How AI Is Rewriting the Compliance Playbook

70% of organizations believe regulatory change will outpace their ability to adapt within the next three years.[1]

The compliance function risks becoming a bottleneck to innovation if it fails to evolve. Today, only 20% of firms have compliance teams empowered to act as true strategic partners rather than tactical enforcers. As a result, most organizations remain constrained by a function built to protect, not propel.

The next evolution of compliance management is powered by technology, with artificial intelligence (AI) at its core.

Compliance is losing ground to the speed and depth of regulatory change

It's not only the pace of regulatory change that firms are struggling with, but the increasing technical depth of the rules themselves. 85% of CCOs feel compliance requirements have grown in complexity since 2022,[2] and "keeping up with regulations" is the number one cause of rising GRC costs.

Rules now go beyond principles-based requirements and impose detailed operational expectations. Recent reforms across financial crime, data protection, operational resilience, ESG, and cybersecurity share common features:

1. Stricter incident reporting obligations: Regulators now impose defined timeframes, escalation triggers, and cross-border notification rules.

2. Granular technical and operational controls: Rules increasingly specify the baseline measures firms must maintain, from encryption standards and access controls to testing, monitoring, and vendor oversight.

3. Accountability at the top: Senior leaders must approve risk measures, ensure compliance with evidence, and drive training across the enterprise.

4. All-hazards approach to risk: Regulators expect firms to consider a broad spectrum of threats, recognizing that one incident can quickly cascade into multiple risks across the extended enterprise.

1. https://www.int-comp.org/insight/navigating-the-future-the-role-of-governance-risk-and-compliance-in-modern-business/
2. https://www.pwc.com/gx/en/issues/risk-regulation/global-compliance-survey.html#:~:text=It%20is%20not%20surprising%20that,consumer%20arkets%20%2883

SAI360
RISK FROM EVERY ANGLE

Example regulatory areas are shown in the table below: [3]

Artificial Intelligence	**EU AI Act**	Classify AI models based on intended use, assessing risk levels accordingly. High-risk applications— such as credit assessments or medical disgnostics—require robust risk management systems, technical documentation, human oversight mechanisms, continuous validation, and cybersecurity controls.
Operational Resilience	**DORA/CPS230**	End-to-end resilience measures, including regular risk assessments, scenario testing, full business continuity planning, and incident reporting.
Cybersecurity	**NIS2/SEC Disclosures**	Establish documented risk assessment methodologies, implement and test incident response plans, and define processes for identifying, reporting, and remediating vulnerabilities. Compliance training must be provided at all levels, with clear audit trails for verification.
Third-Party Risk Management	**All of the Above**	Requirements now extend beyond regulated entities to include the security and resilience of their suppliers. Firms must conduct third-party due diligence, enforce contractual obligations, and implement continuous monitoring to manage operational risk across the supply chain.
Climate Disclosures	**CSRD/CSDDD**	Implement structured sustainability reporting with auditable disclosures on environmental and social impact.
Human Rights Disclosures	**Sapin II/ German Supply Chain Act**	Impose due diligence obligations to ensure ethical supply chain practices and prevent human rights violations.

3 https://www.sai360.com/the-future-of-compliance-management-is-integrated

Traditional compliance approaches are under pressure

Legacy approaches simply cannot keep up. They are slow, reactive, and expensive. Nearly two-thirds of CEOs believe regulation hinders value creation,[4] and global enforcement topped $19 billion in 2024, much of it tied to control failures[5] – evidence that compliance is negatively impacting both the top and bottom line.

Firms cannot afford to increase GRC investment in perpetuity to match rising regulatory demands. Instead, they must seek more strategic ways to allocate capital to deliver faster time-to-insight and reduce the compliance overhead.

This calls for greater adoption of analytics and automation. AI is emerging as the cornerstone of the next evolution in compliance management. It offers not just efficiency gains, but a fundamentally new way to identify, assess, and mitigate risk in real-time.

Artificially intelligent compliance: mastering the speed and complexity of regulation

Traditional analytics are powerful at detecting known risks; those that an organization already understands and can define in parameters. AI's advantage lies in surfacing the unknown unknowns by learning patterns directly from data. This flips the human-to-machine dynamic: instead of telling technology what to look for, AI now reveals what we should be paying attention to. Several core compliance domains stand to benefit significantly:

Risk management

- **Assessing risk:** Machine learning provides the capability to analyze larger and more complex datasets (loss events, control test results, or external incidents) to more accurately and proactively determine the impact and likelihood of risk events.
- **Surface new risk:** Anomaly detection and unsupervised learning spot unusual patterns that may not have been coded into existing rules-based systems. This enables "always on" risk monitoring. Fraud detection is an area where this capability is already mature: combining behavioral profiling, graph analytics, and unstructured signals such as device metadata or communication patterns to identify bad actors.
- **Risk forecasting:** Predictive models trained on historical incidents, audits, and control data can forecast where breakdowns are most likely to occur, highlighting control fatigue or resource gaps before they escalate into compliance breaches.

Training and learning

True personalization: Traditional personalization has been limited to segmentation - users assigned to specific groups defined by role, geography, seniority, etc, and given variations of modules.

AI allows for true personalization, continuously learning from individual behavior and outcomes. It can analyze what questions users struggle with, how learners interact with ethical scenarios, or surface a correlation between training engagement and actual compliance outcomes.

Content can be adjusted in real time based on user characteristics - serving targeted micro-lessons, reinforcement prompts, and follow-ups. That means better compliance outcomes and more user engagement.

Whistleblowing

Although AI cannot access or process the encrypted content of whistleblower reports, it can significantly enhance the surrounding processes.

- **Drafting and customizing reporting forms:** AI can generate and adapt forms for specific use cases, such as fraud, money laundering, or human rights violations in the supply chain. This allows organizations to expand or tailor their reporting channels without manual redesign.
- **Automating report routing:** AI can help categorize and prioritize reports from whistleblower hotlines. When a report concerns specific issues (e.g., potential AML breaches), AI can automatically route it to the appropriate officer, such as the AML or compliance team, ensuring timely handling.

4 https://www.pwc.com/gx/en/ceo-survey/2024/download/27th-ceo-survey.pdf

5 https://www.corlytics.com/enforcement-reports/

Generative AI is broadening the conversation around value creation

Generative AI has garnered significant attention, unlocking contextual understanding and introducing entirely new ways for users to interact with data.

There's enormous potential for this technology to tackle one of compliance managers' biggest headaches: large-scale text analysis and insight extraction. Some example use cases include:

Use case	How generative AI helps
Horizon scanning	Interpret regulatory sources, legal databases, and industry publications. Highlight amendments, additions, and deletions between successive versions of regulations.
Compliance gap analysis	Scan internal policies and map them to relevant regulatory clauses. Identifies overlaps, inconsistencies, and areas of non-compliance.
Policy generation and maintenance	Draft policy language aligned to new requirements, leveraging regulatory text, supervisory guidance, and internal standards.
Internal audit assistance	Automate processing and analysis of audit evidence. Instantly query evidence using natural language, reviewing documents like SOC2 reports, accelerating workflows, and ensuring accuracy without manual intervention.
Communications monitoring	Enhances traditional keyword filters by detecting intent, sentiment, and nuance in unstructured communications to surface more nuanced suspicious behavior.
Detect emerging risk outside of your organization	Continuously scan global sources to detect and categorize emerging risks in real time. Entity-level sentiment analysis and risk scoring to evaluate severity, urgency, and relevance.
Investigative co-pilots	Advanced virtual assistants perform inference over the organization's knowledge base (data) in real time, answering questions, generating insights, and guiding compliance teams with recommendations.

Despite the benefits, AI adoption is still lagging

AI offers a way out of compliance's speed-and-complexity trap. It enables teams to keep up with regulatory change, understand how new rules impact the business, and focus effort where it matters most. This isn't about replacing humans; it's about augmenting them with better training, clearer insights, and operational support with labor-intensive tasks.

In short, AI equips compliance functions to do more, with greater confidence and precision.

But adoption remains in its early stages. Only 1.6% of organizations have fully integrated AI into their GRC processes, while around a third report being in the "early stages" of adoption. Another third had not yet deployed AI in compliance at all.[6]

Building confidence in AI-driven compliance

AI carries real risks, from biased outputs and hallucinations to poor performance on edge cases. Frameworks for governing these systems are still maturing, and many organizations lack the data infrastructure to deploy AI safely and effectively.

The first step toward responsible AI adoption is data readiness. AI's effectiveness depends on access to clean, high-quality, and well-governed data. Yet many organizations remain constrained by fragmented systems and siloed information, limiting AI's ability to generate reliable insights. Poor data quality undermines both performance and trust. Consolidating risk, control, and incident data within a single GRC platform establishes the foundation for accurate insight, robust governance, and auditable outcomes.

Once this foundation is in place, organizations can introduce AI incrementally, embedding it within established compliance workflows such as risk assessments, policy mapping, or training analytics. This phased approach allows firms to measure impact, strengthen oversight, and build confidence in AI-driven compliance, one use case at a time.

6 https://www.int-comp.org/insight/navigating-the-future-the-role-of-governance-risk-and-compliance-in-modern-business/

Empowering modern compliance with AI

The fundamental challenge for compliance today is one of speed and complexity. Traditional systems rely on human bandwidth and rule-based automation, both limited by predefined logic and manual capacity.

AI changes that equation.

That's why SAI360 is leading the charge to modernize compliance, embedding AI directly into a unified GRC platform that already spans more than 20 integrated modules across ethics, compliance, and risk. This foundation gives AI what it needs most: rich, connected, and contextualized data.

From whistleblowing and horizon scanning to training and analytics, SAI360 is making compliance systems smarter, faster, and more intuitive. This is empowering compliance professionals to do more with fewer resources - unlocking real-time insight, stronger oversight, and a more resilient culture of ethics and accountability.

Ready to Strengthen Your Responsible AI Journey?

Building trustworthy, compliant AI isn't just a strategic advantage—it's a necessity. SAI360 empowers organizations with the frameworks, tools, and governance capabilities needed to confidently manage AI risk, ensure regulatory compliance, and embed responsible AI practices across the enterprise.

Take the next step toward transparent, secure, and accountable AI.

Book a Demo with SAI360

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform that spans the entire risk and compliance spectrum.

- Whistleblower and Case Management
- Ethics & Compliance Training
- Policy Management
- Conflicts of Interest
- Incident Management
- Regulatory Compliance
- Regulatory Obligations
- Horizon Scanning
- Enterprise & Operational Risk Management
- Third-Party Risk
- Internal Audit
- Internal Controls
- IT Risk
- Business Continuity
- Vendor Risk Management

SAI360
RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating ethics, governance, risk, and compliance within a single platform, SAI360 helps companies broaden their risk horizon so they can manage risk from every angle.
Visit sai360.com to learn more.

228450 1225