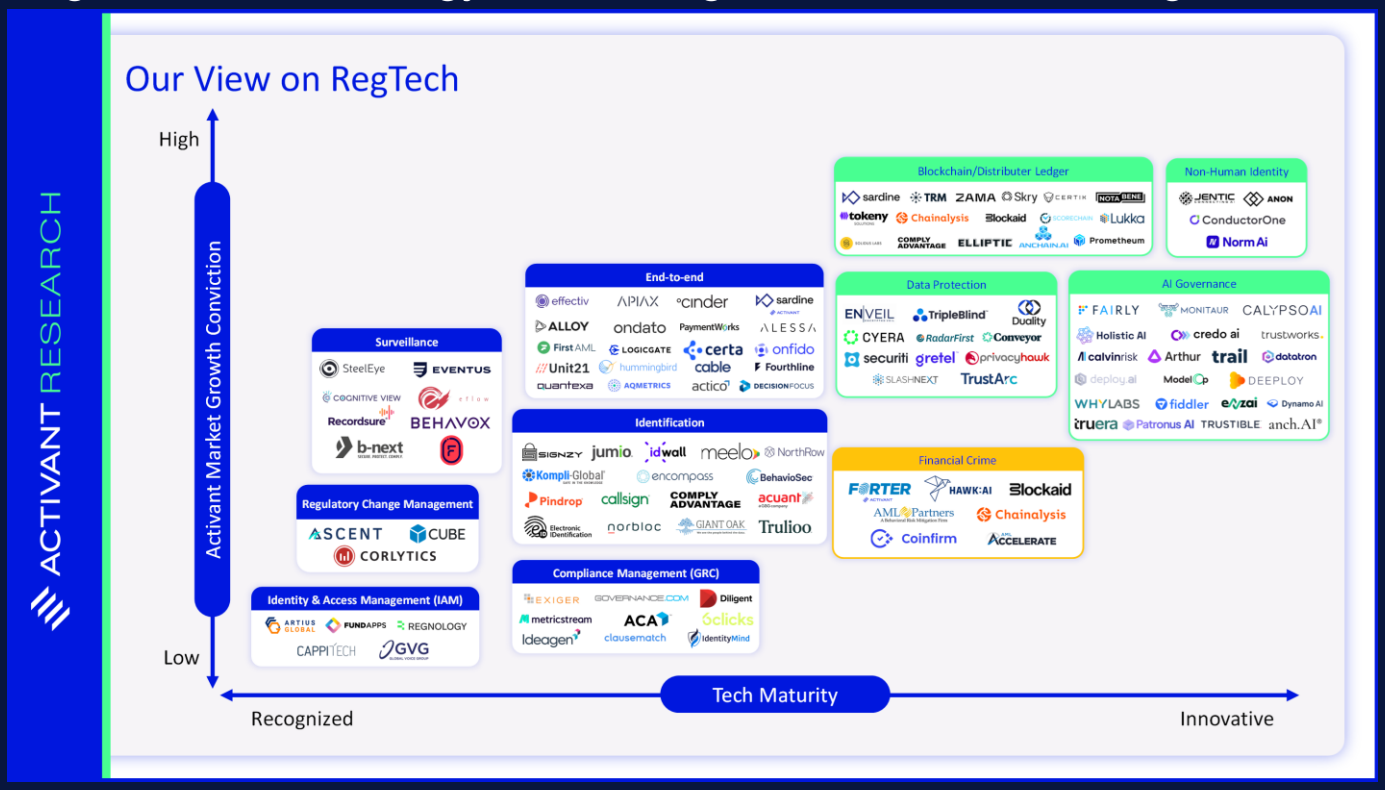
ACTIVANT RESEARCH

Deregulated, Not Unregulated

Regulation Technology In The Age Of Constant Change



Scott Watson, Tim Vetter

The rise of Donald Trump, Brexit, and the global movement toward right-wing populism have ushered in a new era of deregulation, or at least, that's the prevailing narrative. The reality is more nuanced: deregulation doesn't mean no regulation; it means different regulation. And that shift presents a once-in-a-generation opportunity for Regulatory Technology (RegTech).

RegTech has been one of the fastest-growing segments of fintech, originally propelled by the post-2008 crackdown on financial misconduct. Since 2020, the combination of heightened regulatory scrutiny, pandemic-induced disruptions, and the digitization of financial services has further accelerated adoption. Today, financial institutions are spending over $200 million annually on compliance, but non-compliance costs even more, evidenced by multi-billion-dollar fines for anti-money laundering (AML) lapses, data breaches, and ESG violations.[1]

Why Compliance Still Wins in This Deregulation Age

But here's the twist: the new wave of right-leaning governments isn't dismantling regulation, it's redefining it. Anti-globalist sentiment is leading to fragmented compliance standards. Nationalist policies are increasing trade barriers and data localization laws. ESG regulations, once a hallmark of progressive politics, are now being weaponized in unexpected ways. The world isn't moving toward a regulatory free-for-all; it's becoming a patchwork of conflicting rules that financial institutions and corporations must navigate in real-time.

This is why RegTech isn't just resilient, it's mission critical. Unlike the broader fintech sector, which saw volatility in investment cycles, RegTech was the only fintech subsector to increase funding in 2022, jumping to $18.6 billion from $11.8 billion in 2021.[2] Compliance isn't optional and, as regulations shift, the demand for technology-driven solutions is only growing. The next frontier? RegTech is evolving to address new challenges and opportunities emerging from AI advancements and shifting monetary policies. With the global adoption of blockchain transforming B2B transactions, international payments, and distributed ledgers (on-chain recordkeeping), alongside the widespread implementation of AI across enterprises, new sectors in regulation have emerged. AI agents, non-human identities, and ethical AI considerations have opened a metaphorical Pandora's box, necessitating new RegTech solutions. From AML and KYC/KYB to ESG compliance and data security, these technologies demand not only the conventional regulatory frameworks but also enhanced oversight to navigate the complexities of this new digital landscape.

As we move through 2025 and beyond, regulators themselves are arming up with AI, increasing enforcement capabilities, and leveraging technology to detect non-compliance faster than ever. This article explores the RegTech landscape at a high level, highlighting key startups as well as the emerging opportunities that lie at the intersection of regulation, politics, and technology.

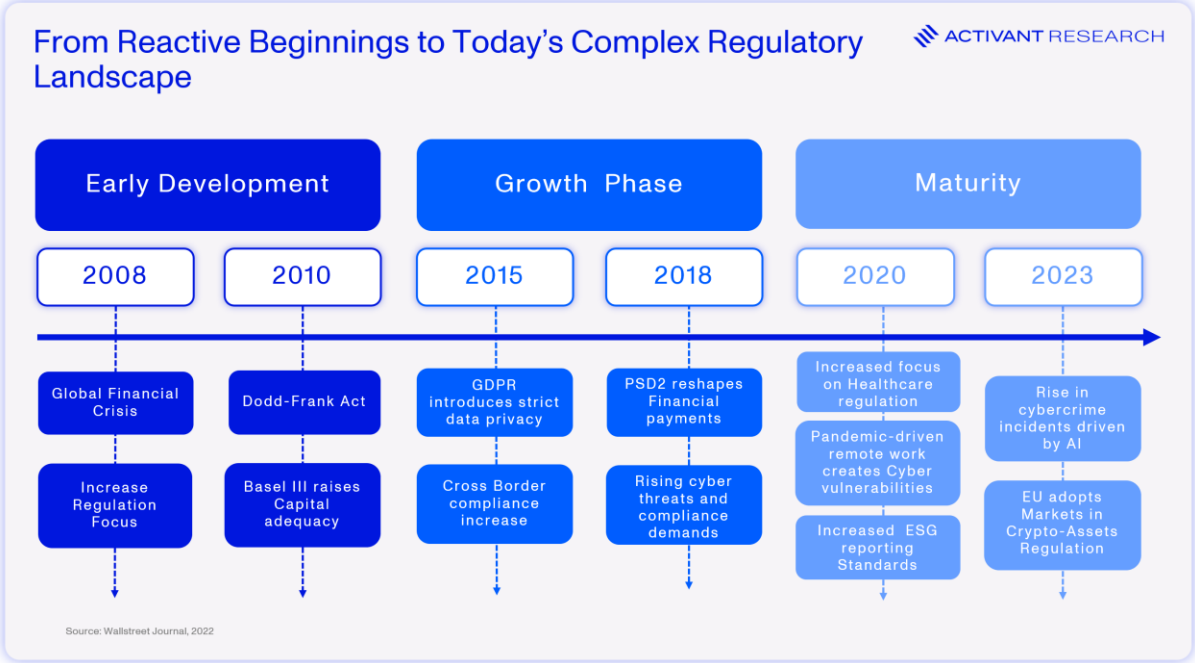
---

[1] Global Finance Magazine, Nasdaq's $10 Billion RegTech Deal Shows Urgency, Cost Of Compliance,2023

[2] KPMG, Global regtech investment at US$18.6 billion, 2022

Looking Back to Understand the Future

RegTech started as damage control. The 2008 financial crisis forced regulators to tighten the reins with Dodd-Frank and Basel III, aiming to curb reckless risk-taking and prevent another meltdown. Dodd-Frank overhauled financial regulation in the U.S., imposing strict reporting and transparency requirements. Basel III raised capital reserves and stress-testing standards to reinforce global banking stability.



From 2015–2018, the EU's General Data Protection Regulation (GDPR) set a new global standard for data privacy, introducing strict rules on user consent, data protection, and hefty fines for noncompliance. Simultaneously, Payment Services Directive 2 (PSD2) reshaped financial services in the EU by requiring banks to open their payment infrastructure to third-party providers, accelerating the rise of fintech innovation while adding new layers of security and regulatory oversight. Cross-border regulations further complicated compliance, making it clear that traditional methods were no longer enough.

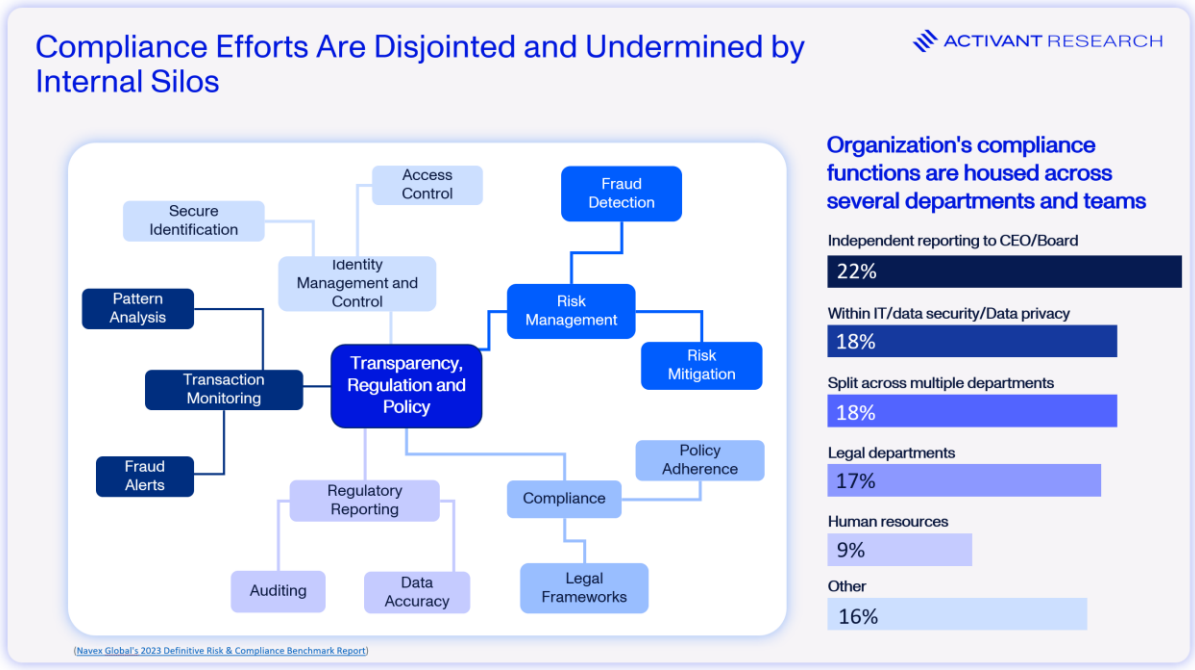
2025: The Status Quo has Failed

Compliance frameworks that have been built on manual processes, fragmented systems, and reactive checks are no longer viable in today's complex regulatory landscape. The inefficiencies and vulnerabilities in these outdated systems have been apparent for years, but they have now become too pervasive to overlook or simply absorb as a cost of doing business.

A company's compliance failures aren't just minor operational setbacks, but represent existential risks that can erode value, destroy investor confidence, and ultimately sink the entire business. Cases like **Credit Suisse**, **Wirecard**, and **FTX** serve as stark warnings. Credit Suisse's repeated regulatory breaches and risk mismanagement led to a liquidity crisis and a forced takeover. Wirecard's $2 billion fraud exposed deep flaws in financial oversight, while FTX's

collapse revealed systemic governance failures and a lack of internal controls. These weren't isolated incidents, but rather the direct consequences of compliance negligence, proving that weak regulatory frameworks can be fatal.

The past several years has exposed how **antiquated compliance tools and siloed organizational structures are leading to costly failures** in large organizations.



The current model, as shown in the figure above, is chaotic. Companies are struggling to manage the complexities within their own organizations while also grappling with increasing demands for transparency, regulation, and governance. It's like driving a car at night without headlights—blindly hurtling toward inevitable disaster.

Traditional vs Modern Compliance

Let's dig a little deeper as to why are these failures happening. **Traditional compliance models**, involving manual audits, Excel trackers, isolated teams, and after-the-fact reporting, simply cannot cope with the speed and complexity of today's rules. By contrast, **modern RegTech-driven approaches** leverage automation, data integration, and advanced analytics to manage risk in real time. Key differences include:

1. **Reactive and Manual vs. Proactive and Automated:** Legacy compliance tends to be *reactive*, addressing issues only after audits or incidents, and heavily manual. Teams slog through paperwork and siloed databases, which is **unsustainable in an era of big data**. Modern approaches flip this script. Tools use real-time data monitoring, AI, and machine learning to spot issues before they escalate. Instead of endless back-looking checklists, companies get continuous surveillance and alerts. For example, banks

adopting AI-driven monitoring have cut false-positive alerts by 40–60% while improving actual risk detection by up to 75%.[3]

2. **Siloed Systems vs. Integrated Platforms**: Traditional compliance often operates in departmental silos as seen in the figure above. Legal, finance, IT, and business units each keep separate records, making it impossible to get a unified view of compliance risk. Citibank's experience showed how a "siloed organization" prevented scale and consistency, with different groups solving the same compliance problems in conflicting ways.[4] Modern compliance platforms break down these silos by centralizing data and workflows. With unified dashboards and data integration, organizations can catch cross-departmental risks and ensure everyone is working off the same playbook. The result is not only better risk coverage but significant efficiency gains. By contrast, siloed companies see productivity drop up to 20% and costs rise ~15% due to duplicated effort[5] that could be avoided through integration.
3. **High Costs & Blind Spots vs. Efficiency & Transparency:** Keeping up with compliance via legacy methods is expensive and prone to human error. Firms often maintain large teams to handle mountains of paperwork and still risk mistakes or omissions. Studies have found that when issues slip through, the **cost of non-compliance (fines, remediation, business disruption)** averages **2.7 times** the cost of upfront compliance investment.[6] In other words, skimping on compliance is a false economy. On the other hand, investing in RegTech can sharply reduce ongoing costs. Automated solutions streamline labor-intensive tasks – one global bank reported compliance cost savings of ~30% after deploying advanced analytics to replace manual reviews.[7] Moreover, modern systems produce **audit-ready trails and real-time reports**, enhancing transparency with regulators and avoiding the opaque "black box" risk that comes with ad-hoc legacy processes. In fact, companies using RegTech for regulatory reporting have seen a 50% improvement in reporting accuracy and 35% fewer error-related penalties.[8]

Market-Wide Impact: Compliance Challenges Across Industries

It's not just banks and tech firms – virtually every industry is grappling with rising compliance complexity, from **finance to healthcare to manufacturing.** Regulatory demands have increased in volume and scope, creating a minefield for organizations.

[3] Sutherland, RegTech Rising: Shaping the Future of Regulatory Compliance,2025

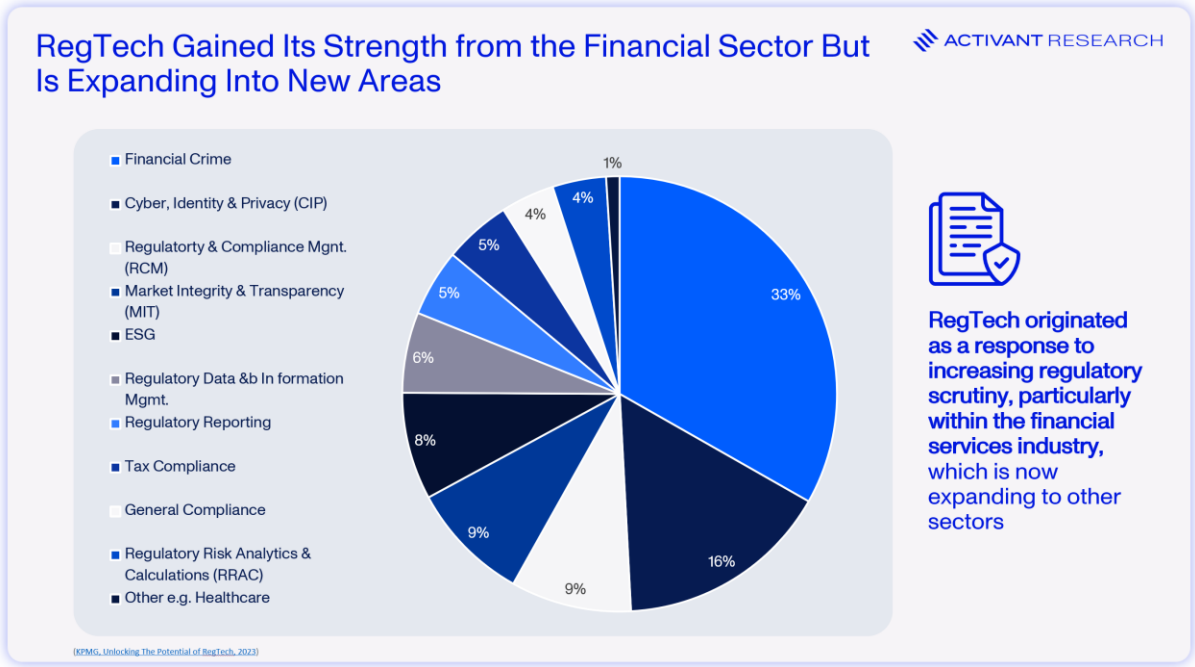
[4] Ovaledge, Citigroup's data governance disaster: A legacy of fragmented systems and heavy penalties, 2024

[5] Corcentric, Company silos create a shortfall for CFO's, 2023

[6] Comply, The True Cost of Non-Compliance, 2019

[7] Sutherland, RegTech Rising: Shaping the Future of Regulatory Compliance,2025

[8] Sutherland, RegTech Rising: Shaping the Future of Regulatory Compliance,2025



- **Financial Services:** Banks, insurers, and asset managers face ever-tougher regulations (AML, sanctions, consumer protection) and the *cost of failure is skyrocketing*. Global financial institutions paid over **$47 billion in fines from 2020 till July 2024** for compliance breaches ranging from money laundering to market manipulation.[9] Compliance is now a board-level issue in finance because the downside risk (both financial and reputational) has become existential.
- **Technology and Telecom:** The tech sector's growth outpaced regulation for years, but that era is over. Today, data privacy, cybersecurity (which we have written extensively on), and content moderation rules are being enforced with unprecedented rigor. Nearly 75% of the world's population will have its personal data protected by a modern privacy law (GDPR, CCPA) by end of 2024.[10] This patchwork of global rules means even a lean tech startup must navigate complex compliance obligations in every market. Major penalties like those against Amazon ($812m GDPR) and Meta (1.2bn euro GDPR) show regulators are willing to levy fines in the *billions* for data missteps. For tech companies, an outdated model (for example, manually managing user consent or data transfers) simply cannot scale – it invites regulatory intervention that can derail growth.
- **Healthcare & Life Sciences:** Hospitals, health insurers, and pharmaceutical firms contend with strict regulations (HIPAA patient privacy, FDA quality standards) and non-compliance can literally be life-threatening. Yet many providers still rely on legacy record systems and error-prone manual audits. The result has been frequent data breaches and violations. A single data breach now costs globally an average of **$4.9 million** in 2024[11] when you factor in fines, remediation, and lost business. In recent

[9] Ffnews, The Price of Non-Compliance: Corlytics Report Reveals $47.05bn in Regulatory Fines Since 2020, 2024

[10] Colligo, The True cost of Non-Compliance, 2024

[11] IBM, Cost of a Data Breach Report, 2024

years, regulators have issued multimillion-dollar HIPAA fines to healthcare groups that failed to modernize their information governance.

- **Manufacturing, Energy & Others:** Traditional industries are not off the hook either. They face evolving compliance standards in areas like worker safety, environmental protection, and supply chain ethics, to name but a few. Manufacturing and construction firms, for example, have been hit with hefty Occupational Safety and Health Administration (OSHA) penalties after fatal accidents revealed compliance lapses in safety training and protocols. Environmental regulations are tightening as well, exposing companies with outdated compliance tracking (e.g. manual environmental impact reporting) to surprise violations. From mines and oil refineries to food processors, we see a common pattern: the ensuing legal and financial fallout hits hard, prompting a scramble to invest in better compliance systems after the fact.

Across sectors, the message is clear, **regulatory compliance has become a market-wide challenge**, and current approaches are increasingly a liability. Businesses run higher risks of something falling through the cracks.

The High Cost of the Status Quo

Legacy compliance models aren't just risky, they are expensive. **"Cheap" compliance approaches end up costing far more in the long run**. In 2023, penalties for non-compliance cost financial institutions an extra $14 billion over and above their baseline $270 billion compliance costs[12]. Every major compliance failure comes with a litany of "hidden" costs: legal fees, management distraction, reputation damage, lost sales, and higher cost of capital. With the FCA's crackdown continuing and fines jumping 230% in 2024 to reach £176 million [13] even the biggest players with vast legal resources are struggling to navigate today's regulatory landscape. As evidenced by several recent cases below, noncompliance is a costly misstep.

- Binance, the world's largest crypto exchange, admitted to anti-money laundering and sanctions violations, resulting in a $4 billion settlement and criminal charges against its CEO.[14]
- Facebook (Meta) was hit with a €1.2 billion GDPR fine, the largest ever under EU data privacy laws, for transferring user data to the U.S. under outdated contractual clauses.[15]
- Goldman Sachs paid a $4 million SEC penalty for misleading ESG fund practices.[16]
- Barclays was fined £40 million by the UK's FCA for failing to disclose financial arrangements dating back to the 2008 crisis.[17]

[12] Boston Consulting Group, The Rising Cost of Compliance, 2023

[13] FCA, 2024 Fines, 2024

[14] U.S. Department of Justice, Binance and CEO Plead Guilty to Federal Charges in $4B Resolution, 2023

[15] European Data Protection Board, 1.2 billion euro fine for Facebook as a result of EDPB binding decision, 2023

[16] The Business Times, Goldman Sachs to pay US$4m SEC penalty in ESG fund case, 2022

[17] Financial Conduct Authority, FCA fines Barclays £40 million, 2024

- The U.K. FCA introduced new rules on the marketing of financial promotions for crypto products in 2023. Within the first 24 hours of those regulations going live, the FCA issued 146 alerts to firms for poor practice.[18]
- Money laundering is a persistent challenge, with the United Nations Office on Drugs & Crime estimating that between $800 billion and $2 trillion is laundered annually globally (2%–5% of global GDP).[19]

The Battle is Set to Intensify as Key Agencies Employ AI

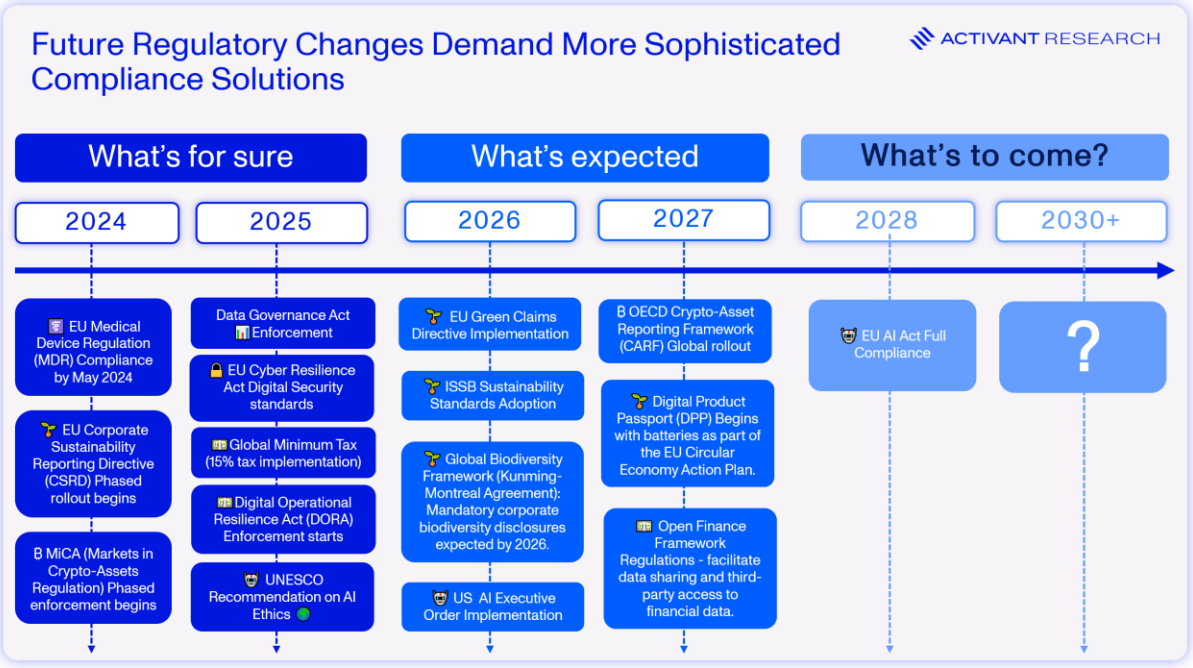
While companies are adopting RegTech solutions, regulatory authorities on both sides of the Atlantic are racing ahead, leveraging AI tools to enforce compliance with greater precision and speed. In Europe, agencies like the FCA are utilizing platforms like Quantexa and SymphonyAI for market abuse detection and AML compliance. The European Securities and Markets Authority (ESMA) employs AI-powered tools such as Palantir, Darktrace, and SAS for risk analytics and trade surveillance, while the European Central Bank (ECB) relies on solutions like BearingPoint and Regnology for compliance reporting and AML measures. The European Medicines Agency (EMA) and the European Environment Agency (EEA) have also embraced AI platforms, focusing on pharmacovigilance, drug approvals, climate monitoring, and regulatory reporting. Meanwhile, data protection authorities (DPAs) utilize tools like OneTrust and TrustArc for GDPR compliance and data privacy audits.

U.S. agencies like the Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA) use AI for fraud detection and market surveillance. Regulators now have unprecedented tools at their disposal to detect and penalize non-compliance. For organizations struggling with integration, data challenges, and transparency issues, the pressure to catch up has never been greater. Companies must not only overcome internal adoption barriers but also advance their compliance capabilities to avoid falling behind in a regulatory environment where authorities are armed with cutting-edge AI technology. The gap between regulators' capabilities and companies' readiness to comply is growing—and failing to close it could have serious consequences.

[18] Financial Conduct Authority, FCA issues 146 alerts in first 24 hours of new crypto marketing regime, 2023

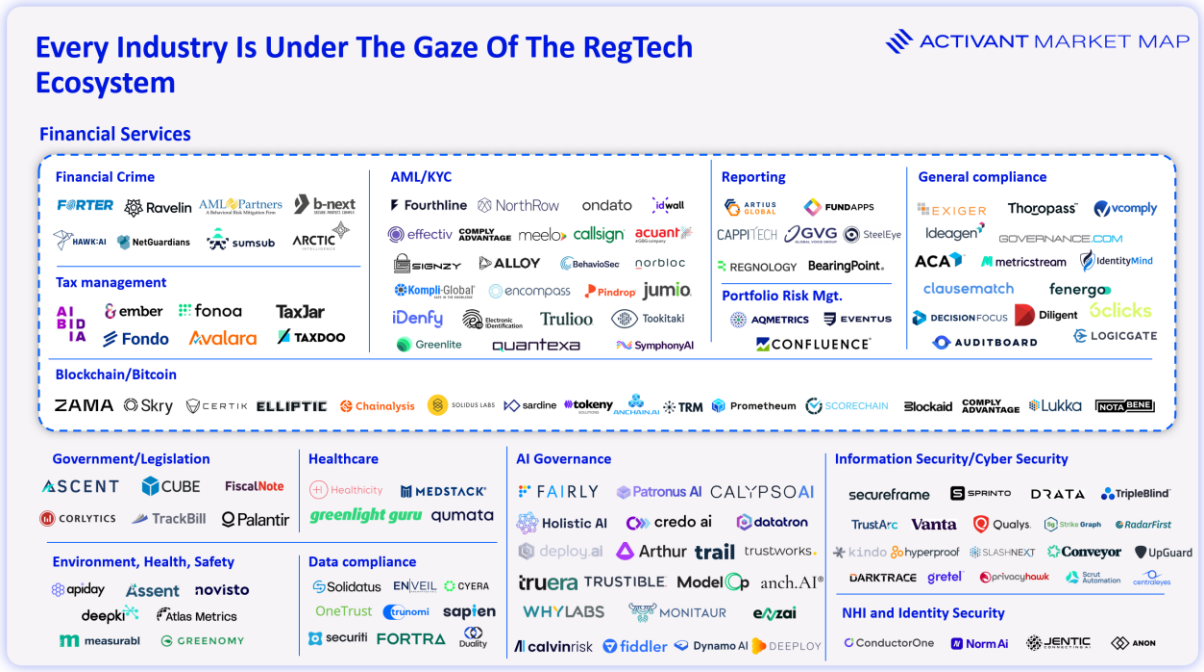
[19] United Nations, Improving regional investigations on money laundering and asset recovery , 2024

Regulation Overload



The landscape will evolve over the coming years, with meaningful milestones driving the need for more sophisticated compliance solutions. In 2024, organizations already faced key changes including compliance with the EU Medical Device Regulation (MDR), the phased rollout of the EU Corporate Sustainability Reporting Directive (CSRD) and Markets in Crypto-Assets Regulation (MiCA). By 2025, enforcement of the Data Governance Act, EU Cyber Resilience Act, and Digital Operational Resilience Act (DORA) will further tighten compliance demands, alongside global initiatives like the implementation of a 15% global minimum tax. Moving into 2026 and 2027, the focus will expand to sustainability and digital innovation with regulations like the EU Green Claims Directive, ISSB Sustainability Standards, and the Digital Product Passport as part of the Circular Economy Action Plan. Looking ahead, the EU AI Act is expected to achieve full compliance by 2028, signaling a broader push toward AI governance. These impending regulations underscore the growing complexity of compliance, requiring RegTech solutions that can adapt to dynamic global requirements and enable businesses to stay ahead of the curve.

RegTech Market Overview and Growth



The global RegTech industry is projected to grow from $15.8 billion in 2024 to $83 billion by 2033, at a CAGR of 22.8%[20,21]. While our market map is not exhaustive, at Activant we specifically see upside in financial crime prevention ($20bn market, 13% CAGR)[22], AI governance ($300m market, 40% CAGR)[23] and Cyber Security ($200bn+ market, 13% CAGR)[24] – particularly within the realm of Non-Human Identity (NHI). For further insight into the Cyber Security market, see Activant's latest research on Securing Non-Human Identity. While definitions and parameters may vary slightly across reports, we view this as a conservative estimate – especially as RegTech expands into new industries and use cases. The momentum is clear, positioning RegTech to become the foundation of modern compliance infrastructure.

Emerging Trends, Sectors and Opportunities

Influenced by both technology advancements and the shifting regulatory priorities of governments, several emerging trends and sectors are shaping the next chapter of RegTech innovation.

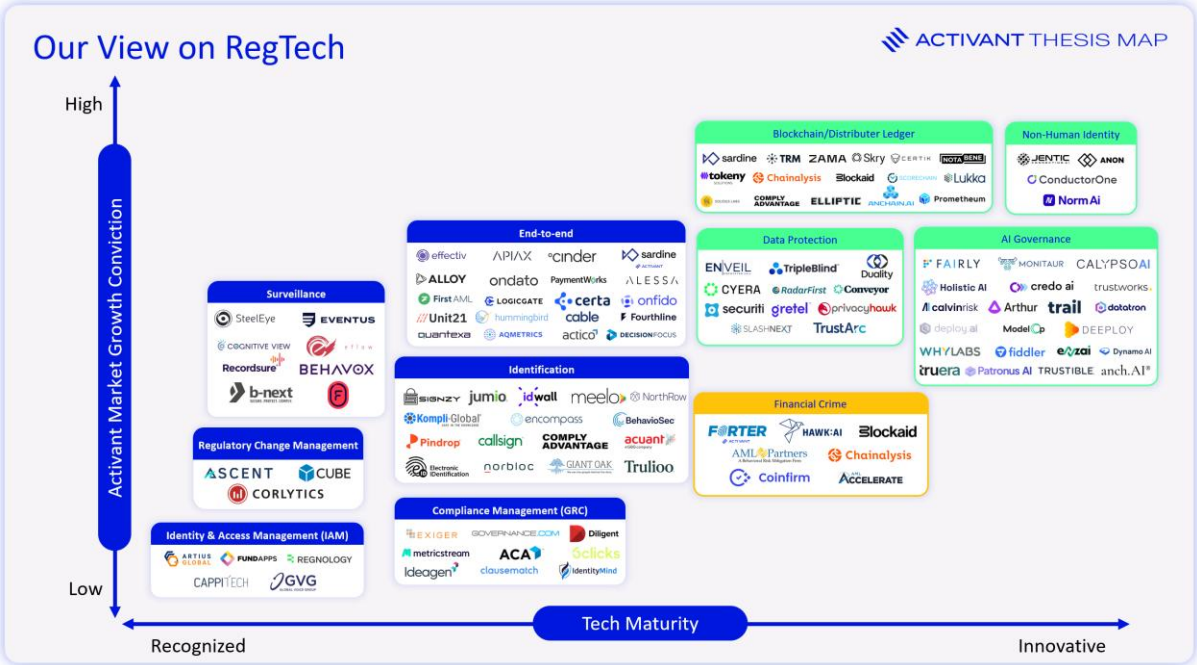
[20] Fortune Business Insights, RegTech Market Size, 2025

[21] Allied Market Research, RegTech Market Research 2033, 2024

[22] Research and Markets, Financial Crime and Fraud Management Solutions Market Report, 2024

[23] Grand View Research, AI Governance Market Size, Share & Trends Report 2030, 2024

[24] Grand View Research, Cyber Security Market Size to Reach $500.70Bn By 2030, 2025



AI regulating AI: The Era of "Guardian Agents"

In the past two years, governments have introduced new rules for trustworthy AI, ranging from the EU's upcoming AI Act to U.S. initiatives like President Biden's 2023 Executive Order on AI and various state-level regulations. This evolving landscape has created opportunities for RegTech startups that help enterprises comply with AI regulations and manage AI risks. Startups like Credo AI, Kindo or Fiddler, which measure, monitor, and manage AI risks while ensuring adherence to emerging regulations, and Calvin Risk, which offers real-time AI risk management insights, provide tools for AI governance. These startups are focusing on inventorying AI models, documenting datasets and biases, monitoring performance, and ensuring human oversight.

> We are past the AI hype cycle and organizations now find themselves at a critical inflection point where they are expected to capitalize on AI systems, but don't feel equipped to address mounting fears about safety and a growing laundry list of emerging rules for them to comply with. Governance is the key that unlocks the full potential of generative AI"
>
> **Navrina Singh**
> Founder & CEO, Credo AI

Regulations Shaping this Trend

The **EU AI Act** (expected to take effect by 2025–26) is a major driver that will impose strict obligations on "high-risk" AI systems (like HR screening, credit scoring, and medical AI) including risk assessments, audit logs, transparency to users, and conformity assessments. Companies like Deeploy, which provides a platform to easily onboard, monitor, document, and explain AI models, are at the forefront of addressing these requirements and ensuring

compliance. **Companies are facing fines up to 7% of global turnover** for non-compliance, so proactive solutions are in high demand. In the U.S., while comprehensive AI legislation is still pending, regulators are signaling expectations through guidance and enforcement. For instance, the FTC has warned against biased AI outcomes under existing consumer protection laws, and states like Colorado and New York have passed their own AI laws. All this creates a **"growing laundry list of emerging rules"** that companies must follow.

> Upcoming regulations like the EU AI Act, requires prioritizing responsible use of AI. This includes measures to create effective human oversight by creating transparency in decision making using explainable AI. Without such measures, we are at risk of losing control in aligning automated decisions with our goals and values. Simply put, it's the responsibility of the makers and users of AI systems that those systems are safe, and act as they are intended. Implementing safe and responsible AI will become a license to operate."
>
> **Tim Kleinloog**
> Co-Founder & CTO, Deeploy

We spoke to multiple European companies to understand how they are responding to the uncertainty introduced by the EU AI Act, and the feedback couldn't have been more fragmented: Some firms, especially smaller or fast-moving tech companies are taking a pragmatic, "do-now-fix-later" approach, meaning they're aware of the upcoming rules but aren't making meaningful changes until they're forced to. In sharp contrast, others are experiencing the complete opposite. One senior technology leader at a major European bank revealed that the Act has led to a *complete halt* of their procurement pipeline for LLM-based solutions:

> Our compliance department is not yet up to speed to get ready for this conversation because our compliance department doesn't know what the requirements are. We are in a paradoxical situation where [...] we couldn't have a conversation with the vendor because we wouldn't know what to ask them to comply with."
>
> **Anonymous**
> Expert Network

The impact of the EU AI Act seems to be a function of both **industry risk profiles** (e.g., banking) and **size,** where it's ultimately going to be the enterprises who must catch up on adoption, all while still being compliant.

Startups that can interpret these rules and embed them into software (checklists, dashboards, audit trails) provide immense value. Over the last two years, venture funding in this niche has grown as enterprises realize AI compliance is not just a legal burden but also key to maintaining

customer trust. A KPMG study found 75% of consumers are concerned about AI risks,[25], demonstrating that **responsible AI** is becoming a competitive advantage.

Future Developments

Going forward, we can expect end-to-end **AI compliance platforms** such as Holistic AI to become as common as privacy compliance tools. As AI systems proliferate across business functions, these platforms will integrate directly into ML pipelines, automatically logging how an AI model was trained, testing it for bias, and flagging any usage that violates new rules similar to explainability, fairness, stability and bias detection of Arthur AI or TruEra (acquired by snowflake). Future regulations will expand to cover AI **ethics** (e.g. requiring impact assessments for algorithms) or **security** (ensuring AI is robust against cyber-attacks). Startups are already speculating about features like "nutrition labels" for AI (summarizing an algorithm's data sources, accuracy, bias metrics) and real-time monitoring agents that halt an AI system if it starts behaving unpredictably. From a VC perspective, the **"responsible AI" market is in its early innings** and we will likely see consolidation as these compliance tools get acquired by larger governance, risk, and compliance (GRC) platforms or cloud providers.

Blockchain and Distributed Ledger Applications

Blockchain's tamper-proof, transparent ledgers are driving RegTech innovation in compliance. RegTech firms have used blockchain to streamline KYC, transaction reporting, and more. Sharing customer due diligence data between banks is traditionally complex but becomes simpler with a blockchain-based KYC network that securely shares verified credentials, reducing redundancy and detecting fraud. As an immutable compliance log, blockchain boosts data integrity and regulator confidence. It's especially promising in trade finance, where paper trails are cumbersome. The UK recently introduced a bill to digitize all trade documents on a blockchain, aiming to become the first major economy to go fully paperless. Such developments underscore blockchain's potential for regulatory transparency and security.

Blockchain and Crypto: In the Cross Hairs of Regulators

Europe's 2023 MiCA regulation established a unified crypto framework across EU member states, setting rules on consumer protection, stablecoin reserves, market integrity, and AML obligations. Exchanges and wallet providers must obtain licenses and implement EU AML checks, driving demand for compliance tools like automated blockchain monitoring. Startups such as Scorechain now offer "MiCA-ready" risk scoring and dashboards.

Globally, the Financial Action Task Force (FATF) Travel Rule requires identifying data to accompany crypto transactions, pushing firms to adopt tech that verifies identity on blockchain transfers. Companies like Notabene are focusing specifically on this rule, positioning themselves as the Swift of blockchain transactions. In the U.S., there's no MiCA equivalent, but regulators are tightening oversight under existing laws. The SEC has deemed many tokens to be potential unregistered securities, forcing exchanges to ramp up compliance or delist risky

[25] Business Wire, KPGM, 2024

assets. The SEC and Commodity Futures Trading Commission (CFTC) have also cracked down on unregistered exchanges and illicit token sales, while the Treasury's Office of Foreign Assets Control (OFAC) penalizes crypto companies for sanctions violations. This "regulation by enforcement" has made compliance tech vital for crypto businesses. Even in the 2022 market downturn, startups like TRM Labs saw increased demand as firms raced to bolster compliance.

Trust isn't just a feature of payment systems—it's the foundation. As we transition from correspondent banking to stablecoins, and from human-initiated to agentic payments, we're not eliminating the need for trust, we're transforming how it's established. The future of finance isn't just about moving value faster or cheaper, it's about transacting with confidence across any rail, any asset, and any medium."

Pelle Braendgaard
Co-Founder & CEO, Notabene

Speculative but Probable Future Impact

In the coming years, **blockchain-driven compliance solutions** will expand beyond cryptocurrency into mainstream finance and other industries one just needs to look at Anchain.ai already adopted by the US government and several banks. One can envision national regulators embracing distributed ledgers for certain reporting. For example, a regulator might require that all trade reports or mortgage documents be logged on a blockchain to guarantee **real-time oversight** and data integrity. We may also see a convergence of **digital identity and blockchain compliance**: projects that tie an individual's verified digital ID (potentially using self-sovereign identity standards) to transactions, making it easier to KYC-check parties in any digital exchange. In the crypto realm, once MiCA is fully in force and if the U.S. passes clearer laws, compliance will be non-negotiable. This will spur a wave of **consolidation or IPOs** where major fintech or cybersecurity companies acquire the likes of Chainalysis, Solidus Labs, ScoreChain or TRM Labs to incorporate their tools into broader compliance suites. There's also the question of **DeFi (decentralized finance)**, an area largely outside today's regulatory perimeter. As authorities figure out how to regulate decentralized protocols, RegTech will need new approaches such as the embedding of compliance checks into smart contracts themselves. Forward-looking startups are already working on this, developing, for example, tools to scan DeFi liquidity pools for illicit funds. Blockchain's use in compliance is part of the larger trend of "regulation going digital." it's plausible that every regulated entity will maintain some kind of **blockchain-based compliance ledger.**

Cryptocurrency crime may start with crypto, but it doesn't end there. Our team has expanded our Agentic AI capabilities beyond crypto to tackle broader financial risks. We are excited to partner with more financial institutions to fight financial crime and streamline compliance."
Victor Fang
Co-Founder & CEO, AnChain.AI

AI Agents, Non-Human Identities, and Regulatory Implications

A novel frontier in RegTech is emerging at the intersection of **AI agents** and digital identity. At Activant we conducted a deep dive in NHI management, identifying startups such as Anon and Jentic that focus on ensuring AI Agents are authenticated and authorized. The advent of autonomous AI agents and authentication raised a fundamental question: how do we handle "non-human" actors under regulatory frameworks built for humans and corporations? In the past two years, AI agents have gone from science fiction to practical pilots. For instance, 2023 saw popular experiments with GPT-4 based agents that can browse the web, execute code, or even make purchases online on behalf of users. Startups are now imagining personal AI assistants that might **open accounts, negotiate contracts, or transact** for you. However, our current compliance regimes assume a human (with verified identity) or a legally registered company is behind any action. New methods will soon be required for identity verification as financial products rely on verifying human identity and agents don't have a digital identity like a human.

In other words, if an AI agent tries to initiate a payment or sign a document, how do we verify and trust it? And if something goes wrong, who is liable – the user or the AI itself? These questions are driving both startups and regulators to explore **non-human identity frameworks** and adaptations to the rules.

Regulatory Adaptation to Digital Identities

Regulators are starting to address AI agents and non-human identities. The EU AI Act requires that users be informed when interacting with AI (e.g. chatbots), and AI-generated content (like deepfakes) be labelled. Similar regulations are emerging globally such as China's draft AI rules requiring watermarks and clear AI identification. Financial regulations are also adapting. If AI handles transactions, KYC/AML rules may apply, requiring verification of the ultimate beneficiary or controller. A brokerage using an autonomous trading algorithm, for instance, must record the responsible human or company.

Some regulators have explored "electronic personhood" for AI to clarify liability, an idea introduced in an EU Parliament report in 2017 and resurfacing in self-driving car debates. Currently, owners/operators are accountable for AI's actions, but future laws we expect will designate a legally responsible person for AI agents. Digital identity standards are evolving as well. The World Wide Web Consortium (W3C) and the Decentralized Identity Foundation (DIF) are exploring decentralized identity frameworks for IoT and AI, aiming to create a standardized credential system for non-human entities. This would allow AI operating in regulated industries (finance, healthcare, etc.) to be audited.

Fraud prevention and cybersecurity rules are also adapting. Financial institutions are deploying fraud detection systems that distinguish AI-led transactions from human ones. Under GDPR, individuals have the right to explanations for AI-driven decisions (e.g., loan denials), and algorithmic accountability laws – including those in the EU AI Act – already govern AI agent

activities. Overall, regulators are playing catch-up, but there's growing recognition that "AI agents with identity" must be integrated into the regulatory framework. New guidelines and identity management standards incorporating AI are emerging and will likely expand as AI evolves.

Future Considerations: The Intersection of AI, Web3 and Digital identities

AI agents could fundamentally reshape compliance and even the nature of **legal identity**. We might see the emergence of **AI compliance officers (AI guardians)**– AI agents that monitor other AI systems for compliance violations in real time. Imagine a bot that observes an algorithmic trading agent and flags if it breaches any risk limit or law, pausing it immediately. Regulators could mandate such "second layer" AI oversight for high-speed AI-driven activities. There's also likely to be a push for some form of **registration or licensing** of advanced AI agents. Just as companies must register algorithmic trading strategies with regulators in some markets, future high-powered AI (like an AI that can negotiate contracts autonomously) might require a registration number and periodic audits. This could give rise to a new service industry: firms that **audit and certify AI agents** for compliance. Another future consideration is **liability insurance for AI**. If an AI agent causes damage (financial or physical), insurance products and legal frameworks will need to handle that. This will loop back into regulation as governments decide whether to make such insurance mandatory for certain AI deployments (like car insurance for autonomous vehicles). From an industry perspective, if non-human agents become prevalent, **identity infrastructure will evolve dramatically** and concepts like global federated identity systems, digital passports for AI, or even blockchain-based AI reputations will become standard. It's speculative but not far-fetched that in a decade enterprises might have more "digital employees" (AI agents) than human ones. Each of those digital employees will need an identity, access controls, and compliance training (in a manner of speaking). This opens a new domain for RegTech to ensure **AI agents behave within legal and ethical bounds**. Ultimately, embracing AI agents will demand a mix of **technical innovation and regulatory foresight**.

An Industry That's Getting New Legs

Deregulation may make for catchy headlines, but beneath the political rhetoric lies a far more complex and fragmented regulatory ecosystem. As nationalist policies intersect with emerging technologies, AI, blockchain, and beyond, organizations face heightened scrutiny and higher stakes. RegTech has therefore become indispensable, evolving from a post-crisis stopgap into a driver of strategic advantage. The next chapter will see regulators employing AI while enterprises scramble to integrate automated compliance platforms and ensure they're prepared for tomorrow's digital realities. In this environment, success hinges on proactive, technology-driven frameworks that transform compliance from a reactive obligation into a core pillar of competitive resilience.