution to reconstruct individual actions across chains of agents and to locate the source of a failure. MAS also suggested that the extent of access to tools and systems may serve as an additional dimension of risk materiality, because agents with wide permissions can compound the risk of data compromise.[6]

The supervisor's own use of data

MAS has applied data analytics to its own work since it created the post of Chief Data Officer, which David Hardoon held when the FEAT Principles were published. Supervisors use analytical tools to process regulatory returns, to screen suspicious transaction reports and to detect patterns of market abuse.[7] The supervisory relationship itself is unchanged by these tools. They help the supervisor to select the institutions and transactions that deserve attention, while the assessment remains a human judgment exercised under the statutes described in Chapter E.I.

Notes

1. MAS, Information Paper, December 2024, para 2.1: decision-tree-based ML models are "commonly used in anti-money laundering (AML) systems to detect suspicious transactions, and in fraud detection systems" – MAS, Information Paper, December 2024, para 2.2: "Regulatory risks, e.g., poor performance of AI used to support AML efforts could lead to non-compliance with regulations." ↩
2. MAS, "COSMIC" (mas.gov.sg, accessed November 2026): launched on 1 April 2024; participants DBS, OCBC, UOB, SCB, Citibank and HSBC; legal basis in the Financial Services and Markets (Amendment) Act 2023 and the Financial Services and Markets (Information Sharing Scheme for Prescribed Financial Institutions) Regulations 2024; three risk areas. ↩

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

3. MAS, Information Paper, December 2024, para 7.2.1: risks from third-party AI include "unknown biases from pre-training data, data protection concerns, as well as concentration risks due to increased interdependencies" – MAS, Information Paper, December 2024, para 7.2.2(a)–(d): compensatory testing, contingency planning, legal agreements with clauses on "performance guarantees, data protection, the right to audit, and notification when AI is introduced", and awareness efforts. ↩
4. MAS, Response to Feedback, 7 October 2026, paras 9.3–9.4: the FI "remains accountable for how third-party AI is used within its organisation"; "the onus is on the FI to ensure that risks arising from its use of third-party AI are appropriately managed". ↩
5. MAS, Response to Feedback, 7 October 2026, para 10.69: definition of "AI incidents"; "MAS does not intend to introduce AI-specific incident reporting requirements at this juncture" – MAS, Response to Feedback, 7 October 2026, paras 10.67 and 10.70. ↩
6. MAS, Response to Feedback, 7 October 2026, para 12.8 – MAS, Response to Feedback, 7 October 2026, para 7.7: an FI may consider "the extent of access to tools and systems granted as an additional dimension for AI risk materiality assessments of agentic AI". ↩
7. On MAS's use of data analytics and machine learning in supervision and in the analysis of suspicious transaction reports, see the MAS annual reports from 2018/19 onwards and speeches by MAS officials on supervisory technology. ↩

Disclaimer

This article is provided for general information only. It is based on publicly available sources as at its date of publication. These sources have not been independently verified against licences, regulatory registers or the records of the entities concerned. It is not legal, tax, financial or investment advice. Nor is it a recommendation to invest in, transact with or use the services of any entity mentioned. Law and regulation change frequently, so the content may be incomplete or outdated. To the fullest

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

extent permitted by law, Dr Alexander Ressos and the publisher of SingaporeIQ exclude all liability for loss or damage arising from the use of or reliance on this article. Readers should obtain advice on their specific circumstances before acting or refraining from action.

Names and trademarks of the entities discussed belong to their owners and are used for identification only. Their mention implies no endorsement, affiliation or allegation of wrongdoing. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. Corrections and updates: contact@ressos.com.

© 2026 Dr Alexander Ressos. This article may be quoted with attribution to SingaporeIQ (SingaporeIQ.com). Reproduction in full and any commercial use require prior written consent. The Legal Terms at https://singaporeiq.com/legal-terms apply.

Author contact: Dr Alexander Ressos, TEP · contact@ressos.com

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.