From reactive to proactive

How managing regulatory compliance is improved with AI

Contents

Executive summary

Proactive compliance represents a fundamental shift in how financial institutions approach regulatory risk. Where reactive compliance focuses on responding to violations, audits, or regulatory change after the fact, proactive compliance anticipates risks, aligns controls to business realities, and demonstrates resilience before threats materialize. The difference is prevention versus detection; strategically deploying resources to manage risk effectively while enabling safe, sustainable growth.

Why this shift matters now

This shift matters now more than ever. Regulatory complexity is accelerating across financial crime domains, while criminal networks are becoming faster, more adaptive, and more sophisticated.

A reactive, one-size-fits-all approach (relying on static rules, generic customer categorization, and manual reviews) inevitably produces risk management inefficiencies, including over-monitoring low-risk customers, underestimating high-risk behavior, and creating alert fatigue among the already stretched resources of compliance operations teams. Worse, it leaves institutions exposed to both operational costs and reputational damage when risks slip through the net.

In contrast, proactive compliance leverages AI to operationalize the risk-based approach (RBA), which focuses on identifying, assessing, and mitigating money laundering risks based on the specific characteristics of customers and transactions, allowing for more efficient allocation of resources.

By continuously monitoring data, learning from patterns and emerging behaviors, and automating lower-value tasks, AI enables compliance teams to focus where risk is greatest, whether at the customer, product, transaction, or enterprise level. This moves RBA from policy theory to everyday practice, delivering agility in adapting to new threats, defensibility in regulatory examinations, and scalability across increasingly complex operations.

The payoff for financial institutions

For financial institutions, the payoff is significant with enhanced detection of sophisticated financial crime by providing a more efficient use of AI and the expertise of investigators, who can focus on higher-level risk management – including mitigation and prevention.

Improving detection and investigator efficiency is easily measured, allowing leaders to re-assign capacity, as necessary. Alongside this, such an approach also helps to provide regulators with clear, data-driven evidence of credible, risk-justified decision-making, with accessible audit logs to enhance consistency.

Proactive, AI-enabled compliance is no longer optional but a strategic imperative. It transforms compliance from a cost of doing business into a competitive advantage, strengthening resilience against financial crime while ensuring that regulatory expectations are not only met but exceeded.

> “By anticipating risks, scaling resilience, and enabling sustainable growth, proactive, AI-enabled compliance transforms regulation from a reactive cost burden into a strategic advantage.”

Regulatory change

The current challenge

The acceleration of regulatory demands

The pace and complexity of regulatory change has never been greater. Global AML authorities, from the Financial Action Task Force (FATF) and Wolfsberg Group and regulators across regions, are issuing an unprecedented volume of updates, guidance, and new standards. These span across sanctions evasion detection, ultimate beneficial ownership transparency, emerging typologies in investment scams and cross-border services, AI risk management, and heightened expectations around outcome-focused compliance. Across all of these, the message is consistent: compliance must be effective, outcomes-focused, risk-based, and dynamic.

Rising expectations for judgment and outcomes

The implication from this regulatory messaging is that static, volume-driven compliance programs are no longer acceptable. Regulators are increasingly scrutinizing how risk decisions are made:

- **What** information is collected
- **Why** it is collected
- **How** it is critically assessed in context of risk.

Regulators expect financial institutions to demonstrate judgment that is proportionate to their customer base, business model, and geographic footprint. The Monetary Authority of Singapore (MAS) have recently released AML/CFT Supervisory Expectations to help in this regard, offering best practice advice for financial institutions based on recent assessments. High-profile enforcement actions, such as AUSTRAC's Mounties case in Australia, underscore the risks of weak frameworks that prioritize process over outcomes – and mismatch the high likelihood of risk occurring with a reactive and overly basic financial crime program.

The breaking point of traditional models and finding the path forward

This shift also exposes the operational limits of current compliance models. The constant cycle of "regulatory catch-up" is costly, exhausting for compliance teams, and increasingly unsustainable. The simple truth is that reliance on manual monitoring, documentation, and gathering evidence drives up costs and creates fatigue and blind spots. This leaves institutions exposed to regulatory, operational, and reputational risk. As supervisory bodies pivot from periodic reviews to expectations of continuous adaptation, the traditional playbook of incremental adjustments has reached its breaking point.

The solution? Adopting proactive, technology-enabled frameworks that embed agility and intelligence into compliance processes. By using automation, data-driven insights, and AI-driven monitoring, institutions can move beyond reactive firefighting to anticipate risks, allocate resources efficiently, and continuously align with evolving regulatory expectations. In this environment, the ability to demonstrate effectiveness, not just adherence, becomes a key differentiator in managing regulatory risk and maintaining institutional resilience.

> "With regulatory change accelerating beyond the limits of manual compliance, institutions must embrace agile, technology-driven frameworks that go beyond adherence and actually prove effectiveness."

Regulatory intelligence with AI

The problem with static compliance

AI-powered regulatory intelligence platforms such as Symphony Risk Intelligence (SRI) are redefining how financial institutions profile and manage risk. Traditional compliance frameworks rely on static, periodic reviews that leave long gaps between regulatory updates, internal assessments, and operational changes. Because of this, it often takes months from the release of new guidance to full implementation across the business. This lag exposes institutions to heightened risk and undermines both compliance effectiveness and credibility with regulators.

What is SRI?

SRI is a cloud-native, AI-led anti-financial crime platform designed to reduce the total cost of compliance by embedding predictive, generative, and agentic AI into financial crime workflows. By intelligently automating and optimizing end-to-end processes, SRI empowers institutions to manage financial crime risk more efficiently and effectively, reinventing the compliance operating model. Respond rapidly to regulatory change, enhance detection, and drive faster business growth with a next generation risk and compliance platform.

A modular product, SRI allows for automating at least 50% of the workload with intelligent, scalable AI with build-your-own agent capabilities, freeing up human investigators to put their expertise into higher value areas. Able to integrate and augment from any data source, standardize and centralize data asset management, provide self-serve risk models, and unify operations, it is an evergreen platform that futureproofs your tech stack.

How SRI closes the gap

SRI closes this gap by enabling continuous, comprehensive risk profiling across different levels. Instead of relying on broad, generic categorizations, AI ingests diverse, dynamic data from customer demographics and behavioral patterns to product usage anomalies, geopolitical developments, and sanctions updates. This data is continuously scored and re-scored in near-real time, allowing institutions to detect subtle shifts in risk before escalating.

Multi-level risk intelligence

This capability is best understood through a multi-risk intelligence framework. By applying AI-driven analysis across different layers of risk exposure – customers, products, transactions, and the enterprise - SRI ensures that risks are assessed in context, monitored dynamically, and addressed proportionately. Each layer builds on the others to create a complete, real-time view of institutional vulnerability and resilience.

- **Customer-level:** AI personalizes monitoring by dynamically adjusting risk scores based on behavior, network associations, adverse media, or new data inputs. This ensures that low-risk customers are not over-monitored while high-risk ones receive focused attention.

- **Product-level:** Risk is differentiated across products, with anomalies (such as unusual spikes in cross-border payments) triggering recalibrated thresholds and tailored controls.

- **Transaction-level:** Machine learning models detect atypical activity that static rules would miss, contextualizing alerts within customer and peer group behaviors to reduce false positives.

- **Enterprise-level:** By integrating AML, sanctions, fraud, and cyber risk data, AI delivers a holistic view of institutional exposure, supports scenario testing, and informs strategic adjustments.

This intelligence translates directly into agility for compliance teams and infrastructure. Where regulatory changes or new typologies once required weeks or even months to assess, approve, and implement, SRI's agentic AI capabilities compress this process into days. Teams can model the impact of regulatory text changes, update processes, and validate adjustments in near real time. This allows for continuous - not periodic - adaptation, with workflows and business logic recalibrated effortlessly as risks evolve.

Business benefits

The benefits include:

- Reduced lag between regulation and response
- Faster detection of emerging risks
- Lower compliance fatigue
- Stronger defensibility in the eyes of regulators

With AI-powered platforms like SRI, financial institutions shift from reactive catch-up to proactive risk management at scale. They strengthen their resilience, reduce costs, and demonstrate an outcomes-driven approach to compliance.

> “AI-powered regulatory intelligence transforms compliance from slow, reactive catch-up into continuous, proactive risk management at every level of the institution.”

Strengthening regulator relationships through transparent RBA

The inadequacy of traditional compliance models

AI-powered risk-based approaches (RBA) are transforming the relationship between financial institutions and their regulators. Traditionally, compliance has been defined by a detect-and-report model, with firms submitting static reports and regulators assessing compliance retrospectively. This model is increasingly inadequate in a world of accelerating threats and regulatory expectations. What regulators now demand, and what AI makes possible, is continuous, transparent, and evidence-based oversight.

Transparent, auditable decision-making

Platforms such as SRI operationalize this by creating clear, auditable chains from risk identification through mitigation and resolution. Every step from data ingestion to alert generation, escalation, and remediation is logged, explainable, and verifiable. This transparency enables regulators to see not just whether an institution is compliant, but how it is making risk-based decisions, how quickly it responds to emerging threats, and how controls are adapted over time. Enhanced reporting and dashboards provide regulators with dynamic views of program effectiveness across customers, products, transactions, and enterprise exposures.

Crucially, AI-powered RBA fosters a more collaborative, data-driven dialogue with regulators. Instead of box-ticking or after-the-fact confirmations, institutions can proactively share evidence of continuous improvement, whether in response to new typologies, evolving sanctions, or geopolitical events. Meanwhile, regulators can test the resilience of programs in real time, even using synthetic data or scenario analysis, while compliance teams can Demonstrate governance maturity and program adaptability.

Compliance as a strategic enabler

This moves compliance from being seen as a defensive exercise to viewing it as a strategic enabler. By evidencing effective, explainable, and continuously improving risk management, institutions earn regulator trust, reduce the likelihood of intrusive intervention, and streamline examinations. At the same time, they strengthen their own resilience by embedding a culture of accountability and proactive stewardship. AI-powered RBA therefore provides regulatory assurance as well as a foundation for a more constructive partnership between institutions and supervisors, built on shared data, transparency, and a commitment to disrupting financial crime.

> "Regulators now expect transparency, speed, and evidence-based oversight. This shifts compliance from static reporting to continuous collaboration."

Conclusion
Business values and outcomes

The necessity of AI-powered compliance and its many benefits

The shift from reactive compliance to an AI-powered, risk-based approach is no longer a choice but a necessity. The accelerating pace of regulatory change and the growing sophistication of financial crime demand compliance frameworks that are continuous, adaptive, and explainable. By embedding AI into the core of compliance operations, institutions can achieve demonstrable results, timely compliance, strengthen their overall risk posture, and foster more constructive relationships with regulators.

Key considerations for leaders

For leaders considering the journey to AI-native compliance, several key considerations stand out:

- New capabilities must be aligned with existing governance, risk, and compliance structures to ensure consistency, auditability, and scalability.
- Integration with legacy systems and data sources is essential, as is equipping teams with the skills to oversee and interpret AI outputs responsibly.
- A phased adoption approach - starting with high-impact, low-friction use cases and expanding to enterprise-wide orchestration - can deliver early wins while building organizational confidence and resilience.

Turning compliance into a competitive advantage

SRI enables a clear transformation within financial crime management. By operationalizing risk-based compliance at scale, it allows institutions to anticipate regulatory change, demonstrate continuous improvement, and embed a culture of accountability.

The result? A compliance function that safeguards against financial crime, enhances credibility with regulators, and turns compliance from a cost center into a source of resilience and competitive advantage.

About Symphony Risk Intelligence

Symphony Risk Intelligence (SRI) is an AI-native FinCrime platform that's designed to help financial institutions move from reactive to proactive risk management. It centralises and optimizes every aspect of compliance operations, from data ingestion and model management to investigation and reporting.

Every layer of the cloud-native platform has been built to leverage the latest predictive, generative, and agentic AI technology to enable greater automation, improved detection effectiveness, and significant operational efficiency savings.

SRI represents a reimagining of the compliance operating model, built to eliminate legacy inefficiencies, unify fragmented systems, and turn compliance into a driver of business growth. With the ability to automate a wide range of processes and operational tasks, SRI halves the compliance workload while equipping teams with powerful AI-driven tools to accelerate workflows and maximise performance.

SRI allows financial institutions to begin their transformational journey to a next generation, evergreen infrastructure that futureproofs payment ecosystems and prepares businesses to scale with speed, efficiency, and regulatory resilience.

SymphonyAI

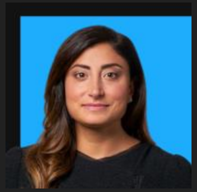
symphonyai.com

About SymphonyAI

SymphonyAI, 2024 Microsoft Partner of the Year for Business Transformation– AI Innovation, is building the leading enterprise AI SaaS company for digital transformation across the most critical and resilient growth verticals, including retail, consumer packaged goods, finance, manufacturing, media, and IT/enterprise service management. SymphonyAI verticals have many leading enterprises as clients. Since its founding in 2017, SymphonyAI has grown rapidly to 3,000 talented leaders, data scientists, and other professionals. SymphonyAI is an SAI Group company, backed by a $1 billion commitment from Dr. Romesh Wadhwani, a successful entrepreneur and philanthropist.

SymphonyAI provides AI-focused SaaS solutions developed from the ground up for fighting financial crime. An end-to-end offering compiled from more than 25 years of knowledge in tackling money laundering and fraud, our award-winning product ecosystem comprises an innovative and modern approach to financial crime investigation using world-leading agentic, predictive, and gen AI. From KYC/CDD and transaction monitoring through to payments fraud, entity resolution, and sanctions, PEP, and adverse media screening, SymphonyAI is a trusted name in finance technology with more than a third of the world's top 100 banks enjoying the power, efficiency, effectiveness and productivity that our solutions provide.

Authors



Craig Robertson

Financial Crime & Compliance SME, APAC

craig.robertson@symphonyai.com

Charmian Simmons

Financial Crime & Compliance SME, EMEA

charmian.simmons@symphonyai.com

Elizabeth Callan

Financial Crime & Compliance SME, NA

elizabeth.callan@symphonyai.com