Parker & Lawrence
Research

REGTECH ANALYST

2026

The Global State of RegTech

Contents

Executive Summary

RegTech has evolved from fewer than 100 largely UK- and US-based point solutions in 2016 into a global, multi-billion-dollar industry of thousands of elite technologists.

The compliance function is beginning to evolve beyond its traditional remit.

Necessarily so, as rising regulatory pressure increased expectations while competition constrained budgets, forcing risk and compliance teams to innovate to survive.

Technological advancements are not only reshaping the solution landscape but redefining the role of risk and compliance itself. By virtue of their position, risk and compliance functions have a uniquely comprehensive view of the business, combining enterprise-wide visibility with deep, data-intensive oversight of processes and systems. The function is beginning to evolve beyond its traditional remit, with perceptions shifting from enforcer to strategic adviser, guiding the organisation on how decisions shape risk, which risks to take, and ultimately how to scale safely.

Vendors are not only leaning into this shift but, in many cases, driving it with solutions that extend beyond compliance into efficiency, intelligence, and growth. As the ecosystem matures and incorporates responsible AI, risk and compliance are increasingly positioned as catalysts for smarter, faster, and more confident growth.

95%

Of financial institutions (FIs) report scaled enterprise use in at least one regulatory domain.

Five Key Findings: Institutions

1. 95% of financial institutions (FIs) report scaled enterprise use in at least one regulatory domain. Financial Crime scores highest in our **RegTech Adoption Index**.
2. 62.7% of FIs plan to increase spending on RegTech in 2026, with 48.3% looking to implement new vendor solutions.
3. 53% of firms still rely on word of mouth for discovering new RegTech solutions, and only 37% conduct deliberate online research.
4. 44.3% of FIs expect AI agents to be among the most heavily invested in technologies within risk and compliance in 2026.
5. We estimate a conservative 2026 global RegTech TAM of $245.4bn for FIs with 50+ employees. **Read more**

$5bn

Was raised by RegTech vendors in 2025 across 216 deals.

Five Key Findings: Vendors

1. $5bn was raised by RegTech vendors in 2025 across 216 deals.
2. 28.3% of vendors expect institutions' technology spend to significantly increase in 2026 (20% or more).
3. 60% of vendors expect AI agents to see the greatest investment within financial institutions' risk and compliance environments in 2026.
4. Regulatory interpretation as machine-executable code is emerging as the next frontier of RegTech, underpinning the safe deployment of these AI agents.
5. 21.4% of vendors believe closer collaboration between industry and regulators is the most effective way to support RegTech adoption.

Approach

This research combines primary data from global surveys and interviews with detailed market modelling and domain analysis to provide a comprehensive view of the RegTech landscape in financial services.

Global surveys of **300** senior risk and compliance decision-makers from FIs and 100 RegTech vendors*.

Qualitative interviews with regulators, regulated institutions and other market experts.

Deep dives across six risk and compliance domains, covering challenges, maturity and emerging themes.

In-depth discussions with 10 leading RegTech vendors, including product demos, roadmaps, case studies and business plans.

Bottom-up market sizing using reported 2026 RegTech spend, population modelling, 2025 vendor funding data and a review of 63 published market estimates.

All data sources were verified, synthesised and interpreted by the RegTech Analyst and Parker & Lawrence Research teams.

*See appendix for survey demographics.

Market Overview

Ten years on since the FCA coined the term, RegTech is now a multi-billion dollar market at the centre of regulation, technology and growth.

54%

of senior risk and compliance professionals cite meeting regulatory compliance obligations as a key driver of RegTech adoption.

Global State of RegTech 2026 Institutions Survey

Risk and Regulation

Regulators worldwide have continued to impose substantial financial penalties for compliance failures.

$35bn+

global regulatory fines since 2023

Enforcement actions remain high despite deregulatory rhetoric intended to promote growth.

At the same time, internal complexity and external threats continue to rise.

- **$15** billion **laundered**
- **2,000** cyber **attacks**
- **300** regulatory **notices**

...every day in 2025.

28%

of senior risk and compliance professionals recognise RegTech as a key driver of growth and competitiveness.

Global State of RegTech 2026 Institutions Survey

Competition and Growth

The rise of FinTechs and challenger banks has strengthened RegTech's role as a competitive advantage and an opportunity to realise growth without compromise.

15% of operating costs

spent on risk and compliance*

The cost of compliance is a clear target for efficiencies.

The persistence of traditional risk management and compliance methods means that costs are still rising, not falling.

- **80%+** of compliance teams still rely on some amount of **manual** processes
- **$57.1bn** projected **legacy-system** spend by 2028, up from $36.7bn in 2022.
- **49%** of compliance professionals say that reducing cost is a key driver of RegTech adoption ( ).

*Based on PwC and TheCityUK estimates that UK financial services firms spend over £33.9bn annually on compliance, equivalent to more than 13% of operating costs; we scale this to ~15% to account for broader risk and compliance activities beyond the scope of their analysis.

Technological Maturity

Regulatory and cost pressures have coincided with key technological advances, offering firms a route to sustainable compliance.

A significant increase since 2021, when 38% reported adoption, at least "in part".

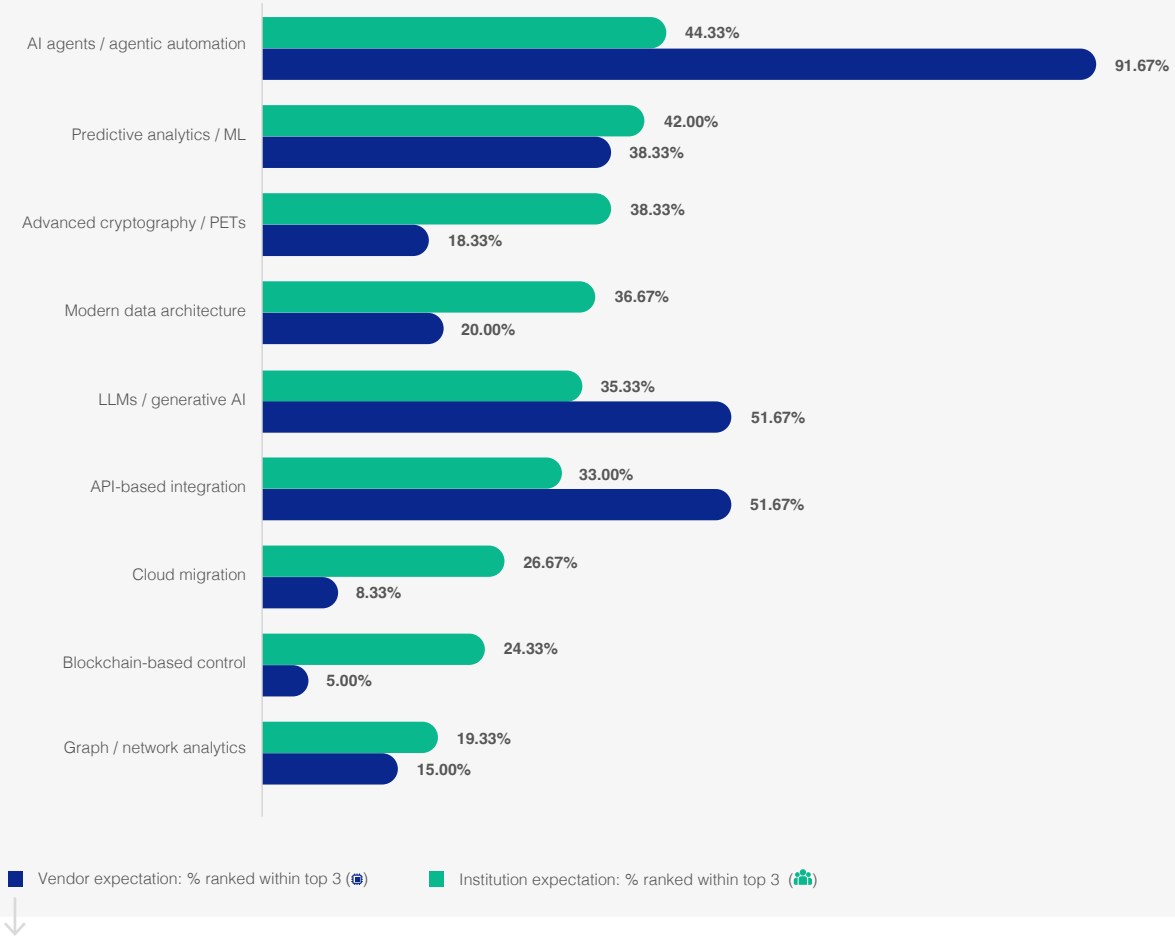
64% of firms

say RegTech is a core part of their control environment in at least one regulatory domain.

Technology Initiatives

RegTech adoption has been powered by maturing, long-term digital transformation projects, breakthroughs in artificial intelligence and a competitive vendor landscape.

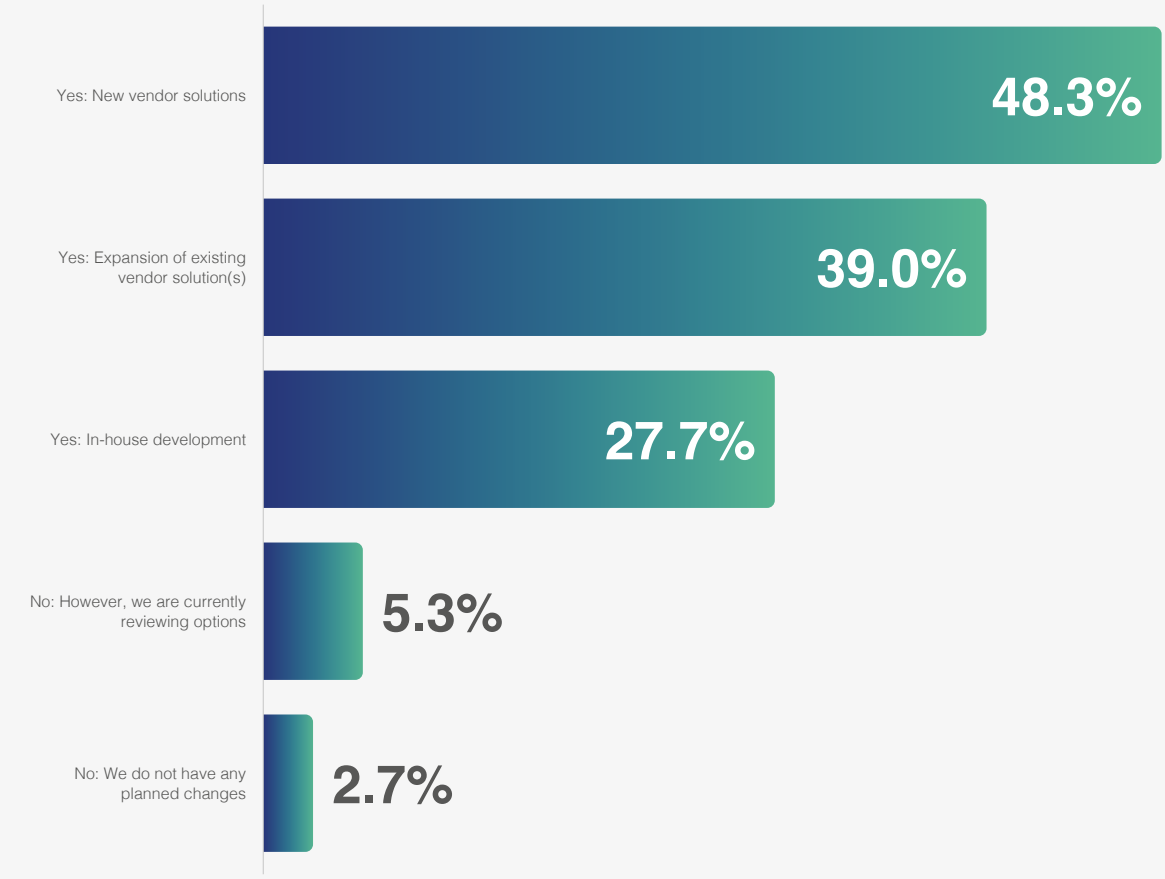
Which technology initiatives do you think will see the greatest investment within financial institutions' risk and compliance environments in 2026?



AI is also reshaping the build versus buy decision. AI lowers the cost of internal prototyping, but specialist vendors still hold an advantage in production-grade delivery, governance and ongoing support. Institutions with stronger engineering teams are nevertheless moving further with in-house development.

- AI projects, especially agents, sit at the top of 2026 technology agendas. More established AI techniques, such as predictive analytics using statistical machine learning, remain important and benefit from better explainability and applicability to large structured datasets.
- Vendors have more concentrated priorities, reflecting their role in following the greatest perceived market momentum. They also signal the longer-term technology vision that vendors are tasked with developing.
- AI momentum is also driving spend on modernising data architecture, which is a key barrier to technology adoption as a whole. This area may currently be underestimated by vendors.
- Beyond speculative assets, blockchain and cryptography continue to build practical momentum within FIs, which vendors may not have fully anticipated.

Do you expect to implement new or expanded RegTech solutions this year?



Not all of these responses were/are mutually exclusive, so the percentages shown correctly sum to more than 100%.

Vendor Momentum

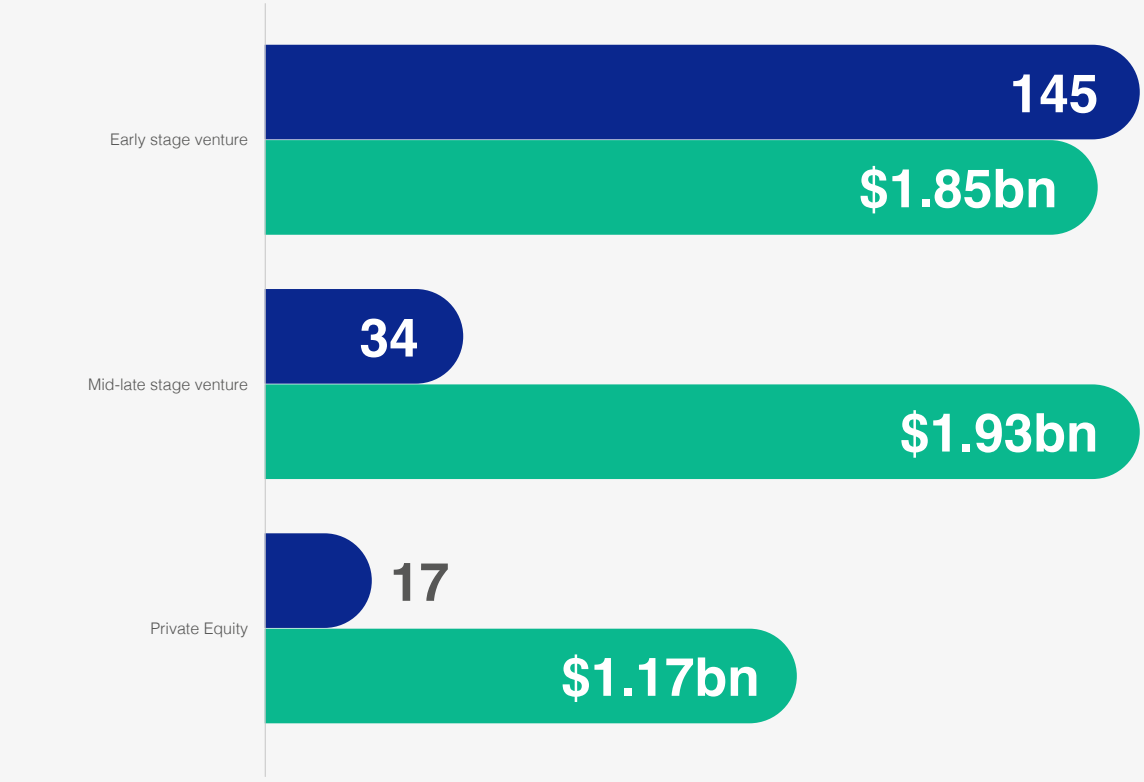
To see how this funding was distributed across the **RegTech taxonomy**, see **domain deep dives**.

$5bn

disclosed funding for RegTechs in 2025 across 216 deals

As the market surpassed 4,000 products from over 1,300 vendors.

2025 RegTech Funding Stages



This chart excludes some deals that do not fit the three relevant funding categories.

After a period defined by consolidation, the vendor landscape is fragmenting again:

- Consolidation at the top end is creating a very different market from the one being built by AI-first start-ups at the lower end.
- Platforms still matter, but lower-cost solutions are becoming more credible in the lower to mid-market.
- Within the divide, there are significant opportunities for collaboration. In this phase, partnerships can enable firms to rapidly enhance or extend their platforms, adding value and deepening customer relationships.

Caveats on AI

- While this research highlights strong momentum behind AI in risk and compliance, and survey respondents did not rank AI concerns highly as barriers to adoption, there is another side to the story.
- Some organisations remain cautious. This reflects both internal readiness constraints and lingering concerns around the technology itself, which we explore **later in the report**.*
- Leading vendors are therefore selective in their use of AI, applying the most appropriate techniques rather than defaulting to the latest architectures, and embedding risk management from the outset. Our survey suggests that vendors are, in many cases, more attuned to AI risks than institutions themselves.

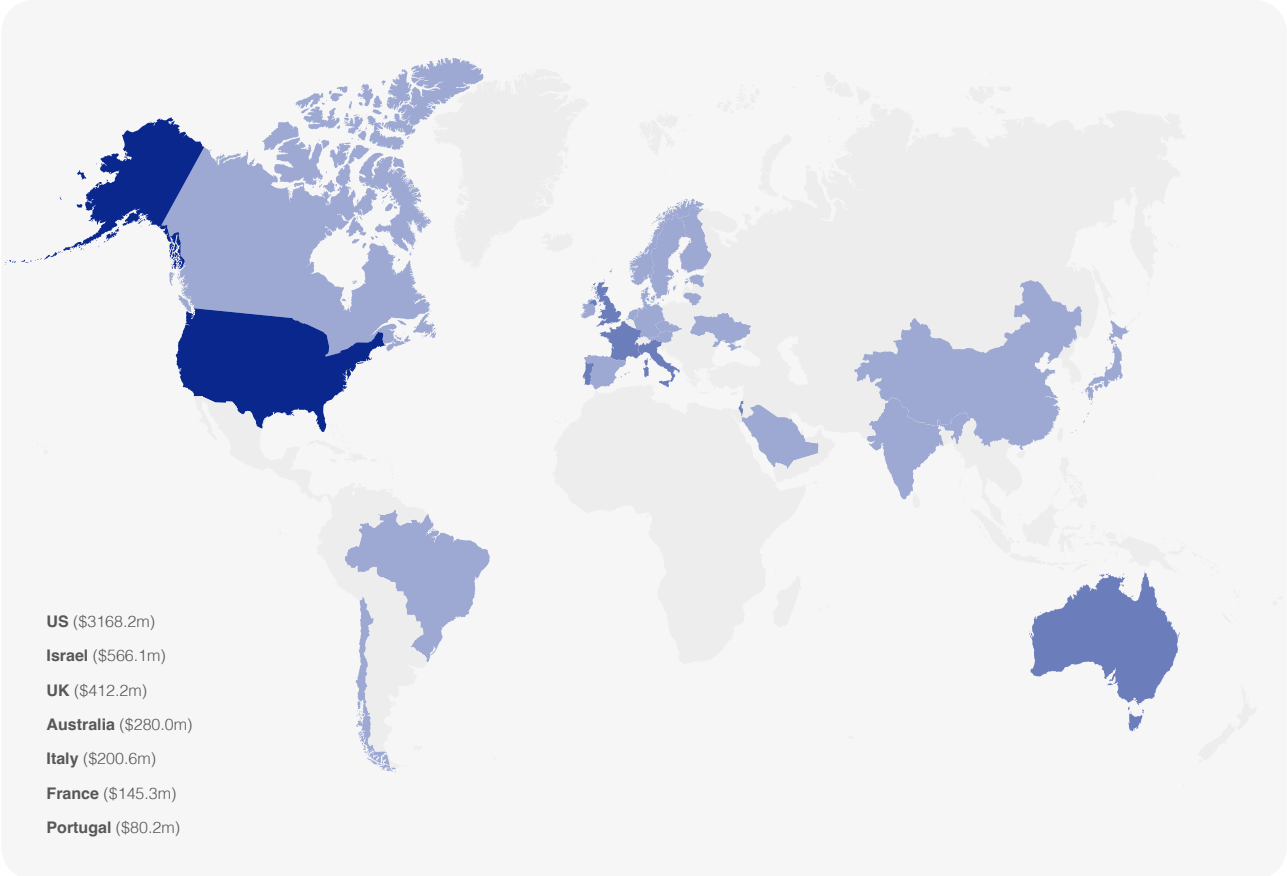
*For a deeper dive on institutions' struggles to achieve ROI with AI, read our previous report: **https://www.parkerlawrence.co.uk/research/generative-ai-in-risk-and-compliance-2025**

$3.17bn

raised by US-based RegTechs in 2025 alone.

Global Funding by HQ

- RegTech fundraising is now global, with disclosed raises across at least 28 countries in 2025 alone. The US remains the clear centre of activity.
- Capital is also coming from a broad mix of investors, including some of the largest and most successful firms globally.



Top Investors by Value

Investor	Rounds Participated	Disclosed Round Value USD	Primary Continent (No. Deals)	Primary Category
General Catalyst	4	$751,800,000	North America	Compliance Management
Evolution Equity Partners	3	$595,000,000	Asia	Information & Technology Security
Goldman Sachs Growth Equity	2	$585,000,000	North America	Compliance Management
Brookfield Growth	1	$435,000,000	North America	Information & Technology Security
CapitalG	1	$435,000,000	North America	Information & Technology Security
Sequoia Capital	4	$345,000,000	North America	Compliance Management
Spectrum Equity	2	$300,000,000	North America	Financial Crime
Mubadala	1	$300,000,000	North America	Compliance Management
Ballistic Ventures	7	$295,300,000	North America	Information & Technology Security
Georgian	3	$295,000,000	North America	Information & Technology Security

Top Investors by Volume

Investor	Rounds Participated	Disclosed Round Value USD	Primary Continent (No. Deals)	Primary Category
Y Combinator	8	$265,298,837	North America	Compliance Management
Ballistic Ventures	7	$295,300,000	North America	Information & Technology Security
Lightspeed Venture Partners	6	$184,000,000	North America	Information & Technology Security
Andreessen Horowitz	6	$182,500,000	North America	Information & Technology Security
Insight Partners	5	$252,224,811	Europe	Resilience
General Catalyst	4	$751,800,000	North America	Compliance Management
Sequoia Capital	4	$345,000,000	North America	Compliance Management
Accel	4	$247,224,811	Europe	Information & Technology Security
Silver Buckshot Ventures	4	$197,800,000	North America	Information & Technology Security
Evolution Equity Partners	3	$595,000,000	Asia	Information & Technology Security

Market Size

These developments have driven an explosion in the market size (total addressable market, TAM) of RegTech, which we estimate to be $245.4bn. This is a conservative estimate, covering FIs with 50+ employees only.

300 survey respondents alone reported $2.37bn of expected 2026 spend. Even before any population scaling, the bottom-up spend base is substantial.

Estimated global TAM (2026)

$245.4bn

Conservative estimate. Excludes firms with fewer than 50 employees.

Model range

$207.6bn to $284.7bn

Low and high cases from the clustered global model.

Six-country anchor markets

$125.5bn

Ground-up result across the six surveyed core markets.

Domain Breakdown

Traditional RegTech

Regulatory domains included in other broad market estimates

% Share

47.3%

Estimated TAM

$116.1bn

Domains

Financial Crime, Market Conduct, Compliance Management

Broader taxonomy

Additional domains within our broader RegTech definition

% Share

52.7%

Estimated TAM

$129.3bn

Domains

Information & Technology Security, Resilience, ESG

See the full **RegTech Taxonomy** used in this research.

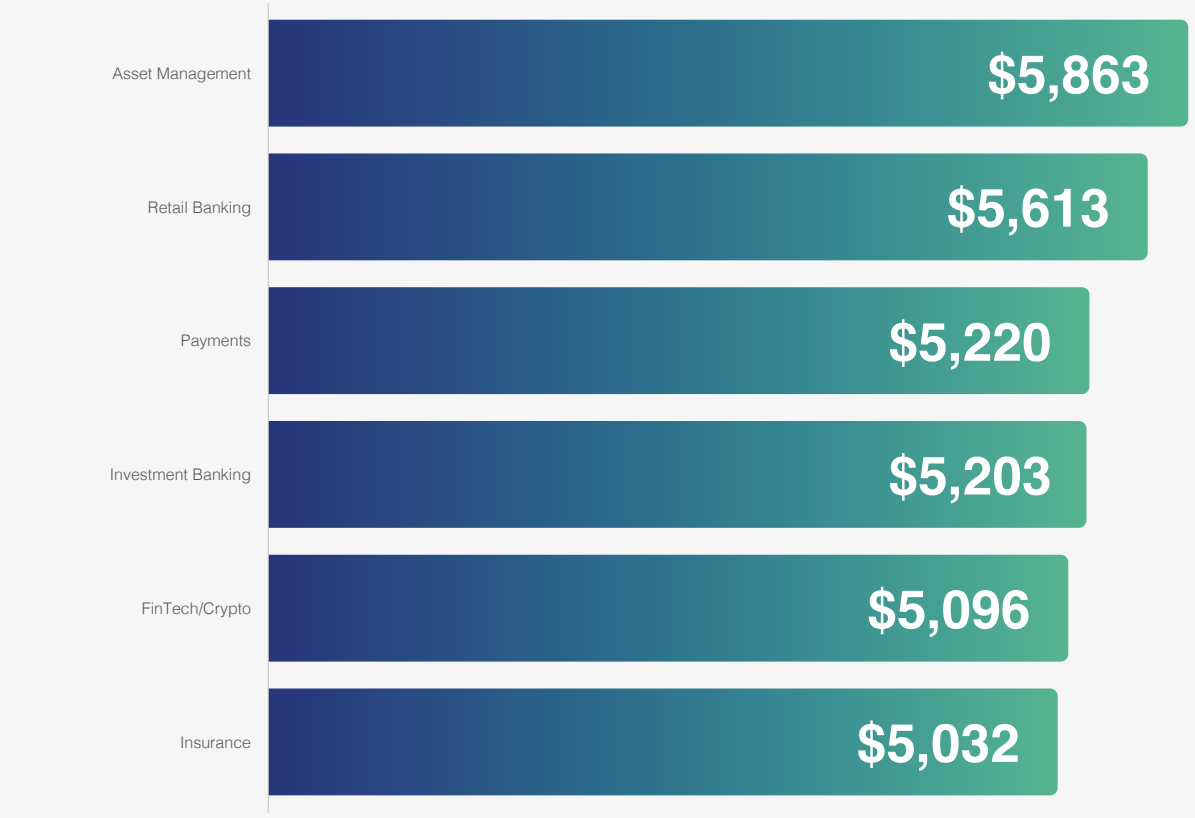
How This Estimate Differs From Other Benchmarks

- It measures risk and regulation technology spend, not just vendor revenue.
- It includes internally-built specialist systems as well as third-party solutions.
- It uses a broader RegTech definition across six domains, not just a few core compliance areas.
- It is built bottom-up from actual buyer spend, not primarily from top-down assumptions.

Method in Brief

- Bottom-up spend benchmarks from 300 senior decision-makers.
- Population modelling by country, sector and firm size.
- Global extension across 46 countries plus residual rest-of-world buckets.
- Category split estimated from survey adoption patterns and external market-sizing benchmarks.

Average RegTech spend per employee by subsector



62.7%

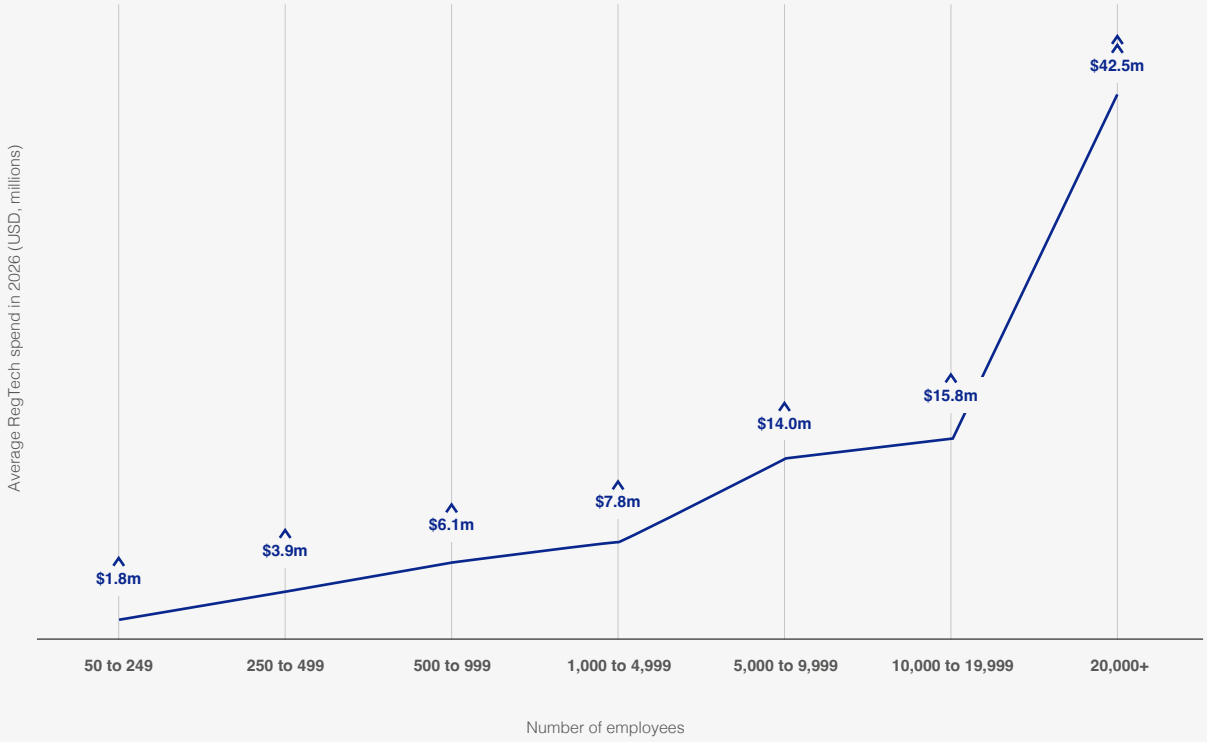
of FIs plan to increase RegTech spending in 2026 compared to 2025.

Market Size by Region

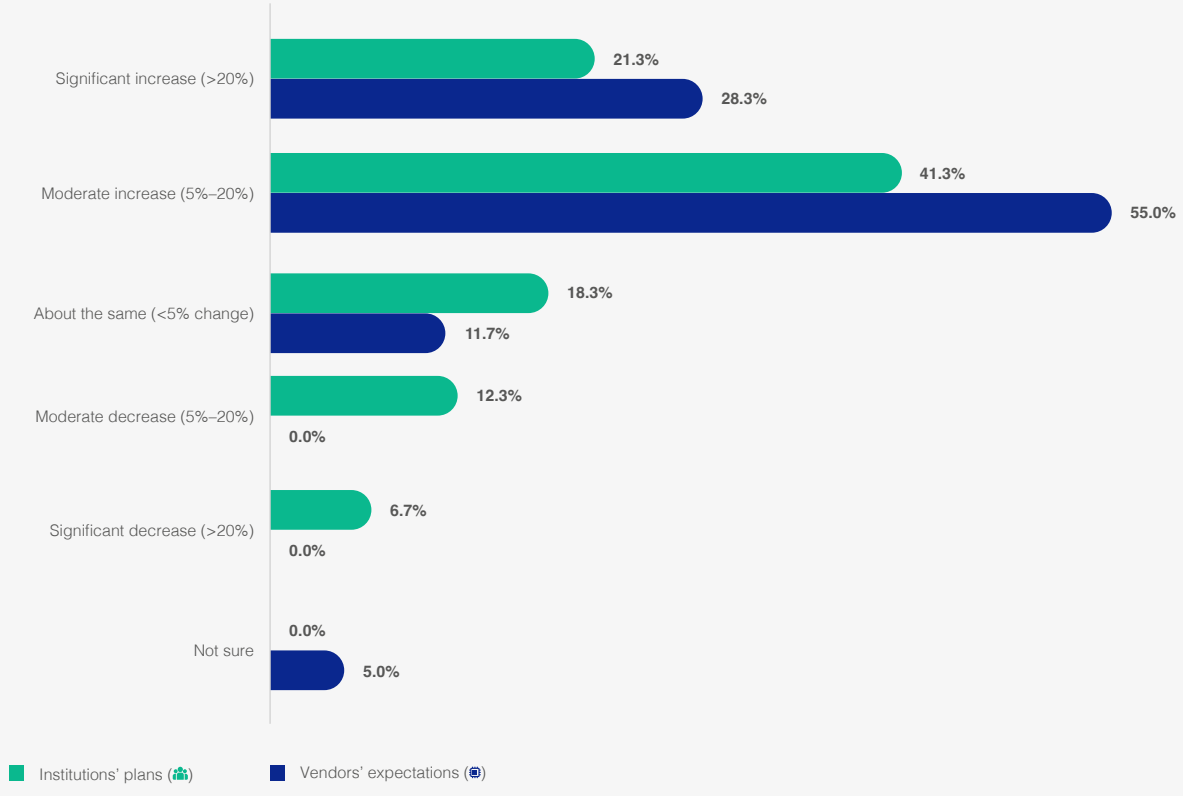
Region	2026 TAM	Share
Americas	$120.6bn	49.1%
APAC	$66.7bn	27.2%
Europe	$51.1bn	20.8%
MENA	$7.0bn	2.9%

- Scale is the clearest spending driver. Average reported spend rises from $1.8m at 50-249 employees to $42.5m at 20,000+.
- Asset Management is the largest sector in the model at $98.1bn, followed by Retail Banking at $46.9bn and Insurance at $39.9bn.
- Current spending is higher among firms with more mature deployments. Organisations with advanced RegTech adoption across four or more regulatory domains report an average spend of $9.8m, versus $6.8m among firms with two or fewer.
- Adoption maturity also supports forward growth. 69% of firms with advanced RegTech adoption across four or more regulatory domains expect spending to rise in 2026, versus 58% among firms with two or fewer.

Average 2026 RegTech spend by company size



How will financial institutions' RegTech spending change in 2026 compared to 2025?



The RegTech Adoption Index is calculated as the average score of reported adoption levels (scaled from 0 to 100) within each regulatory domain.

Market Structure

This research uses a simplified RegTech taxonomy consisting of 24 subcategories (RegTech use cases) from top-level 6 categories (risk and compliance domains).

Financial Crime

Solutions designed to detect, prevent, and respond to crimes impacting financial institutions, such as fraud, money laundering, sanctions evasion, and terrorist financing.

Subcategories:

- Sanctions Screening
- KYC / KYB
- Fraud Prevention & FRAML
- Transaction Monitoring

Leading adopters;

- Payments
- Investment Banking

RegTech Adoption Index **68**

Market Conduct

Solutions ensuring fair, transparent, and compliant trading and market activities, preventing market manipulation, misconduct, or breaches of market regulations.

Subcategories:

- Trade Surveillance
- eComms Surveillance
- Communication & Disclosures
- Trade Reporting

Leading adopters;

- FinTech
- Investment Banking

RegTech Adoption Index **54**

Compliance Management

Solutions addressing regulatory challenges across multiple domains or frameworks, enabling firms to proactively manage regulatory obligations, changes, and assurance activities at an enterprise-wide level.

Subcategories:

- Regulatory Change Management
- Regulatory Intelligence
- Compliance Assessment
- Compliance Orchestration

Leading adopters;

- Payments
- Retail Banking

RegTech Adoption Index **44**

Information & Technology Security

Solutions focused on identifying, assessing, and mitigating risks arising from cybersecurity threats, IT systems and data management practices.

Subcategories:

- Identity & Access Management
- Network & Endpoint Security
- Data Protection
- Data Privacy

Leading adopters;

- Payments
- Asset Management

RegTech Adoption Index **61**

Resilience

Solutions focused on ensuring the continuity of critical business services by enabling firms to prepare for, respond to, and recover from disruptions across operational and third-party environments, while addressing systemic, cross-cutting risk domains, such as AI.

Subcategories:

- Enterprise Risk Management
- Incident Response
- Third Party Risk
- AI Governance

Leading adopters;

- Retail Banking
- Investment Banking

RegTech Adoption Index **46**

ESG

Solutions facilitating the measurement, management, and reporting of environmental, social, and governance factors for sustainable investing and corporate responsibility.

Subcategories:

- ESG Ratings
- ESG Reporting & Disclosures
- ESG Risk Management
- Climate Risk Quantification

Leading adopters;

- FinTech
- Retail Banking

RegTech Adoption Index **40**

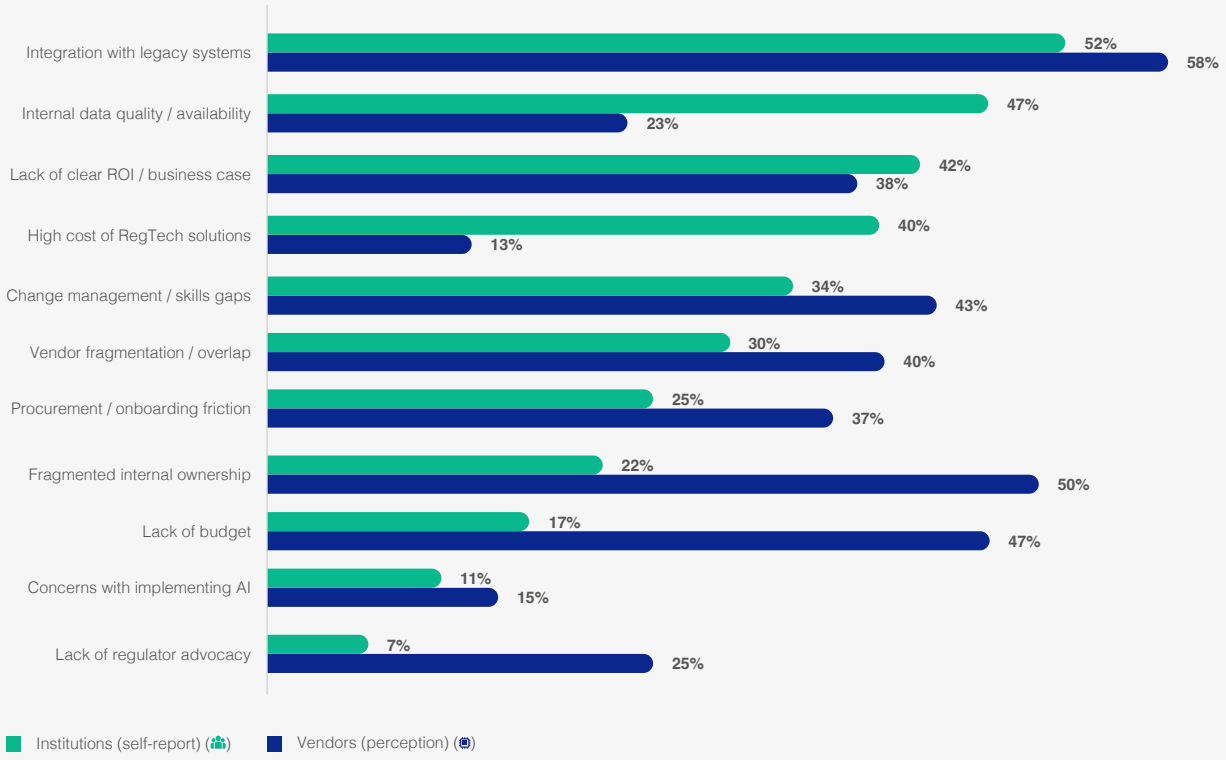
For a closer look at the trends within each subcategory, check out our **domain deep dives**.

52% of FIs say legacy systems create significant barriers to RegTech adoption.

Market Challenges

The RegTech market has grown despite its challenges, which are prominent but evolving.

What are financial institutions' most significant barriers to adopting third-party RegTech?



Commercial Alignment

- Less than half of FIs recognise the business case (42.3%) or cost (39.7%) of RegTech as a barrier to adoption, marking a meaningful improvement in understanding its value.
- Vendors are acutely aware of the need to align commercial incentives and have made significant progress in developing solutions that extend beyond compliance into operational efficiency and growth enablement.
- There is room to go further: an opportunity for risk and compliance to not just enable, but direct growth by becoming a strategic function. **See Market Opportunities**.

Technical Foundations

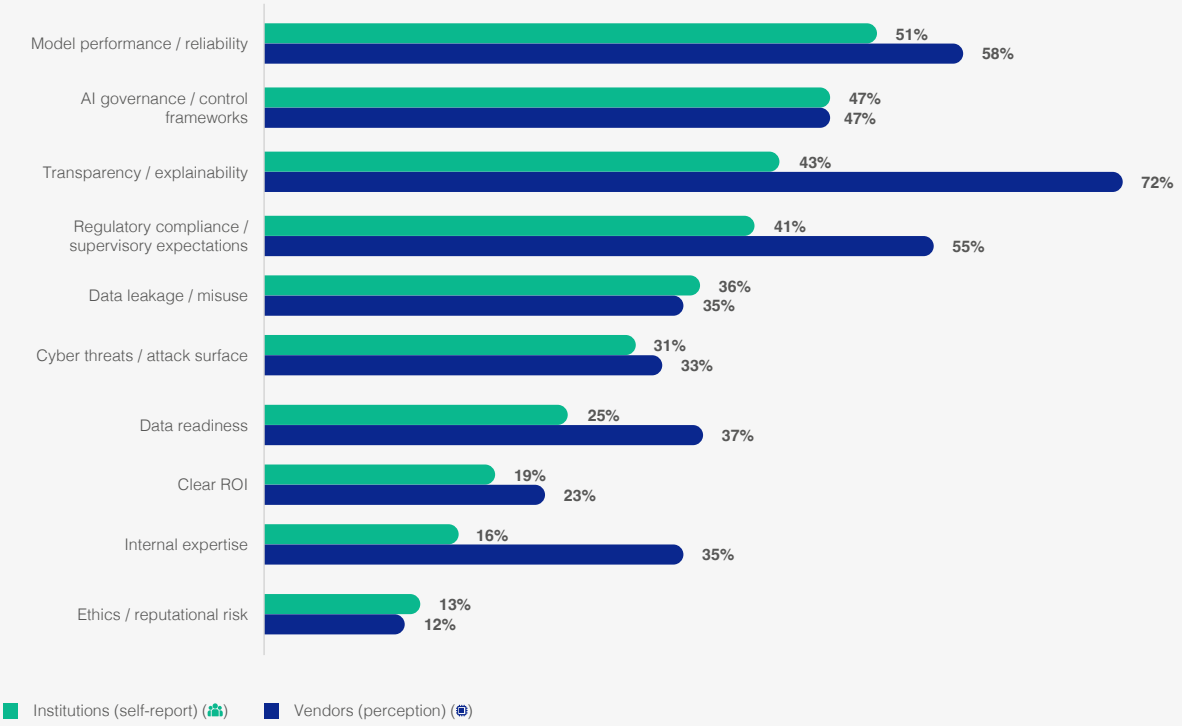
- FIs' lack of technical and data readiness remains the single biggest constraint on third-party RegTech adoption.
- The cost and difficulty of integrating modern platforms with legacy infrastructure is well known, and many vendors have become accustomed and skilled in deep, complex implementations.
- FIs at both ends of the size spectrum (especially large and especially small headcounts) are most likely to struggle with legacy systems, although likely for different reasons. FinTechs and insurers are the least affected subsectors.
- FinTechs are most likely (52%) to struggle with data quality and availability. This challenges the perception of technical sophistication, but is consistent with fast-growth firms whose risk and compliance systems have not fully kept pace with scale.

Concerns with Artificial Intelligence

Surprisingly few institutions cite AI itself as a major barrier to RegTech adoption (11%). This partly reflects the work that the market has done to build AI features securely, with human review and accountability in mind, as well as the industry's significant appetite for AI adoption. It may also reflect the fact that many firms are still focused on more basic data and technology issues.

Notably, not a single institution responded that they have "No significant concerns" with AI:

What are financial institutions' main concerns regarding the use of AI in risk and compliance?



This research has not found an AI capability gap. In fact, a surprising amount of AI capability is currently unused in vendors' products as institutions are not yet ready or able to adopt, often due to governance.

- Vendors overestimated FIs' current perception of AI risk. Although misalignment is ordinarily a cause for concern, this reflects vendors' understanding of AI risk, and the high bar that is required for technology in risk and compliance use cases.
- Despite improvements in AI, 51% of institutions regard model performance / reliability as a main concern. This calls into question exactly which models risk and compliance professionals are being granted access to in their work environment.
- AI presents new risks while also promising new ways of working. The technology is, itself, still early and evolving quickly. Creating and implementing robust governance and controls in this environment is a major challenge, and was cited by 47% of FIs. For a qualitative deep dive on AI Governance, **check out this report.**

Financial Institutions' AI Concerns by Region

(% respondents selecting each concern in each region)

	UK + Europe	North America	APAC	MENA
Model performance, accuracy and reliability (e.g. hallucinations)	49%	48%	58%	55%
Adequacy of AI governance and control frameworks	43%	50%	62%	30%
Lack of transparency and explainability	42%	40%	47%	48%
Regulatory compliance (e.g. EU AI Act) and supervisory expectations	36%	41%	47%	45%
Unintended data leakage or misuse	46%	29%	25%	48%
Exposure to cyber threats (e.g. increased attack surface, system compromise)	26%	32%	32%	40%
Lack of data readiness (quality, format, structure and architecture)	21%	29%	28%	23%
Demonstrating clear return on investment	15%	24%	18%	20%
Lack of internal expertise	16%	17%	13%	20%
Ethical considerations and reputational risk	14%	12%	17%	8%
Other	-	-	-	-
No significant concerns	-	-	-	-

Regulators are acknowledging the value of technology: Only 6.7% of FIs cite a lack of regulator advocacy among their main barriers to adoption.

Overcoming Challenges: A Look Back to 2021

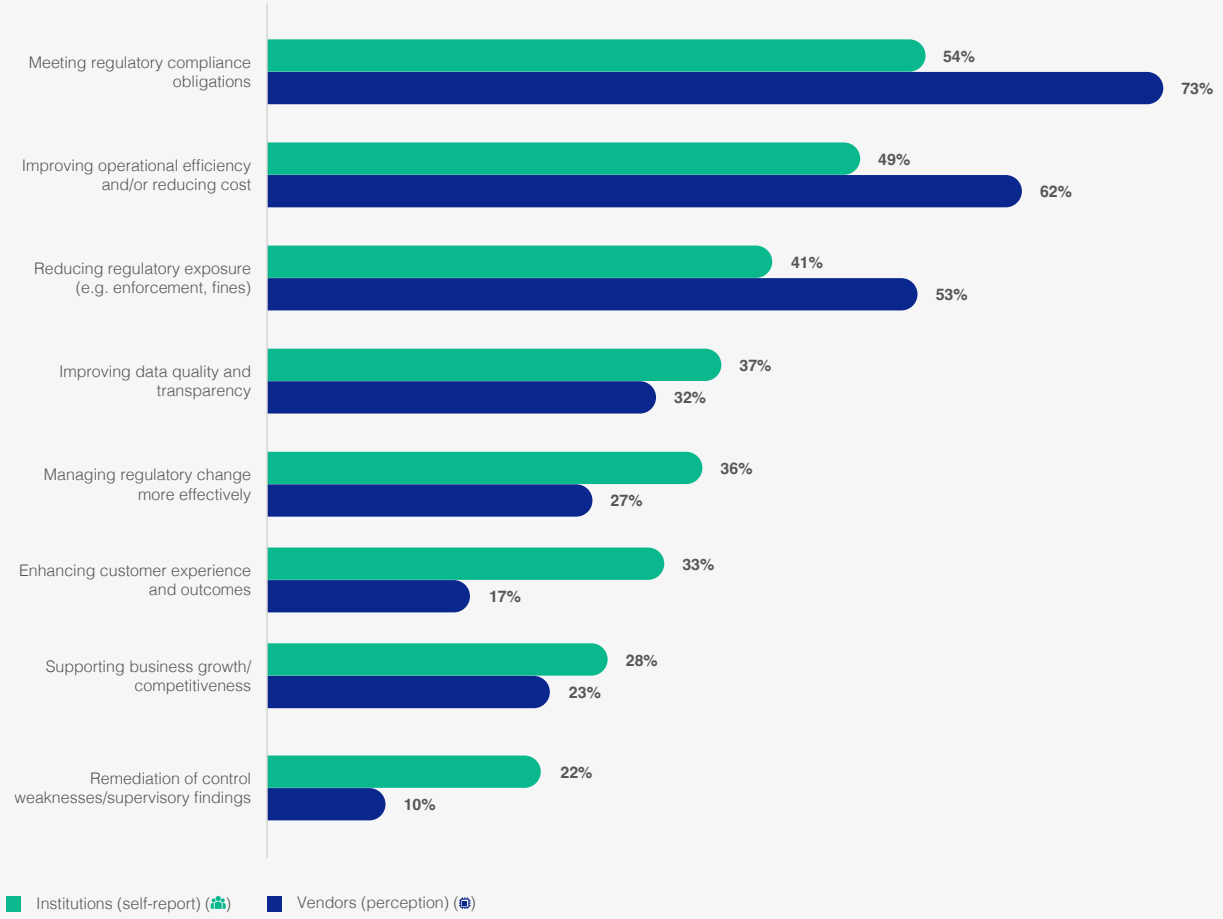
Today's challenges matter, but the market is materially more mature than it was five years ago. In 2021, The City of London and RegTech Associates documented **ten challenges** that the RegTech market faced:

Challenge	2021 Commentary	2026 Update
Awareness	"It is still unclear what RegTech is and how it helps firms. Financial services institutions (FSI) also feel vendors must do more to be aware and respond to their needs"	The industry is now very aware of what RegTech is: 100% of FIs have implemented RegTech to some extent, and 95% report scaled enterprise use in at least one regulatory domain.
Regulator Stance	"Desire to maintain 'tech neutrality' reduces visible regulator support for RegTech. Still not part of day-to-day supervisory discussions."	Regulators are acknowledging the value of technology: Only 6.7% of FIs cite a lack of regulator advocacy among their main barriers to adoption.
Scale	"FSIs discouraged by 'riskier' small vendors, natural preference for 'BigTech'. Naivety sees inexperienced firms propose unsuitable tools."	FIs are more likely to prioritise merit over reputation: Only 26% of institutions report reputation / perceived financial stability as a priority in vendor selection.
Vision	"There is a lack of an overall vision or strategy for the RegTech sector which filters down into tactical deployments at the individual firm level."	Not apparent in 2026. Vendors are taking the lead on exploring new technologies, collaborating directly with regulators and raising billions in capital as a result.
Representation	"Lack of a unified voice for RegTech prevents effective collaboration and lobbying on behalf of the sector."	Progress is uneven. The UK has strong initiatives through Innovate Finance and UK Finance, and the FCA is engaging directly. These dynamics are less prominent in the US, but the market is thriving regardless.
Technology	"Legacy IT is harder to connect to, magnifying challenges of integration and interoperability. Weakens case for digitally enabled regulation."	Still a major challenge: 51.7% of FIs cite integration with legacy systems as a major barrier to RegTech adoption. FIs are still modernising infrastructure, and 39% are prioritising RegTech solutions that are easiest to integrate.
Standards	"Myriad rules and data types create a complex solution landscape for buyers to navigate. Lack of standardisation holds back adoption."	Fragmentation remains: 30% of FIs cite vendor fragmentation as a major challenge to adoption. And 35% also said that regulatory standardisation across jurisdictions would support adoption.
Board Education	"RegTech adoption is stymied by a lack of board awareness. Limits engagement, saps confidence to invest and drives 'apathy'."	This year's research has repeatedly revealed interest and even pressure from the top to adopt RegTech. Only 17% of respondents noted a lack of budget as a barrier to RegTech adoption.
Talent	"Lack of access to IT workers with required skills (Tech + FS + Compliance). RegTech image needs a 'revamp' to help attract talent."	The skills gap remains a challenge: 34% of FIs report change management and skills as a barrier to adoption. This challenge may grow with **reports** of burnout and mental health challenges in compliance teams.
Finance	"Scale ups in the RegTech space share the challenge of accessing finance to grow. Lack of support for FSIs to invest in 'risky' projects."	$5bn funding in 2025 tells a different story.

33% of FIs adopt RegTech in order to improve customer experience and outcomes.

Market Opportunities

Which outcomes currently drive RegTech adoption in financial institutions?



49%

of FIs adopt RegTech in order to improve operational efficiency and/or reduce cost.

Vendors are broadly aligned with institutions on the drivers of RegTech adoption. The larger opportunity is to improve how solutions are discovered, evaluated and justified*.

- Regulatory compliance remains the primary use case. Broader value is increasingly recognised, but not always assumed.
- Commercial outcomes divide the market. Many institutions see efficiency gains, while others still perceive RegTech as an **added cost**.
- More than a quarter of respondents already treat RegTech as an enabler of growth and competitiveness. This research indicates that risk and compliance as a function may go further still.

*This chart separates "meeting compliance obligations" and "reducing regulatory exposure". While clearly highly correlated, they are separate outcomes: "Meeting regulatory compliance obligations" refers to fulfilling required controls, processes and reporting standards, whereas "reducing regulatory exposure" reflects the effectiveness of those controls in preventing breaches, enforcement actions or fines in practice.

Anonymously, one chief risk officer told us that a RegTech implementation had significantly reduced the workload of its compliance officers, but the business realised no bottom-line improvement. The benefits sat with the compliance team, who simply had more time outside of work. The firm had no vision for what the function should become once manual backlogs were removed. This is a bug, not a feature.

An Example: Scaling with AI

This dynamic is particularly visible in AI strategies. McKinsey estimates that **30–50%** of "innovation time" with generative AI is spent making solutions compliant or waiting for clarity from control functions.

Firms with mature risk and compliance frameworks can compress this time significantly. More importantly, they are better positioned to take the right risks, justify their decisions and implement targeted mitigations, enabling faster and more secure scaling. The role of risk and compliance is not only to remove friction, but to help define the path forward.

A Vision for Risk and Compliance

The perception of risk and compliance as a cost centre is self-reinforcing. Underinvestment leads to fragmented systems, manual processes and delayed decisions, which in turn reinforce the view that the function slows the business down.

Leading firms already recognise that RegTech supports business growth. These 28% of FIs are part of a growing minority. Earlier still is an even more ambitious vision that can redefine risk and compliance as a function.

Risk and compliance already touch every product, transaction and customer interaction, combining forward-looking mandates with deep, real-time data. With the right tooling, this can fundamentally change the function's role.

At its best, risk and compliance can:

- inform which risks are worth taking, not just which to avoid
- guide how those risks are taken, embedding controls into decision-making upfront
- influence broader strategy by providing clarity earlier in the process.

This is not about doing the same work faster. It is about introducing a risk-based perspective into strategy and execution, allowing firms to move with greater confidence and precision. But this will not emerge by accident.

Achieving this requires a shift in both perception and capability. Internally, firms must move beyond treating risk and compliance as a constraint. Externally, leading vendors are already building towards this vision, embedding intelligence, workflow and decision support into their products.

Vendors can support the transition by continuing to drive awareness and market education. Progress is evident, yet more than half of buyers still rely on peer recommendations when selecting solutions. With only 37% using deliberate online research, there remains a gap in objective, detailed market intelligence.

How do you typically discover new RegTech vendors or solutions?

(% respondents selecting each channel in each region)

	Total	UK + Europe	North America	APAC	MENA
Peer recommendations/word of mouth	53%	58%	54%	47%	48%
Industry conferences and in-person events	48%	47%	46%	47%	55%
Industry research reports/analyst coverage	43%	47%	39%	47%	38%
Deliberate online research (e.g. Google search)	37%	30%	36%	42%	50%
Professional networks (e.g. LinkedIn)	31%	33%	31%	27%	35%
Digital events (e.g. webinars, virtual summits)	27%	23%	29%	32%	28%
Direct outreach from vendors	17%	15%	21%	13%	18%
Regulator-led initiatives or sandboxes	11%	11%	11%	15%	5%
Other	-	-	-	-	-
Not applicable, no meaningful awareness of vendors	-	-	-	-	-

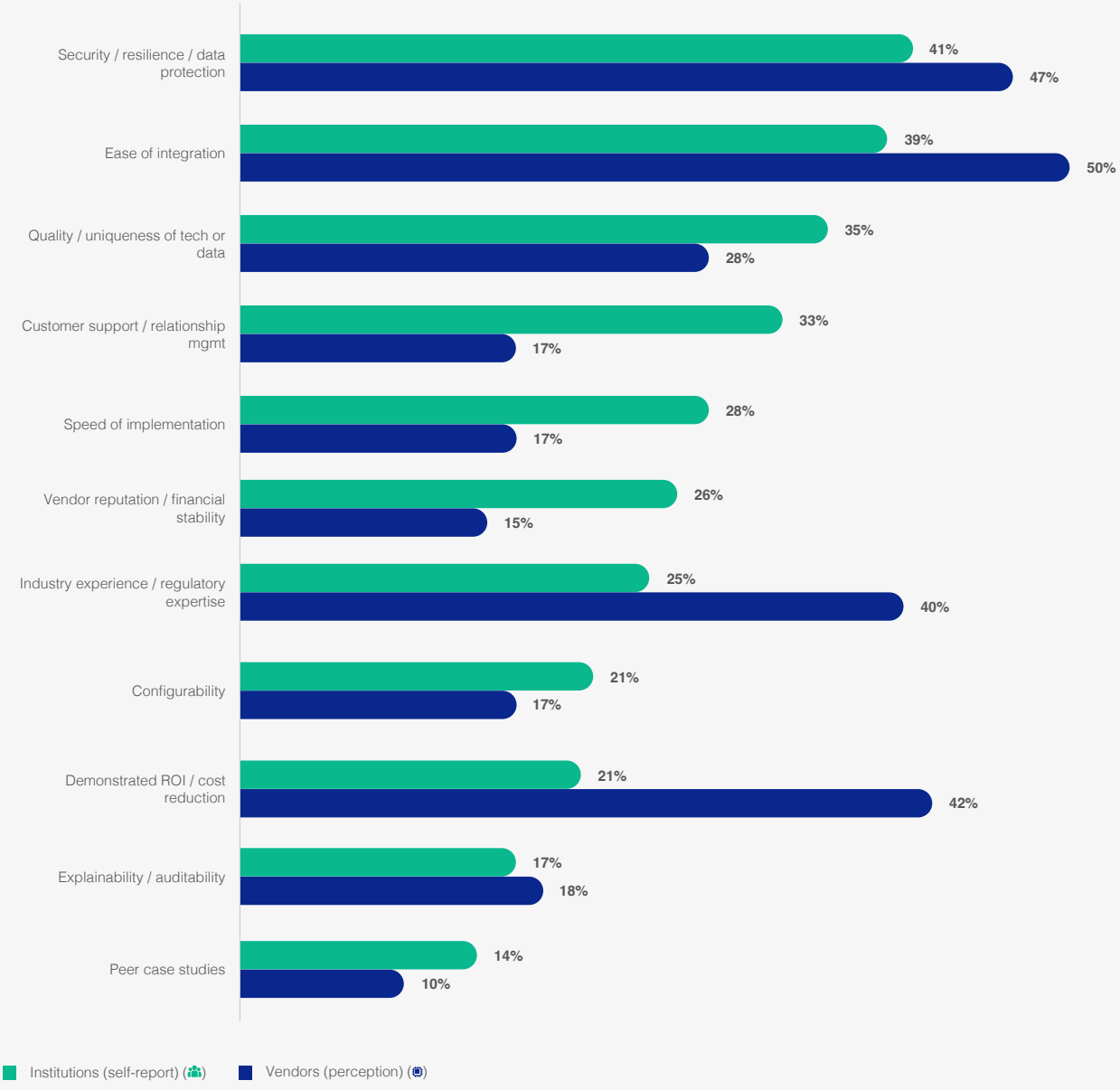
Buyers often lack the time and expertise to assess and compare the tens, or sometimes hundreds, of relevant vendors. As a result, confidence in decision-making is constrained, and many turn to external sources to guide and validate their choices.

Discovery is typically led through peer recommendations, industry events, and research reports – channels that provide initial orientation in a crowded landscape. Consultancies then play a more hands-on role, supporting vendor shortlisting and detailed assessment.

Beyond addressing capacity constraints, buyers are clearly seeking evidence-based validation and demonstrable capabilities before committing to a solution. Trust is not easily earned.

Vendor Selection Criteria

When selecting a third-party RegTech solution, which factors are most important to financial institutions?



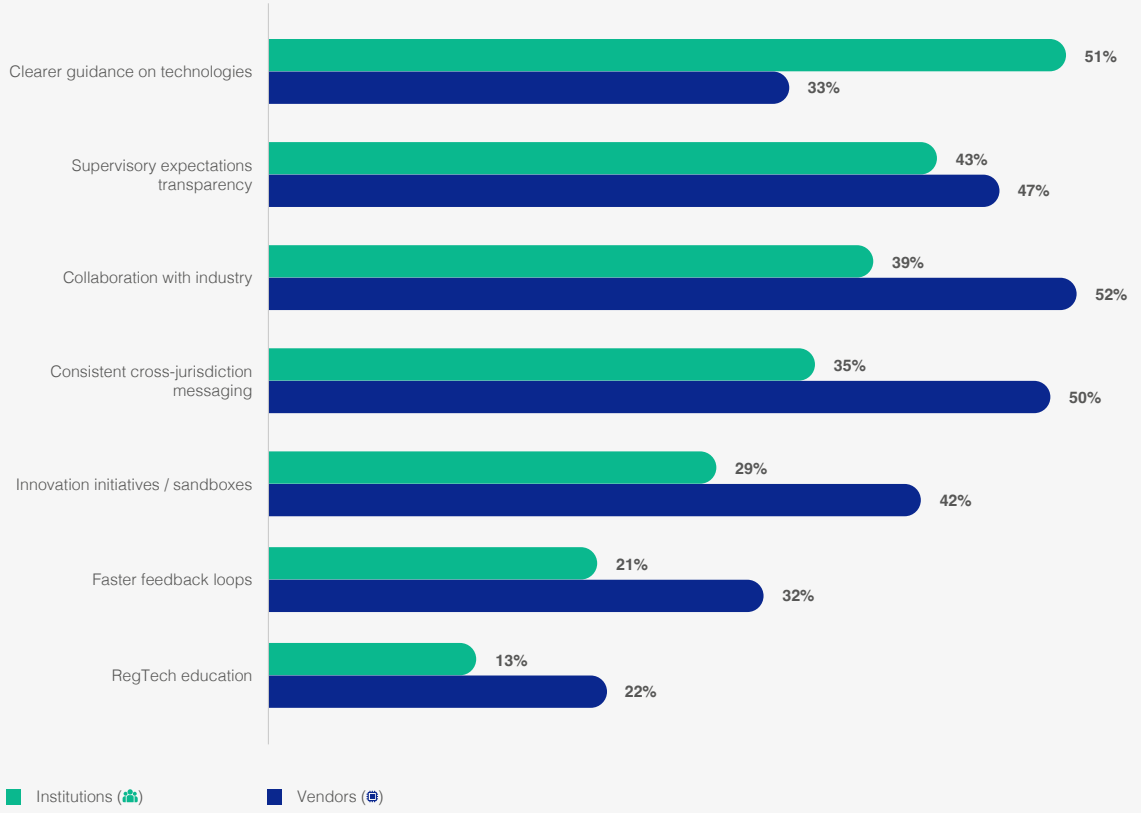
41%

of FIs cite security / resilience / data protection among their key vendor selection criteria.

- Buyers and sellers are aligned on the most critical criteria; security, resilience and ease of integration.
- Vendors may underestimate the value of customer support and relationship management, as well as the speed of implementation.
- Buyers place less emphasis than expected on demonstrated ROI. While this may appear to conflict with their struggles to justify the business case, it reflects the idiosyncratic nature of many institutions and a scepticism that results achieved elsewhere will translate to their own environment.

The Role of the Regulator

What would you most like to see from regulators to support effective RegTech adoption?



We support firms across the *innovation lifecycle*: helping them navigate complexity, test propositions safely, and move towards market deployment with greater confidence.

— Jessica Rusu and Colin Payne, *FCA Innovation* Insights Foreword

51% of FIs want clearer guidance from regulators on acceptable technologies in risk and compliance.

Institutions want clarity on technology and regulatory expectations. Vendors are more likely to emphasise collaboration and cross-border consistency. Regulatory approaches vary significantly by jurisdiction.

In the UK, the FCA has taken an open and engaged stance, promoting innovation through sandboxes and other initiatives while maintaining neutrality across technologies and vendors*. UK regulators are broadly seen as accessible, with a willingness to work with firms as challenges arise. By contrast, the US landscape is more fragmented across states and agencies, with a greater reliance on enforcement-led influence.

Despite continued scrutiny and high levels of enforcement, the role of regulators is evolving. Alongside financial penalties, regulators are increasingly using a wider set of tools to support the industry, including closer engagement during supervisory reviews, credit for self-reporting and structured innovation initiatives.

*The FCA recently published **Innovation insights 2025**, a report covering its learnings on the global FinTech market and how firms are using its innovation services.

Domain Deep Dives

Deep Dive: Compliance Management

Subcategories

Compliance Assessment: Solutions that evaluate an organisation's adherence to regulatory requirements and internal policies through controls testing, gap analysis, risk scoring, and reporting.

Compliance Orchestration: Solutions that coordinate and integrate multiple compliance activities, systems, and workflows across the organisation, enabling seamless execution of regulatory processes.

Regulatory Change Management: Solutions that help firms systematically assess, implement, and document responses to regulatory changes, involving impact analysis, task assignment, workflow automation, and compliance tracking.

Regulatory Intelligence: Platforms that provide structured insights into regulatory environments, including analysis, interpretation, and contextualisation of regulations to support informed compliance decisions.

Vendor Snapshot

900+
products from 500+ providers

58%
of vendors expect financial institutions' related technology spend to increase in 2026

$787m
raised by Compliance Management vendors in 2025, across 32 deals

RegTech Adoption

	UK + Europe	North America	APAC	MENA
Core part of control environment	6%	10%	22%	8%
Scaled enterprise use	22%	19%	15%	18%
Functional use in some teams	29%	39%	27%	30%
Pilot/limited use	27%	21%	28%	15%
No meaningful use	16%	11%	8%	30%
Don't know/prefer not to say	-	-	-	-

End-to-end compliance management is seldom automated for many institutions. Global "core control" adoption remains at just **11%**. Technology use is fragmented; many firms deploy RegTech for horizon scanning and regulatory alerts, but revert to manual spreadsheets for analysis, interpretation, and execution.

15% of firms report no meaningful use of technology at all, a figure that is both striking and unsustainable. This is now beginning to shift. The pace and complexity of regulatory change, increasing board accountability, and the maturation of RegTech solutions are forcing firms to rethink their approach.

Trends

Key pain points

- **Data overload and interpretive complexity:** Firms can access more regulatory information than before, but they struggle to turn it into prioritised, actionable decisions. The issue is no longer aggregating regulatory updates; it is understanding what matters, to whom, and what to do next.
- **Defensibility and enforcement exposure:** Firms need to prove not just that they monitor change, but that they can show regulators what they knew, when they knew it, and how they responded. In vague or principles-based regimes, interpretation risk is itself a major pain point.
- **Board and senior management accountability:** Senior Manager accountability regimes are increasing personal responsibility for compliance failures. Boards want visibility into what is coming, what it means, and whether the institution is prepared.

Emerging threats

- **AI is being deployed across client-facing and compliance-sensitive workflows**, and firms risk breaching the legal and compliance frameworks that govern those interactions. It is not enough for AI to avoid obviously problematic behaviour; it must align with the actual regulations that would apply if a human were performing the task. That creates urgency wherever firms want to introduce AI into client-facing, advisory, marketing, communications, or compliance-sensitive workflows.
- **Shift toward continuous regulatory oversight:** Regulators are moving away from periodic supervision to more continuous, technology-enabled oversight. Firms face more frequent scrutiny, ongoing reporting requirements, and faster regulatory responses to emerging risks. This demands more real-time visibility into compliance performance.

Traditional compliance assurance models are breaking: Legacy compliance tools measure whether controls exist, not whether they work.

- **Traditional compliance assurance models are breaking:** Legacy compliance tools measure whether controls exist, not whether they work. Most maturity assessments and audits do the same thing. Risk is documented, controls are marked as "in place," and policies are recorded, creating a perception of compliance that may not reflect actual operating conditions. Complex, technology-enabled and data-heavy operating environments put this model under strain, and there is a growing disconnect between reported compliance and real risk exposure.

Emerging compliance capabilities

- **AI-enabled supervisory control layers for regulated workflows:** Embedding regulatory interpretation directly into operational workflows and AI interactions, enabling real-time validation of outputs, constraint of non-compliant actions, and dynamic enforcement of jurisdiction-specific rules. These capabilities extend compliance from post-hoc review into continuous, in-line control of both human- and AI-driven activities.
- **Predictive compliance intelligence:** Integrating external threat signals, regulatory history, and internal control performance data to identify emerging risk vectors and forecast potential supervisory focus areas. These capabilities enable early detection of new typologies, forward-looking control gap analysis, and pre-emptive alignment of compliance frameworks ahead of regulatory or risk escalation.
- **Intelligent regulatory change orchestration:** Leveraging AI to deconstruct new rules into actionable obligations, assess applicability, route work across teams, and create a traceable path from source text to implementation.

VIXIO

At the frontier of Regulatory Change Management

Vixio combines human expertise with AI-enhanced technology to deliver real-time, actionable regulatory intelligence across 200+ jurisdictions within a unified regulatory change management platform.

Founded: 2006 (UK)

Number of employees: 51-200

Regions: Global

Industries: Financial Services, Gambling & Gaming

Subsectors: Payment Services, Retail Banking, Digital Assets

Regulations addressed: Agnostic

Website: https://vixio.com

Funding: Backed by Perwyn Investments

Executive Chair: Christian Erlandson

Customers PayPal barclaycard Google bet365 playtech

Vixio

The Vixio platform provides end-to-end regulatory change management, combining horizon scanning with structured workflow execution in a single, integrated environment. By bridging the gap between intelligence and execution, the platform delivers three core value pillars: delivering curated, AI-supported intelligence to help firms stay on top of relevant developments; improving operational efficiency by streamlining compliance processes; and strengthening auditability through automated mapping and reporting aligned with governance requirements.

Key features

Horizon scanning: Monitors 8,000+ regulatory authorities across 200 jurisdictions, classifying activity into actionable, indicative, and informative updates. Customisable watchlists filter by jurisdiction, authority, and document type, with flexible alerting. Supported by detailed country reports, jurisdiction-specific requirements reports for key activities, and analyst-led commentary and thought leadership.

Intelligent filtering: Aggregates watchlist activity and prioritises updates using a proprietary scoring algorithm, combined with human validation to ensure relevance, accuracy, and materiality.

Obligations library: A centralised repository of regulatory obligations, enabling teams to extract, categorise, assess risk, and determine applicability.

Task management: Enables creation, assignment, tracking, and escalation of tasks across compliance and second-line stakeholders, ensuring accountability through to completion.

Country report builder: Generates jurisdiction-specific compliance assessments for gap analysis by generating tailored questionnaires based on jurisdictional requirements. Enables firms to evaluate compliance posture and convert outputs into remediation tasks.

Predictive obligations workflow: Uses obligation-to-policy linkages to anticipate remediation needs before changes are formally enacted.

Users

Primary: Chief Compliance Officers, Compliance Analysts.

Collaborative: Product, Marketing, and Operations teams (task assignees).

Underlying technologies

- **Digitised Regulatory Rule Sets:** Converts regulatory documents into a standardised digital format, creating a central, searchable repository within the platform.
- **Vectorised Regulatory Database:** A curated, closed corpus enabling semantic search and retrieval-augmented generation via tools like Vixio's AI assistant (VIQ).

Artificial intelligence

- **VIQ:** A domain-constrained LLM that enables users to query Vixio's proprietary regulatory dataset, generating summarised insights with traceable source references.
- **Supervised machine learning:** Vixio's proprietary SCANS technology (Scan, Collate, Aggregate, Normalise, Surface) applies supervised learning, trained on 20+ years of regulatory expertise, to capture and filter updates, eliminating up to 80% of irrelevant noise before analyst review.
- **Hybrid AI + human intelligence layer:** Combines machine learning and LLM-based processing with expert analyst validation to determine relevance, interpret regulatory change, and ensure outputs are accurate, contextualised, and actionable.
- **Pre-configured AI "lenses":** Task-specific prompts (e.g. regulatory tracking, board briefings) that standardise outputs for common compliance use cases.

Top value drivers

- **Managing regulatory change more effectively:** Transforms regulatory change management from an ad hoc, reactive process into a structured, repeatable, and scalable system.
- **Improving operational efficiency and reducing cost:** Reduces manual effort across the compliance lifecycle through automated alert triage, AI-assisted research, and streamlined reporting.
- **Improving data quality and transparency:** Establishes a single, centralised source of truth for regulatory obligations across jurisdictions, replacing fragmented, individual-dependent records with consistent, auditable data.

Case study

Client type
Financial services firm

Challenge
Following a major acquisition, the client faced fragmented AML/CTF frameworks across business units, with no centralised, scalable policy framework. This led to reliance on siloed documents and tribal knowledge rather than consistent, auditable processes.

Solution
Instead of retrofitting legacy systems, the client used the Vixio platform to build a standardised compliance framework. Using flexible board-building capabilities, they mapped regulatory obligations into a structured digital environment with the control of a custom solution.

Outcome

9

specialised management boards created a centralised global compliance hub. This shift to an auditable, structured system reduced operational risk and established a repeatable framework ready for expansion.

Two-year outlook

The category will shift from content delivery to decision support and execution. The regulatory change management process is evolving to become less about reacting to regulatory change, and more about adding business value through foresight to enable growth through new market entry and adaptability.

Agentic workflows (AI that autonomously monitors, flags, and pre-populates tasks) will become more prevalent. However, in high-stakes compliance environments, these capabilities will remain advisory rather than substitutive, with human oversight and sign-off continuing to be essential.

Compliance operating models will shift toward strategic, intelligence-led functions. Demand will grow among firms repositioning compliance as a strategic capability rather than a cost centre. Organisations prioritising forward-looking intelligence, structured obligation management, and cross-functional coordination will increasingly invest in platforms that enable scalable, operationalised compliance.

Norm Ai

At the frontier of Regulatory Intelligence

Norm Ai is building agentic law, the embedding of law into AI agents. The company pioneered Legal Engineering—training elite lawyers to translate legal and regulatory frameworks into AI-driven workflows, fundamentally reshaping how legal expertise delivers business outcomes.

Legal Engineers transform complex rules into structured, machine-readable logic, enabling the creation of scalable, technology-driven solutions. This proprietary approach allows organisations to operationalise regulations and internal policies directly within AI systems.

Norm Ai's platform supports the compliant deployment, oversight, and governance of AI agents in regulated environments, helping organisations scale AI adoption while maintaining control, transparency, and accountability.

Founded: 2023

Number of employees: 201-500

Regions: Global

Industries: Financial Services

Subsectors: Asset Management, Investment Advisory / Wealth Management, Broker-Dealers, Private Equity, Investment Banks, Retail Banks, Insurance

Regulations addressed: Global coverage

Website: https://www.norm.ai

Funding: Raised over $140 million to date, with backing from Blackstone, Bain Capital, Vanguard, Citi, and Coatue and more.

Founder & CEO: John Nay (Previously founded an AI-powered investment platform acquired by TIAA Nuveen, and brings a background spanning NSF- and ONR-funded AI research, academic roles at Harvard and NYU, and pioneering work in AI and law at Stanford's CodeX.)

Customers Blackstone BainCapital New York Life Vanguard Capital Group

Norm Ai

The Norm Ai platform converts laws, regulations, and firm-specific policies into machine-executable logic embedded within domain-specific AI agents. These agents automate compliance by evaluating information against defined standards and making consistent, explainable determinations across business workflows.

This core capability can be applied across a wide range of compliance use cases, with pre-built agents available for common workflows and the flexibility to configure solutions to firm-specific requirements.

Key features

Standards-based reasoning: Evaluates inputs against regulatory frameworks, internal policies, and defined standards to produce structured, defensible compliance decisions.

Citation-backed explainability: Provides transparent reasoning with direct references to relevant regulations, policies, and source materials for every determination.

Substantiation and evidence validation: Extracts and verifies claims against approved source-of-truth data to ensure outputs are accurate, consistent, and defensible.

Automated remediation and redlining: Generates compliant revisions and corrective actions to resolve identified issues in line with regulatory and firm requirements.

Auditability and decision traceability: Maintains full audit trails, version history, and decision lineage to support regulatory review and internal governance

Users

Primary: Legal & Compliance

Companies use Norm for an array of critical regulatory assessments, but some core use cases include:

Regulated content and marketing review: Evaluating marketing and communications against regulatory and internal standards, identifying non-compliant content, including statements, charts, and images, missing disclosures, and unsubstantiated claims.

DDQ / RFP automation and validation: Generating and validating due diligence and RFP responses using approved source-of-truth materials. Documents can also be processed against the same regulated content review agents.

Supervisory AI: Real-time and post-hoc monitoring of AI-generated outputs (e.g. copilots, chatbots), with compliance validation and escalation pathways.

Underlying technologies

- **LEAP (Legal Engineering Automation Platform):** Proprietary platform used by legal engineers to encode, test, and maintain regulatory and policy logic within AI agents, enabling continuous adaptation to evolving legal and compliance requirements.
- **Enterprise data layer:** Integrates the firm's canonical data – product lines, jurisdictions, organisational structures, and internal policies – into agent logic, ensuring AI agents operate within the specific business and regulatory context required to execute workflows.
- **Decision graph:** Proprietary language to represent government regulations and corporate policies as decision trees.

Artificial intelligence

- **Regulatory AI Agents:** Large language models convert regulations into "Regulatory AI Agents": executable programs that capture the full scope of regulatory requirements. These agents can make real-time compliance determinations, execute complex multi-step workflows, and provide clear, actionable feedback to enterprise users.

Top value drivers

- **Supporting business growth:** Enables organisations to deploy AI agents across business-critical compliance workflows. This unlocks speed, scale and new capabilities that would otherwise be constrained by legal and compliance limitations.
- **Improving operational efficiency and reducing cost:** Transforms heavily manual, resource-intensive legal and compliance workflows into automated, scalable processes, significantly increasing throughput and removing compliance bottlenecks.
- **Reduced regulatory exposure:** Applies consistent, standards-based compliance controls across workflows and AI systems, reducing the risk of non-compliant outputs, regulatory breaches, and downstream remediation.

Two-year outlook

AI expands into regulated decision-making. AI will be deployed across a growing range of regulated workflows, taking on tasks previously performed by humans or not feasible at scale. This will drive demand for infrastructure that ensures continuous alignment with legal and regulatory requirements.

Compliance becomes code. As AI agents scale, firms will need to encode regulatory frameworks and firm-specific policies directly into systems, enabling real-time, standards-based decision-making and AI-to-AI supervision. Compliance will evolve from a downstream control to an always-on layer integrated directly into business processes, underpinning the safe deployment of AI at scale.

Supervisory AI will become a de facto control layer. As organisations deploy copilots, chatbots, and autonomous agents across customer-facing and internal workflows, a new class of AI systems will be required to monitor and validate those outputs in real time.

At the frontier of Compliance Assessment

Argus Pro helps regulated firms show whether compliance controls work in practice. The firm was founded by a team with complementary experience across government policy and compliance culture, global financial crime investigations, and commercial data and advisory, bringing together perspectives from the regulator, the practitioner and the boardroom. They built the product to address a consistent gap in traditional maturity assessments, which often show that controls exist but not whether they are being applied consistently or effectively. It is particularly relevant for firms facing supervisory scrutiny, regulatory change or multi-jurisdiction obligations.

Founded: 2022 (UK)

Number of employees: 2-10

Regions: Global

Industries: Financial Services, Insurance, Professional Services, Legal, Crypto & Digital Assets.

Subsectors: Investment banks, Retail (challenger banks and building societies), Payment service providers and e-money firms, Insurers and reinsurers, Crypto exchanges and custodians

Regulatory areas: Financial crime; cybersecurity and digital operational resilience; AI governance; ESG.

Website: https://arguspro.co.uk

Funding: Self-funded

Co-founder & Partner: Mike Falvey (25+ years of senior leadership across Financial Services, Government, Private Equity in the US and the UK, and regulated industries.)

Partners TRAVERSE FinTech-Tables

Argus Pro

Aegis Compass is a structured compliance assessment platform that turns mapped regulatory requirements into multi-respondent assessments, weighted scoring, dashboards and context-aware remediation outputs. It captures responses anonymously across roles, locations and seniority levels, compares how different teams describe the same control, and links each question back to the underlying regulatory clauses. The result is a clearer picture of where policy exists, where execution breaks down, and what action should be prioritised.

Key features

Regulatory-mapped assessment frameworks: Decomposes legislation, regulation and guidance into domains, obligations and questions, so assessments are anchored to specific requirements rather than generic checklists.

Dual scoring of maturity and effectiveness: Evaluates both whether controls exist and how well they work in practice, avoiding the false comfort of maturity scores alone.

Anonymous triangulation across the organisation: Uses stratified, multi-respondent sampling to compare answers across roles, locations and seniority levels, surfacing hidden gaps and perception differences that workshop-based approaches often miss.

Clause-level traceability and dashboards: Lets users move from domain scores to question-level variance and see the relevant underlying clauses and jurisdictions behind each issue.

Targeted, context-aware remediation: Distinguishes execution gaps, capability gaps and other root causes, supporting more precise remediation than broad redesign programmes.

Users

First line: Control owners, subject matter experts, compliance managers, financial crime specialists, cybersecurity and operational resilience respondents.

Second line: Heads of Compliance, MLROs, Heads of Financial Crime, CISOs, Heads of Operational Resilience, General Counsel teams.

Third line: Chief Compliance Officers, Chief Risk Officers, boards, risk committees and non-executive directors.

Underlying technologies

- **Regulatory ingestion and decomposition engine:** Ingests legislation, regulation and guidance across jurisdictions, then decomposes them into harmonised domains, obligations and mapped questions.
- **Multi-respondent sampling and scoring engine:** Supports randomised sampling, anonymity, weighted scoring and comparison across roles, teams and locations.
- **API-based integration layer:** Designed to connect with existing GRC and workflow tools such as ServiceNow and MetricStream, and with client policy environments in Azure or AWS.

Artificial intelligence

- **Natural language processing:** Used upstream of assessments to ingest and interpret regulatory updates, identifying changes between new and existing legislative, regulatory and guidance instruments.
- **Machine learning:** Will be applied to detect patterns and relationships across structured and unstructured data, supporting the identification of emerging risk typologies which can trigger a review of relevant assessment results and be prioritised for future assessments.
- **Generative AI:** Compares regulatory updates to internal policies to identify gaps and suggest changes, which can then feed new assessments.

Case study

Client type
Global RegTech provider (serving crypto and trading environments)

Challenge
The client required a transaction monitoring rule framework that would withstand regulatory scrutiny across multiple jurisdictions, with an initial scope of 40 rules

Solution
Argus Pro anchored the framework to FATF standards and expanded coverage across 12 regulatory bodies, delivering a fully mapped, implementation-ready rule set with direct regulatory traceability

Outcome

254

implementation-ready rules, providing global coverage across 15 key risk areas and enabling a single, scalable framework aligned to regulatory expectations

Top value drivers

- **Reducing regulatory exposure (e.g. enforcement, fines):** Surfaces inconsistencies in interpretation and execution across teams and locations, helping identify issues before they lead to breaches or enforcement action
- **Remediation of control weaknesses/supervisory findings:** Distinguishes root causes of failure (e.g. execution vs capability gaps), enabling targeted, evidence-based remediation rather than broad control redesign
- **Improving operational efficiency and/or reducing cost:** Reduces reliance on manual workshops and fragmented assessments, while focusing effort on the areas of greatest risk and variance

Two-year outlook

Supervision will become continuous and outcome-focused: Regulators are moving away from periodic assessments toward ongoing scrutiny, requiring firms to evidence how controls are applied in practice. Argus Pro is responding by developing scenario-based assessment capabilities that allow firms to demonstrate, in a fully auditable way, how staff apply policies and training in live environments

Risk intelligence will become more forward-looking and predictive: Institutions will increasingly combine emerging threat signals with historical regulatory response patterns to anticipate both new typologies and likely supervisory expectations. Argus Pro's NexEdge roadmap reflects this shift, aiming to provide intelligence that helps firms get ahead of both risk and regulation

AI will accelerate the gap between threat and response: As bad actors rapidly deploy AI at scale, regulated firms will remain constrained by governance and explainability requirements. This asymmetry is likely to drive regulatory adaptation, with firms adopting AI-enabled capabilities that prioritise speed, transparency and accountability

Deep Dive: Financial Crime Compliance

Subcategories

KYC / KYB: Solutions that verify and screen customer (KYC) and business (KYB) identities to support regulatory compliance and financial crime risk management, including data collection, identity verification, sanctions screening, and adverse media checks.

Transaction Monitoring: Systems that analyse financial transactions to detect and flag suspicious activity linked to money laundering, terrorist financing, or sanctions evasion, using rules, behavioural analytics, and alerting workflows.

Sanctions Screening: Solutions that screen customers, counterparties, and transactions against global sanctions lists and watchlists to identify prohibited or high-risk relationships and ensure compliance with regulatory requirements.

Fraud Prevention and FRAML: Technologies that detect and prevent fraudulent activity by combining fraud and anti-money laundering controls, using behavioural analytics, machine learning, and real-time decisioning across customer and transaction data.

Vendor Snapshot

1000+
products from 400+ providers

81%
of vendors expect financial institutions' related technology spend to increase in 2026

$892m
raised by Financial Crime vendors in 2025, across 48 deals

RegTech Adoption

	UK + Europe	North America	APAC	MENA
Core part of control environment	29%	28%	28%	25%
Scaled enterprise use	39%	31%	37%	43%
Functional use in some teams	19%	27%	22%	25%
Pilot/limited use	11%	11%	7%	8%
No meaningful use	2%	3%	7%	-
Don't know/prefer not to say	-	-	-	-

Financial Crime Compliance is the benchmark for RegTech maturity, boasting the highest core control adoption globally at **28%**. This space has benefited from decades of regulatory forcing functions and a highly competitive vendor landscape, shifting the focus from adoption to optimisation.

In a category where only **3%** of firms have "no meaningful use," the competitive advantage revolves around how that tech is integrated. Buyers are re-architecting for real-time decisions, cross-domain risk and provable effectiveness. The stronger solutions are those that combine unified operating workflows, entity-centric intelligence and governed AI, rather than adding another point tool to a fragmented stack.

Trends

Key pain points

- **Operational overload from low-precision controls and manual investigation work**. Too much of the operating model is still built around labour-intensive review of low-value noise. That matters more in 2026 because supervisors are increasingly judging programmes on whether controls are effective in practice, not merely documented on paper.
- **Fragmented entity data is undermining KYC, KYB, sanctions and fraud controls**. Many firms still struggle to build a reliable picture of who a customer, business or counterparty really is. Legacy approaches built around periodic refreshes, fragmented master data and name-only screening struggle because modern financial crime risk signals are relational, not just attribute-based.
- **The tension between speed, customer experience and defensible control is getting harder to manage**. Institutions are under pressure to reduce corporate onboarding friction. Legacy batch screening, channel-specific fraud tools and episodic KYC/B refreshes are poorly suited to this environment because the decision window is shorter, the customer tolerance for friction is lower, and the rationale for every intervention must still be auditable.

Financial institutions are seeing increased suspicious activity involving deepfake media and fraudulent identity documents used to bypass verification and authentication.

Emerging threats

- **AI-enabled impersonation, synthetic identity and industrialised scam operations**. Financial institutions are seeing increased suspicious activity involving deepfake media and fraudulent identity documents used to bypass verification and authentication, while law enforcement assessments now describe scam operations as globally distributed, polycriminal and increasingly AI-augmented.
- **Sanctions evasion is becoming more networked and geopolitically fragmented**. The practical result for firms is a more expensive and legally fraught operating environment, especially where one regime focuses on ownership thresholds while another expects broader diligence around de facto control or circumvention risk.
- **Faster and more interconnected payments are compressing intervention windows**. The Bank for International Settlements has warned that faster cross-border transactions can increase fraud and illicit use, driving stricter AML/CFT screening and higher compliance costs.* Payments have shifted from hours to seconds, and that fundamentally reduces the time available for detection, intervention and recovery.

Emerging compliance capabilities

- **Entity-centric, cross-domain financial crime decisioning layers:** Unified decisioning environments that orchestrate alerts, cases, and risk signals across domains in real time. These capabilities combine transaction behaviour, customer lifecycle data, and external intelligence into a single, contextual risk view, enabling institutions to make faster, more consistent decisions at the entity level rather than at the alert level.
- **Law-mapped, explainable decision engines for automated onboarding and lifecycle compliance:** Translating legislation and regulatory guidance directly into machine-executable logic, enabling platforms to produce auditable, jurisdiction-specific “go / no-go” decisions for onboarding, classification, and suitability in real time. These capabilities embed regulatory interpretation into the decision layer itself, combining symbolic AI, machine learning, and agent-based orchestration to deliver straight-through processing while maintaining traceability back to source regulations.
- **Network-based risk intelligence and relationship-driven screening:** Dynamic, graph-based intelligence that maps ownership, control, trade, and indirect relationships between entities. These capabilities use knowledge graphs, exposure scoring, and AI-assisted research to uncover hidden risk pathways and provide explainable, source-backed evidence for investigations.

*https://www.bis.org/publ/bisbull119.pdf

muinmos

At the frontier of KYC / KYB

Muinmos' platform performs client onboarding and lifecycle management using AI-orchestrated agents. Its platform is particularly well-suited to firms managing complex, cross-border onboarding where regulatory interpretation and investor protection requirements materially impact business operations. Founded by technology, compliance and legal practitioners, Muinmos is built on the principle that onboarding should deliver a fast, clear, law-based answer to a single question: whether or not a client can be compliantly onboarded (and the relationship maintained), based on the applicable regulation and the institution's policies.

Founded: 2012 (Denmark)

Number of employees: 11-50

Regions: Global

Industries: Financial services, professional services

Subsectors: Investment firms, Banks, FinTechs including crypto, Payment providers, Wealth managers

Regulatory areas: KYC and KYB, AML including PEP, sanctions & adverse media screening and monitoring, client risk assessment, client classification / investor categorisation, suitability & appropriateness.

Website: https://muinmos.com

Funding: Private

CEO: Remonda Kirketerp-Møller (Over 25 years of experience as a qualified lawyer, compliance executive, and tech entrepreneur, founding Muinmos with firsthand experiences of systemic inefficiencies in global client onboarding.)

Customers MAREX CROSSOVER GCEX Acuity

Muinmos

Muinmos' platform is an end-to-end client onboarding and lifecycle management solution that uses advanced AI to orchestrate the entire compliance journey. It performs KYC/KYB checks, including screening, regulatory classification, suitability and appropriateness, client risk assessment, and ongoing monitoring.

At its core is a configurable, law-mapped decision engine that combines proprietary regulatory logic with integrated data sources. This enables the platform to assess both individuals and complex corporate structures, apply jurisdiction-specific rules across products and services, and deliver a fully auditable go/no-go onboarding decision.

Key features

End-to-end orchestration of client onboarding and lifecycle management (CLM): Performs end-to-end onboarding of clients, including a hosted application, data storage and more. Allows for continuous pKYC throughout the client lifecycle.

Individual KYC & identity verification: Verifies identities in various ways including IDV, liveness, eIDV and document validation, supporting over 2,050 identity document types across 200+ jurisdictions and connections to 260+ registries across 73 jurisdictions.

Corporate KYB & entity intelligence: Automates corporate onboarding using data on over 650 million corporates and 290 million directors, sourced from 9,100+ registries and data sources to validate ownership structures and business activity.

AML & PEP, sanctions and Adverse Media screening: Screens clients against 2,200+ watchlists, covering over 4 million entities and individuals across 200+ jurisdictions and 230+ sanction regimes, supporting consistent and globally scalable compliance checks.

Client classification and suitability assessment: Determines regulatory client category (e.g., MiFID, MiCA) and assesses whether clients can access products based on knowledge, experience, financial profile and objectives, ensuring alignment with regulatory requirements and investor protection standards.

Users

Business: COO, CFO, CEO, Business Development and Digital Transformation Leads

Compliance: Compliance Officer, Risk Officer, Legal

Sales / Onboarding: Sales Lead, Onboarding Lead

Underlying technologies

- **Law-mapped decision engine:** Built from legislation and regulatory guidance, with rules, questions and outcomes mapped to the relevant legal requirement to support explainability, consistency and auditability.
- **Identity and entity data layer:** Supports ID scanning, OCR, liveness, corporate data retrieval and ownership-structure analysis for both individuals and legal entities.
- **API, reporting and control layer:** Supports API integration into CRM and back-office systems, generates white-labelled PDF reports and audit trails, and keeps production data encrypted and under customer control.

Artificial intelligence

- **Rule-based / symbolic AI:** Translates legislation and regulatory guidance into structured, explainable decision logic.
- **Machine learning and natural language processing:** Used for minimisation of false-positives, lowering manual work and supporting more accurate risk scoring.
- **Agentic automation:** An orchestration agent coordinates multiple specialised agents across the onboarding lifecycle, enabling end-to-end, straight-through processing while maintaining control, auditability and human oversight.

Case study

Client type
Global multi-asset brokerage

Challenge
The client's onboarding processes were manual and fragmented, consuming too much time from valuable experts, unable to scale and increasing the risk of inconsistencies and errors.

Solution
Muinmos' platform allowed the client to automate their end-to-end onboarding process and continuous due diligence (pKYC) in one platform.

Outcome

96%

reduction in onboarding time, along with structure, consistency and auditability across automated KYC processes.

Value drivers

- **Scalability across jurisdictions:** Scalable frameworks and reusable controls aligned with existing and incoming regulatory requirements allow easier expansion across markets and product lines.
- **Straight-through onboarding at scale:** Agentic orchestration of the entire onboarding journey removes breakpoints and hand-offs and shortens "time-to-yes". One global multi-asset brokerage achieved a 96% reduction in onboarding time while freeing expert reviewers for genuinely complex cases.
- **Enhancing customer experience and outcomes:** Less friction, fewer document loops and improved user experience.

Two-year outlook

The category will gradually move toward end-to-end automation of onboarding decisions. This will drive consolidation of fragmented technology stacks, deeper integration with core CRM and operational systems, and more advanced use of AI to enable real-time, decision-ready processes.

Heightened scrutiny driven by investor protection. Increasing regulatory focus on investor protection will raise expectations for the accuracy and consistency of onboarding decisions. Firms will face greater scrutiny on process design and on the integrity, auditability, and outcomes of their onboarding frameworks.

Board-level ownership of compliance transformation. Boards are increasingly treating onboarding automation as a strategic rather than operational decision – driven by cost pressure on large compliance teams and the opportunity to turn compliance into a business enabler.

At the frontier of Transaction Monitoring

IMTF is a Swiss RegTech provider focused on anti-financial crime compliance. Its Siron®One platform and related services span transaction monitoring, screening, KYC/CDD, fraud and case management, with a particular emphasis on configurable detection logic, workflow orchestration and cross-domain decisioning. The company sits between startup and incumbent models: long-established and privately owned, but still agile in how it develops and adapts the product with clients.

Founded: 1987 (Givisiez, Switzerland)

Number of employees: 201-500

Regions: Europe, North America, Middle East & Africa, and Asia-Pacific

Industries: Financial Services

Subsectors: Retail and commercial banking; private banking and wealth management; fintechs and payment service providers; trade finance and corporate banking environments

Regulatory areas: AML/CFT transaction monitoring; sanctions and embargo compliance; KYC/CDD and client lifecycle compliance; suspicious activity reporting; fraud prevention; trade-based money laundering controls

Website: imtf.com

Funding: Privately owned

Co-CEOs: Gion-Andri Büsser and Dr. Sebastian Hetzler (ex-Google and McKinsey)

Customers: DBS, HSBC, Luminor, Finanz Informatik, Vodafone

IMTF

Within transaction monitoring, Siron®One combines configurable scenarios, customer segmentation, dynamic risk scoring, simulation and integrated alert-and-case management in a single detect/decide workflow. It links detection with investigation so teams can review alerts in a broader customer-risk context, automate routine routing and documentation steps, and adapt monitoring logic without code. As part of the broader Siron®One platform, it connects transaction monitoring directly with adjacent domains such as sanctions, KYC, and fraud, enabling cross-domain orchestration and a more holistic, contextual view of risk. This allows institutions to move from siloed controls toward a more unified and intelligence-driven approach to financial crime compliance.

Key features

Scenario-based transaction monitoring: Configurable AML scenarios support customer categories, segment-specific thresholds and risk-based logic without requiring code, and can leverage data from onboarding and KYC processes to enrich detection with more accurate and contextual information.

Simulation and controlled rollout: Forward and backward simulation allows teams to test thresholds and assess impact on real data before moving changes into production.

Cross-domain alert and case management: Analysts can review transaction monitoring alerts alongside related screening and KYC signals in a 360-degree customer view rather than working in silos.

Workflow orchestration and tasking: Alerts can be prioritised, assigned, routed, documented and escalated through configurable tasks, forms and decision workflows.

Regulatory and management reporting: The platform supports governance reporting, model-performance visibility and regulatory reporting such as SAR/STR workflows.

Feedback-driven learning loop: Incorporates investigation outcomes and performance analytics to continuously refine detection logic, alert prioritisation, and workflows.

Users

Operational Users: AML analysts, compliance officers, investigators

Risk and Compliance Leadership: MLRO, Head of Financial Crime, Chief Compliance Officer

Technology and Governance Stakeholders: CIO, CTO, Head of IT, governance stakeholders

Underlying technologies

- **Unified data integration and normalisation layer:** Consolidates onboarding/KYC, transaction and external intelligence data into a consistent structure that can be reused across monitoring and investigations.
- **Modular open architecture:** Supports cloud, on-premise and hybrid deployments, high-volume real-time processing, and API-based integration with banking, payments and third-party systems.

Artificial intelligence

- **Alert Predictive Score (APS):** Compares new alerts with historically confirmed alerts to help prioritise analyst review.
- **Entity Deviation Score (EDS):** Uses AI-based clustering to identify when a customer behaves differently from its peer group and feeds that signal into detection logic.
- **Behavioural and entity-centric profiling:** Supports anomaly detection, contextual risk assessment and network-based analysis across customers, transactions and related entities.

All AI capabilities are designed with strong governance, explainability, and human-in-the-loop controls, ensuring transparency, auditability, and alignment with regulatory expectations.

Case study

Client type
Large Tier 1 international retail bank

Challenge
Slow, manual onboarding processes and high volumes of false positives created operational inefficiencies and limited visibility into customer risk

Solution
IMTF deployed real-time automated screening and intelligent case management, replacing paper-based workflows and introducing prioritised, risk-based alert handling.

Outcome

86%

reduction in alerts requiring manual investigation, significantly improving productivity, lowering operational costs, and enabling faster, more proactive decision-making process.

Value drivers

- **Reducing false positives and manual workload:** Helps institutions improve analyst productivity and shorten investigation times by ranking and contextualising alerts more effectively.
- **Improving contextual risk assessment:** Links customer lifecycle, transaction and external data to support more consistent, entity-centric decisions across financial crime workflows.
- **Supporting real-time and scalable compliance:** Helps institutions adapt monitoring and decisioning to instant payments, digital channels and multi-jurisdiction operations.

Two-year outlook

Transaction monitoring will become more platform-based and cross-domain, with institutions expecting alerts, cases and customer context to be orchestrated across AML, sanctions, KYC and fraud within a unified entity-centric decisioning layer rather than managed in separate tools.

Hybrid AI will move from experimentation to governed operational use embedded directly into workflows, combining rules, machine learning and human oversight, while regulators focus more directly on explainability, accountability and model transparency.

Continuous testing, feedback loops, and outcome-driven optimisation will become standard expectations, as institutions move toward more data-driven and evidence-based compliance operations.

Real-time and network-based monitoring will matter more as instant payments, cross-border activity and technology-enabled financial crime increase, shifting teams from retrospective detection toward faster, more contextual and entity-centric decisioning.

KHARON

At the frontier of Sanctions Screening

Kharon is a data and technology company specialising in risk intelligence for sanctions compliance, export controls, and financial crimes. Its proprietary platform combines continuously updated risk data, exposure analysis, and AI-enhanced, analyst-validated research to reveal ownership structures, trade flows, shipping activity, and financial relationships that conventional screening misses. Kharon helps organisations move beyond watchlist matching to screen against the full network of risk — identifying exposures through ownership, control, and other indirect relationships. The same intelligence powers partner platforms across the compliance ecosystem, embedding Kharon's risk data where decisions are made.

Founded: 2016 (Denver, Colorado, United States)

Number of employees: Private / not publicly disclosed

Regions: Global, with offices in Washington D.C., New York, Los Angeles, London, Madrid, and Tokyo.

Industries: Financial Services, Corporates, Manufacturing & Industrial, Public Sector.

Subsectors: Global banks (compliance, financial crime, and investment departments); exporters and advanced technology manufacturers; importers; supply-chain-intensive multinationals; government and enforcement agencies.

Regulatory areas: Sanctions ownership and control screening; sanctioned securities and investment restrictions; export controls and military end-use risk; forced labour and supply chain due diligence; AML / financial crimes investigations, investment risk.

Website: kharon.com

Funding: Private

CEO: Matthew Epstein (Senior U.S. Treasury background across OFAC and TFI, including regional sanctions leadership in the Middle East.)

Customers BARCLAYS · CISCO · U.S. DEPARTMENT OF THE TREASURY · U.S. Customs and Border Protection

Kharon

Kharon delivers network-based risk intelligence for sanctions, trade controls, and financial crimes compliance. ClearView provides interactive network visualisation, letting analysts explore ownership chains, control relationships, trade patterns, and other connections – every relationship source-backed and exportable for audit. GraphCast feeds structured risk data into existing screening environments, reducing false positives and enabling one-click alert analysis. CoreStream delivers AI-powered, continuous risk monitoring with tailored intelligence summaries. The Kharon API supports custom workflows and automation at scale. Together, the platform moves firms from flat watchlist matching toward relationship-based screening, reducing noise, cutting review time, and making compliance decisions more explainable.

Key features

Network visualisation: ClearView lets analysts visualise ownership chains, control relationships, trade flows, and other connections — turning complex risk networks into explainable, auditable intelligence.

Structured risk data for screening: GraphCast delivers curated, analyst-validated datasets into existing screening and analytics systems — covering exposure across sanctions, export controls, financial crimes, and investment risk.

Exposure scoring: Proprietary scoring surfaces how exposed an entity is to specific risk themes, prioritising the most relevant connections and helping analysts focus where it matters.

Flexible workflow integration: Kharon data can be delivered in formats aligned to existing screening tools, with deep links that bring analysts directly from an alert into the underlying network view.

Continuous risk monitoring: CoreStream enables teams to define themes of interest in natural language — such as forced labour exposure in a specific supply chain, or sanctions risk across a counterparty portfolio — and receive tailored, continuously updated risk insights and narrative summaries as new information enters Kharon's analytic environment.

Users

First line: Sanctions analysts, KYC/due diligence analysts, investigations analysts, supply-chain risk analysts.

Second line: Head of Sanctions, Head of Financial Crime, Trade Compliance Manager, Investigations Lead.

Third line: Chief Compliance Officer, Chief Risk Officer, General Counsel, Global Trade Compliance leadership.

Underlying technologies

- **Knowledge graph intelligence layer:** The Kharon Core is where entities, individuals, vessels, ownership chains, control relationships, trade relationships, and other hidden connections are mapped into a continuously updated graph — the foundation that powers all of Kharon's products and data.
- **Analytic engine and exposure scoring:** A proprietary scoring layer ranks entity exposure to the risk themes Kharon tracks and surfaces the most relevant connection pathways and surfaces risk scores in its platform via Dynamic Exposure Scores.
- **Multilingual open-source data acquisition:** Dedicated research and data operations teams acquire, process, and structure public-domain records across jurisdictions, languages, and source types — publishing only risk-relevant data validated by subject matter experts, not bulk corporate records.

Artificial intelligence

- **AI-assisted data curation:** AI reviews, queries, and prioritises incoming data, helping researchers focus on the most relevant material.
- **AI-enhanced research productivity:** AI tools accelerate analysis of new information and publication of updated networks.
- **Prompt-based insight generation:** CoreStream uses AI to surface network-based insights from user-defined themes and generate narrative summaries grounded in Kharon's verified data.

Top value drivers

- **Reducing screening noise and investigative effort:** More relevant, better-structured risk data reduces time spent on loosely connected or low-value results.
- **Productised, network-based risk intelligence:** Moves beyond flat list screening by mapping ownership, control, and other indirect relationships — delivering structured, explainable intelligence that reveals exposures that would otherwise remain hidden.
- **Driving strategic value from risk:** Transforms risk intelligence into a reusable asset supporting customer enhanced due diligence, supply chain due diligence, export controls, and investment decisions — extending value far beyond core screening.

Case study

Client type
Global industrial technology provider

Challenge
The client's prior data provider generated high-volume, low-confidence results for sanctions and forced-labour due diligence, slowing decisions across a complex supply chain.

Solution
The client integrated Kharon's sanctions-related 50-Plus data and broader risk intelligence into its existing global trade management workflow, supported by Kharon's network visualisation.

Outcome

80%

reduction in review time — detailed reviews cut from 80 hours to 16 hours.

Two-year outlook

Traditional watchlist and screening stacks will face pressure as AI commoditises basic list-building and matching workflows. The differentiator will shift toward curated, explainable risk intelligence — not raw data volume. Firms that treat risk intelligence as a system of record, rather than a point-in-time check, will be better positioned to manage emerging threats and demonstrate compliance to regulators.

Sanctions, export controls, and investment restrictions will converge in practice, requiring institutions to build broader control frameworks than traditional sanctions screening alone can support. Trusted network-based intelligence — connecting ownership, trade, and financial relationships across regulatory domains — will become the operational standard for compliance in an AI-driven environment.

Compliance teams will increasingly use risk intelligence proactively — in past-transaction analysis, portfolio de-risking, and strategic decision-making — rather than only in reactive alert handling. The organisations that embed continuously updated, analyst-validated intelligence into their workflows will define the next generation of compliance infrastructure.

Velocity FinCrime Suite

At the frontier of Fraud Prevention and FRAML

Velocity FSS provides an AML and payment fraud management platform for financial institutions. The company was founded by practitioners who grew frustrated with the systems available to them. Their hands-on background shapes everything from how the product is designed to how the company engages with clients, combining deep subject matter expertise with a clear focus on real-world outcomes.

Founded: 2018 (United States)

Number of employees: 50-200

Regions: United States, Australia, Europe, and the UK

Industries: Financial Services, Gambling & Gaming

Subsectors: Community banks, credit unions, smaller fintechs, MSB-servicing banks, bankers' banks.

Regulatory areas: BSA, AML and Fraud

Website: https://velocityfss.com

Funding: Self-funded

Chief Product Officer: Vineet Mishra (20+ years of experience in FinTech, RegTech, and Financial Crime Compliance)

Customers bet365 NewtekBank CFSB ACBB SuperChoice

Velocity

The Velocity FinCrime Suite is a modular, cloud-based financial crime platform built for financial institutions that need enterprise-grade capabilities without enterprise-grade complexity. It brings together distinct AML and fraud suites within a single environment, underpinned by a proprietary Data Tools layer – including entity and country resolution – that addresses the fragmented, poor-quality data that undermines most compliance programmes at source. AI-assisted investigation and automated workflow tools are designed to help lean compliance teams improve throughput, strengthen auditability, and reduce dependence on multiple point solutions.

Key features

Fraud prevention: a full value-chain approach covering prevention, detection, response, monitoring, rule tuning and sandbox testing. Screening occurs at onboarding and at both ends of every transaction, with behavioural models trained on institution-specific historical data across ACH, wire, cards, check, and identity fraud typologies.

Data remediation and enrichment: resolves fragmented customer and transaction data across banking systems, enriches monitoring with entity resolution, country-risk (scored quarterly for 256 countries) and entity-linkage context.

Workflow management: supports alert triage, assignment, investigation, escalation, and oversight. Provides a single investigation and workflow layer across AML and fraud with integrated dashboards and analytics.

AI-assisted investigation: automatically compiles investigation summaries and supporting evidence for investigations and subsequent suspicious activity reports. Maintains a human role as the final decision maker.

Orchestration Platform: Integrates with core banking systems and third-party solutions (e.g. point solutions for data), acting as a central compliance ecosystem. Partnered with solutions like CLEAR, LNRS and Signzy.

Users

First line: AML investigators

Second line: MLRO, Head of Financial Crime, Head of AML, MLCO

Third line: CCO, Internal Audit

Underlying technologies

- **Clustering and visualisation:** fund flow and structuring, behavioural pattern monitoring, false positive reduction
- **Data ingestion and schema normalisation:** Global data parsers ingest and standardise internal and external data from multiple banking systems, ensuring analysts see a consistent monitoring interface regardless of the original data source.
- **RPA digital workers:** Exception management, automatic data report creation, automatic alert generation, board-level report preparation.

Artificial intelligence

- **Machine learning:** Used in transaction monitoring and fraud detection to identify patterns of suspicious activity, as well as entity and country resolution.
- **Deep learning:** Multi-layer neural networks that learn from historical behaviour and improve fraud detection accuracy over time.
- **Retrieval-augmented generation (RAG):** AI Investigator gathers and summarises key case information to accelerate the work of compliance officers.

Case study

Client type
US-Based Correspondent Bank

Challenge
Operating under a regulatory consent order, the client faced fragmented AML systems, inefficient alert investigation processes, and gaps in customer due diligence and case management, with a strict remediation deadline and significant regulatory, financial, and reputational risk if unmet.

Solution
Velocity deployed its integrated FRAML platform across the client and its network of 350+ respondent banks, combining transaction monitoring, KYC/risk rating, case management, and automated SAR reporting, with data cleansing and normalisation as the foundation.

Outcome

200%

increase in AML program efficiency, alongside a significant reduction in false positives and streamlined regulatory reporting, as the client successfully exited the regulatory consent order within the required timeline.

Top value drivers

- **Enhanced regulatory compliance:** Velocity's primary purpose is to improve regulatory outcomes. It enables institutions to demonstrate effective end-to-end financial crime controls, which have proven value in remediating consent orders and addressing MRA and MRIA findings.
- **Direct revenue generation:** Velocity enables bankers' banks and sponsor banks to offer financial crime monitoring as a managed service to other banks, fintechs, and MSBs, allowing them to generate revenue from compliance infrastructure.
- **Hands-on data transformation:** Velocity addresses a major operational challenge for smaller banks – fragmented, inconsistent data across legacy systems – by integrating and resolving data into a unified monitoring environment that improves visibility, risk analysis, and reporting.

Two-year outlook

The market is evolving toward a platform-plus-ecosystem model. Core systems handle monitoring, case management, and regulatory workflows while integrating specialist tools rather than attempting to build every capability internally.

Agent-based automation will increasingly support financial crime operations, assisting analysts with tasks such as alert triage, data gathering, investigation preparation, and workflow orchestration.

Stablecoin monitoring is expected to become a growing compliance requirement as banks begin supporting digital asset payments alongside fiat transactions, driving demand for monitoring systems that can manage AML and fraud risks across both environments.

Deep Dive: Market Conduct

Subcategories

Trade Surveillance: Tools that monitor trading activity to detect market manipulation, insider trading, and abusive behaviours.

eComms Surveillance: Technologies that capture, store, and analyse electronic communications (e.g. email, chat, voice) to identify potential misconduct.

Communication and Disclosures: Solutions that ensure timely, accurate, and compliant dissemination of market disclosures and investor communications.

Trade Reporting: Technologies that automate the accurate and timely submission of transaction data to regulators and trade repositories.

Vendor Snapshot

150+
products from 80+ providers

100%
of vendors expect financial institutions' related technology spend to increase in 2026

$25m
raised by Market Conduct vendors in 2025, across 5 deals

RegTech adoption

	UK + Europe	North America	APAC	MENA
Core part of control environment	14%	19%	12%	38%
Scaled enterprise use	25%	27%	30%	25%
Functional use in some teams	28%	29%	27%	13%
Pilot/limited use	23%	15%	22%	18%
No meaningful use	10%	10%	10%	8%
Don't know/prefer not to say	-	-	-	-

Market abuse is fundamentally about intent. Proving behaviours such as insider trading or spoofing requires correlating trades with communications, market events, and price movements in context. This kind of multi-modal surveillance, linking structured trading data with unstructured communications and external signals, represents the "holy grail" of maturity, but most institutions have yet to operationalise it.

In many firms, Trade, eComms, and Reporting are managed by three different teams with three different tools. Moving to core control requires an integrated surveillance stack. Many firms lack the internal capability to build this themselves, and while the vendor landscape is evolving, true end-to-end integration remains relatively nascent.

Trends

Key pain points

- **System and control deficiencies:** Regulators are increasingly challenging the effectiveness of surveillance frameworks. Poor threshold calibration and weak governance create either surveillance blind spots or overwhelming alert volumes.
- **eComms recordkeeping:** Firms' recordkeeping frameworks continue to fall short, particularly in capturing off-channel communications. Regulators have issued over $3bn in fines to date.
- **Data governance:** Fragmented architectures, weak validation, and unclear ownership leave firms uncertain whether surveillance is operating on complete and accurate data, undermining the effectiveness of the entire control framework.

Emerging threats

- **Crypto:** As digital assets enter mainstream finance, firms must extend surveillance across on-chain activity, off-chain trading, social media signals, and settlement infrastructure to meet evolving regulatory expectations.
- **Prediction markets:** The rise of prediction markets introduces new forms of tradable instruments, increasing risks of insider trading and market manipulation, while challenging firms' ability to scale surveillance coverage.
- **Cross-product manipulation:** Bad actors are increasingly exploiting relationships across instruments, venues, and asset classes, exposing the limitations of siloed surveillance systems.

38%

of FIs in MENA have implemented RegTech as a core part of their market conduct control environment, double that of North American firms.

Emerging compliance capabilities

- **Integrated trade and eComms:** Unifying trade and communications data to correlate activity with intent, enabling more effective detection of coordinated misconduct.
- **LLM-enabled eComms surveillance:** Moving beyond lexicon-based approaches by leveraging contextual understanding to identify intent in sarcasm, coded language, emojis, and multilingual communications.
- **AI in trade surveillance:** Primarily delivering value in enhancing detection of known abuse patterns, improving alert prioritisation, and reducing false positives, while more advanced use cases such as contextual analysis and copilot-style support remain nascent.*

*https://www.eflowglobal.com/research/global-trends-in-market-abuse-and-trade-surveillance-form

At the frontier of Trade Surveillance

Eventus provides multi-asset trade surveillance and related financial risk technology for capital markets firms and market operators. Its core platform, Validus, was developed by capital markets experts and compliance practitioners for firms dealing with high data volumes, complex market structures and broad regulatory expectations across traditional and digital asset markets.

Founded: 2014 (Austin, Texas, United States)

Number of employees: 51-100

Regions: Global

Industries: Capital Markets / Financial Services

Subsectors: Banks, Broker-dealers and intermediaries, Market venues and digital asset venues, Exchanges and regulators, Prediction/information markets, Proprietary trading firms

Regulatory areas: Trade surveillance, market abuse, risk controls, algo monitoring, market risk

Website: eventus.com

Funding: Private equity (Majority investment from Terminus Capital Partners, 2026)

Co-Founder & COO: Jeff Bell (Three decades of financial markets and technology experience; former CEO of Lime Brokerage and EVP of Clearing & Technology Division at Wedbush, with broad leadership experience across operations, compliance, engineering, client service and regulatory affairs.)

Customers coinbase MAREX FORIS CAPITAL A CRYPTO.COM COMPANY VELOCITY TRADE Webull

Eventus

Validus is a multi-asset trade surveillance platform that combines configurable detection logic, advanced analytics and AI-enabled tooling within a single investigative workflow. It supports the full lifecycle from alert generation through to investigation, escalation and reporting, with flexible data ingestion and normalisation enabling coverage across complex, high-volume trading environments. Built-in automation, visual analytics and natural-language querying tools help surveillance teams prioritise risk and adapt monitoring approaches as market structures evolve.

Key features

Customisable surveillance coverage: 150+ procedures covering market manipulation, risk controls and related surveillance use cases, with adjustable parameters across asset classes

Alert workflow and automation: Users can manage alert status, tagging, escalation and continuity in one place, while built-in automation reduces low-value alert volume

Advanced investigations: Visual tools support analysis of order lifecycle, market context, news and price movement, alongside supporting evidence for flagged activity

Flexible data ingest: Eventus normalises client data from multiple formats and environments, enabling consistent surveillance across high-volume, multi-venue trading activity

Frank AI: A natural-language interface that enables users to query Validus data directly, generating charts, tables and fully auditable, code-backed outputs while lowering reliance on technical resources

Users

First line: Trade surveillance analysts, market conduct analysts, front-office supervisors

Second line: Surveillance managers, compliance managers, heads of market surveillance

Third line: CCO, market oversight leadership, internal audit, regulators / supervisory stakeholders

Underlying technologies

- **Distributed processing architecture:** Supports large-scale data throughput and real-time or near-real-time alert generation in complex trading environments
- **Rules engine with parameterisation layer:** Enables flexible configuration of surveillance logic across asset classes without requiring code changes
- **Integrated data model for market and reference data:** Links trade data, order lifecycle events, market data and external context into a unified analytical framework

Artificial intelligence

- **Machine learning models:** Used for risk-scoring, reducing low-value alerts and focusing analyst reviews
- **Retrieval-augmented generation (Frank):** Converts user prompts into executable queries on underlying trade data, from which it can quickly answer analyst questions
- **Secure query architecture:** Prompts are processed externally, while client data remains within the hosted environment

Case study

Client type
Tier 1 US bank

Challenge
Existing vendors were unable to support RTS 6 (MiFID II) algo monitoring across complex markets and legacy infrastructure

Solution
Eventus deployed a customisable, real-time trade surveillance solution with 12 tailored automations, integrated into existing systems

Outcome

Under 2 months

to full RTS 6 compliance, with improved alert precision, reduced false positives and more efficient monitoring at scale

Top value drivers

- **Modernising legacy surveillance stacks:** Offers firms a route away from aging incumbent systems without sacrificing scale or depth
- **Managing data complexity:** Helps surveillance teams normalise, interrogate and act on complex datasets more efficiently
- **Supporting expansion into new markets:** Gives firms a platform that can extend into new asset classes, venues and market structures without rebuilding surveillance from scratch

Two-year outlook

Prediction markets will become a major frontier for surveillance, with growing focus on event-based contracts, social-driven order flow and sharp activity swings around catalysts.

Blockchain-derived data is likely to become more relevant to mainstream surveillance as tokenisation and digital asset activity continue converging with traditional markets.

AI-enabled analytics will keep advancing, but adoption is likely to be paced by client readiness, explainability and governance requirements rather than model capability alone.

FINGERPRINT

At the frontier of eComms Surveillance

Fingerprint provides a communications supervision platform for regulated firms and compliance service providers. Its product is built around policy-driven monitoring, workflow and reporting, helping firms supervise people-led risk across employee, client, appointed representative and secondee communications in one environment. The platform is particularly well suited to lower to middle market firms, as well as multi-client oversight models where evidencing supervision matters as much as detection.

Founded: 2016 (UK)

Number of employees: 11-50

Regions: UK, Europe, and the US

Industries: Financial Services

Subsectors: Regulatory hosts and principal firms, Compliance consultancies and outsourced CCO providers, Hedge funds, asset managers and newly launched funds, Standalone investment firms

Regulatory areas: Communications recordkeeping and supervision; market conduct and market abuse surveillance; insider risk and information leakage monitoring; conduct risk and non-financial misconduct; marketing and sales communications compliance.

Website: www.fingerprint-supervision.com

Funding: Private / not publicly disclosed

Founder & CEO: James Hogbin (30+ years of experience at the intersection of financial markets and technology, spanning messaging and infrastructure roles at IBM and BT, and systematic asset management at RBS.)

Customers Gresham House Specialist investment · VALEUR · Oakley Capital Investments · REGENTS GATE CAPITAL · SEILERN

Fingerprint

Fingerprint is an end-to-end communications compliance platform that ingests, risk-ranks and organizes communications data across channels into a single supervisory workflow. It supports communications recordkeeping and supervision, market abuse and insider risk review, conduct and culture monitoring, customer treatment oversight, and the evidencing of supervisory activity for audit, due diligence and regulatory review.

Key features

Policy-driven supervision workflows: Monitoring categories, risk terms, KPIs and review tasks are configured against a firm's policy, so activity is aligned to exactly how the business aims to supervise communications.

Cross-channel investigations: Compliance users can review email, chat, voice and collaboration channels in one place, with timelines and case workflows that support investigation, review and sign-off.

Reporting and evidencing: Built-in KPI, activity and supervision reports are designed to show not only that monitoring exists, but that it is being carried out consistently and proportionately.

Multi-tenant oversight: A single environment can support oversight across multiple firms, departments, offices or client books, with role-based visibility where different users only see the data relevant to them.

Network analysis and behavioural scoring: Surfaces patterns such as new joiners, leavers and unusual communication relationships to support prioritisation.

Users

First line: Compliance analysts, monitoring reviewers

Second line: Heads of Compliance, compliance managers, outsourced CCO teams

Third line: CCO, COO, internal audit, risk committee, external due diligence stakeholders

Underlying technologies

- **API-first application layer:** the front end is driven through APIs, which supports integration with broader compliance and GRC environments, allowing communications supervision outputs to feed other workflows and dashboards.
- **Unified communications ingestion and normalization:** pulls email, voice, chat and collaboration data into one searchable investigation layer, so reviewers are not manually switching between archives and channels.

Artificial intelligence

- **Natural language processing and machine learning:** Used to isolate usable email body content from disclaimers, footers and reply chains, improving search quality and review efficiency.
- **Anomaly detection:** Highlights unusual behaviour such as language shifts across conversations or the presence of encrypted attachments and adjusts risk scoring accordingly.
- **AI-assisted policy drafting and tuning:** Generates monitoring categories and terms, and can suggest score adjustments where repeated no-action outcomes indicate policy over-sensitivity.

Case study

Client type
UK regulatory hosting firm, principal oversight of 70+ Appointed Representatives (ARs)

Challenge
A five-person compliance team carried full principal responsibility for 70+ wholesale market AR businesses, each requiring discrete, ring-fenced oversight. Manual processes made proactive supervision impossible at that volume.

Solution
Fingerprint centralised all AR monitoring into one platform, with individual client environments fully segregated. Portfolio-wide risk visibility and structured reporting replaced manual tracking.

Outcome

14

businesses supervised by each compliance analyst, with 100% of ARs monitored proactively. The firm scaled its AR book without adding headcount, turning oversight capacity into a competitive differentiator.

Top value drivers

- **Improving auditability:** Helps firms demonstrate that communications supervision is active, consistent and traceable for operational due diligence, audit and regulator review.
- **Operational efficiency:** Reduces the manual burden of logging into multiple systems, searching archives and assembling evidence after the fact.
- **Broadening conduct oversight:** Extends communications monitoring beyond narrow market abuse use cases into culture, conduct, client treatment and wider people-led risk.

Two-year outlook

Communications supervision will move beyond passive archiving toward continuous, policy-led oversight, where monitoring activities, KPIs and workflows are explicitly tied to regulatory purpose and evidencing requirements. As the market matures, leading firms will go further, using communications data not just to demonstrate compliance, but to generate insight across conduct, culture, and client-facing activity.

Buyers will increasingly expect communications surveillance to integrate with GRC and adjacent conduct tools, rather than operate as a standalone monitoring layer. This will drive partnerships among vendors, increasing their value and adoption.

Deep Dive: Resilience

Subcategories

Enterprise Risk Management: Platforms that enable organisations to identify, assess, monitor, and mitigate risks across the enterprise through risk registers, assessments, controls management, and reporting.

Incident Response: Solutions that detect, manage, and resolve operational and security incidents through alerting, workflow orchestration, investigation tools, and remediation tracking.

Third-party risk: Tools that assess, monitor, and manage risks associated with external vendors and service providers through due diligence, ongoing monitoring, risk scoring, and contract oversight.

AI Governance: Platforms that ensure the responsible and compliant use of artificial intelligence through model oversight, risk assessment, validation, monitoring, and policy enforcement.

Vendor Snapshot

350+
products from 200+ providers

100%
of vendors expect financial institutions' related technology spend to increase in 2026

$797m
raised by Resilience vendors in 2025, across 24 deals

RegTech adoption

	UK + Europe	North America	APAC	MENA
Core part of control environment	7%	16%	10%	20%
Scaled enterprise use	20%	24%	20%	23%
Functional use in some teams	36%	31%	33%	20%
Pilot/limited use	17%	19%	25%	18%
No meaningful use	20%	10%	12%	20%
Don't know/prefer not to say	-	-	-	-

Resilience requires firms to map dependencies across systems, understand third and fourth-party exposure, and achieve real-time breach visibility and incident response. That's not a single tool; it's an orchestration layer. Most firms don't have clean architecture maps tied to critical business services, and many still operate in silos with legacy infrastructure, limiting their ability to industrialise controls.

Resilience is a strong regulatory focus area, particularly in Europe (e.g. DORA, NIS2, CER Directive). The region has the most mature RegTech adoption for IT security, and the lowest for resilience. Although both domains are increasingly integrated within regulatory frameworks, firms have historically prioritised investment in security, where threats are clearer, controls are more defined, and outcomes are easier to measure. Resilience, by comparison, is outcome-based and cross-functional, making it more complex to implement and scale.

Trends

Key pain points

- **Regulatory pressure:** 79% of organizations feel ill-equipped to comply with new operational resilience regulations, and only 20% of executives believe their firms are fully prepared to prevent or respond to outages.* This aligns with the survey's lower reported maturity in the UK and Europe, with heightened regulatory scrutiny exposing gaps in tool sophistication.
- **Incident reporting:** Reporting timelines are compressing significantly, driven by regulatory requirements (e.g. early warning within 24 hours and detailed reporting within 72 hours under NIS2) and heightened stakeholder expectations. Incidents may also need to be disclosed to multiple regulatory bodies, depending on the nature of the breach, the impacted systems, the jurisdictions involved, and whether sensitive data was exposed.
- **Supply chain and "nth-party" fragility:** 84% of third-party incidents result in operational disruption, yet many firms still lack visibility beyond tier 1 suppliers.** Vendor risk management, ecosystem mapping, and scenario testing capabilities remain underdeveloped, constraining firms' ability to anticipate and mitigate cascading failures.

* https://www.cockroachlabs.com/blog/the-state-of-resilience-2025-reveals-the-true-cost-of-downtime/

**Gartner, Annual ERM Survey, 2023

79%

of organizations feel ill-equipped to comply with new operational resilience regulations, and only 20% of executives believe their firms are fully prepared to prevent or respond to outages.

Emerging threats

- **Shadow AI and governance gaps:** Shadow AI is the new shadow cloud. Usage is decentralised. Generative AI isn't limited to data scientists; it's in the hands of employees across the business. Unauthorised or unmanaged AI usage creates blind spots in governance, limiting visibility into data flows, model dependencies, and decision pathways. This lack of transparency weakens an organisation's ability to understand how failures, data leakage, or model errors propagate through systems.
- **"Polycrisis" and interconnected risk:** Organisations are facing a structurally more complex and continuously intensifying risk landscape. Increasing reliance on technology, automation, and the extended enterprise has created deeply interconnected dependencies, where geopolitical, cyber, and AI-related risks can quickly cascade across systems and partners. Disruption has become an inevitability: 35% of firms experience downtime at *least* weekly.*
- **Convergence of physical and digital resilience:** The distinction between IT and operational technology (OT) is eroding as organisations digitise physical infrastructure and embed connectivity across critical operations. Organisations must adopt unified resilience frameworks that account for both physical and digital dependencies.

Emerging compliance capabilities

- **AI-driven continuous compliance mapping and scenario validation:** Generative AI is enabling dynamic alignment between resilience frameworks, regulatory obligations, and operational realities. By combining retrieval-augmented generation with constraint-based reasoning, platforms can continuously map policies to controls, identify compliance gaps, and generate context-specific remediation actions. These capabilities extend into scenario generation, where AI produces tailored stress scenarios and tabletop exercises grounded in actual risk data.
- **External threat intelligence:** Vendors are evolving beyond traditional OSINT aggregation into an intelligence layer that leverages AI to dynamically contextualise external risk signals (news, social media, regulatory developments, and geopolitical events) against internal exposure (third-party dependencies, geographic footprint, and critical services). This ultimately allows firms to actually use external data to better understand material business impacts.**
- **AI-powered observability:** AI-driven observability platforms now analyse telemetry data across infrastructure, applications, and models to detect anomalies, trace root causes, and, in some cases, predict failures before they occur. This is extending to " AI observing AI," with agentic systems monitoring model behaviour, data flows, and decision pathways.***

*New Relic **2025 Observability Report**

****https://signal-ai.com/**

*****https://www.ibm.com/think/insights/observability-trends**

RiskSmart

At the frontier of Enterprise Risk Management

RiskSmart provides a connected risk management platform centred on enterprise risk management, designed for organisations that have outgrown spreadsheets and fragmented workflows or are struggling with legacy, complicated platforms. The platform links risk, control, action and obligation data in one environment, helping firms improve visibility, streamline reporting, and embed risk management more consistently across the business. It is particularly suited to mid-market organisations seeking a more structured, easy-to-use and scalable approach to enable growth.

Founded: 2020 (Manchester, United Kingdom)

Number of employees: 51-200

Regions: UK and Europe focus, with growth in the Middle East and North America

Industries: Financial Services, Legal, Insurance, Utilities, Retail

Subsectors: Banks, fintechs, e-money and payments firms, insurance brokers

Regulatory areas: Enterprise risk management, operational resilience, internal controls and assurance, policy, reporting and board oversight, third-party risk

Website: www.risksmart.com

Funding: Backed by NPIF Maven Equity Finance

Co-founder: Ryan Swann (An accomplished Fintech lawyer and Chief Risk Officer; Built, led and developed in house legal, compliance, risk and regulatory teams.)

Customers Cambridge & Counties Bank Built on understanding · PensionBee · Monavate. · JENSTEN

RiskSmart

RiskSmart is an enterprise risk management platform built around a connected data model that links risks, controls, actions, indicators and obligations in a single system. It enables users to assess and score risk, track control effectiveness, manage actions and workflows, and generate reporting through configurable dashboards and data views. The platform supports automation of key processes such as notifications, approvals and periodic reviews, while allowing users to analyse risk data across multiple dimensions and produce tailored outputs for different stakeholders.

Key features

Connected risk model: Risks, controls, actions, indicators and obligations are linked in one system, helping teams avoid duplicate work and see how issues connect across the business

Smart dashboards and report builder: Users can create and share drag-and-drop dashboards and custom widgets, rather than relying only on fixed, vendor-defined reports

Risk register and scoring workflows: Supports structured assessment of inherent and residual risk, with the option to automate elements of residual scoring based on control performance

Workflow automation: Notifications, approvals, tasking and periodic reviews can be managed within the platform rather than through manual spreadsheet chasing

AI assistance: Current AI use cases focus on drafting and suggesting risks, controls and actions, plus writing support, with an emphasis on supporting human decision making and control

Users

First line: Business risk owners, department heads, control owners

Second line: CRO, CCO, Risk analysts, risk managers, enterprise risk and compliance teams

Third line: Executive committees, audit and risk committee stakeholders

Underlying technologies

- **Configurable relational data model:** Connects risks, controls, actions, policies and related records in one source of truth
- **Robotic process automation:** Automates recurring risk management tasks such as reminders, approvals, scheduled assessments and elements of residual risk scoring based on control effectiveness

Artificial intelligence

- **AI-assisted drafting:** Suggests risks, controls and related content based on the context of the record
- **Prompt-based assistants:** Roadmap features include custom prompts, navigation help and suggested actions for issues and other workflows
- **Accuracy-first AI approach:** Focused on a small number of high-value use cases, prioritising reliability and usability over expansive or experimental deployment

Case study

Client type
FinTech (Comparitec)

Challenge
Comparitec lacked centralised visibility over risk, with processes constrained by limited internal resources and reliance on spreadsheets. This created inefficiencies and made it more difficult to manage compliance effectively.

Solution
Implementation of RiskSmart's Risk & Control and Compliance modules to centralise risk management activities. This enabled greater process consistency and introduced automation across key compliance workflows.

Outcome

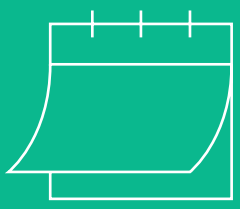
25 hours

saved per month

while simplifying and evidencing compliance to auditors.

Top value drivers

- **Replacing spreadsheets and manual reporting:** Frees risk teams from low-value admin and reduces reporting effort
- **Improving decision support:** Gives management a more connected and forward-looking picture of the business's risk position
- **Strengthening risk culture:** Makes risk ownership more accessible to first-line teams rather than keeping it trapped inside the central risk function



Two-year outlook

Enterprise risk management will become more continuous and dynamic, moving away from static periodic assessments toward more connected, live risk views.

As adoption grows, AI will be recognised as a fundamental threat to operational resilience, forcing firms to move beyond fragmented ownership and clearly define accountability for AI risk across risk, compliance, technology and business functions.

Connected data will matter more as firms try to link risk management, resilience, third-party oversight and AI governance rather than manage them in separate silos.

Deep Dive: Information & Technology Security

Subcategories

Identity and Access Management: Solutions that control user access to systems and data through authentication, authorisation, and lifecycle management.

Network and Endpoint Security: Technologies that protect networks, endpoints, and infrastructure from cyber threats using firewalls, intrusion detection, and endpoint protection tools.

Data Protection: Tools that safeguard data from loss or unauthorised access through encryption, backup and recovery, and monitoring controls.

Data Privacy: Solutions that support compliance with privacy regulations, including consent management, data subject requests, and breach response.

Vendor Snapshot

1500+
products from 500+ providers

83%
of vendors expect financial institutions' related technology spend to increase in 2026

$2.3bn
raised by IT Security Vendors in 2025, across 78 deals

RegTech adoption

	UK + Europe	North America	APAC	MENA
Core part of control environment	26%	17%	12%	20%
Scaled enterprise use	34%	35%	33%	40%
Functional use in some teams	28%	30%	32%	25%
Pilot/limited use	9%	9%	15%	10%
No meaningful use	3%	9%	8%	5%
Don't know/prefer not to say	-	-	-	-

IT Security is now firmly a boardroom priority, supported by one of the most mature vendor ecosystems. With **19%** of firms globally implementing related solutions within core controls and **35%** in scaled enterprise use, it is one of the most industrialised domains in the market, second only to Financial Crime.

UK & Europe maturity **(26% Core / 34% Scaled)** reflects a real shift from security as an "IT problem" to a fundamental compliance control. Regulation, particularly Digital Operational Resilience Act (DORA), has been a key catalyst.

Global maturity is not driven by regulation alone. Cybersecurity benefits from a well-established set of globally recognised frameworks, including NIST Cybersecurity Framework, ISO/IEC 27001, CIS Critical Security Controls, and SOC 2. These have provided both a blueprint for best industry practice and a foundation for vendors to build against, something largely absent in many other risk and compliance domains. As a result, only **6%** of firms report having no meaningful technology in place for IT security, the second lowest across the entire study.

Trends

Key pain points

- **Security lag amid AI-accelerated development:** There is a gap between the speed of software development and security teams' ability to evaluate security. With AI, this gap is widening, effectively turning every employee into a developer, or a significantly more capable one.
- **Expanding attack surface from third parties:** Third-party involvement in breaches has doubled (15%-30%), highlighting growing dependency risks and limited visibility/control over external ecosystems.*
- **Persistent vulnerability exploitation and slow remediation:** Exploitation of vulnerabilities is rapidly increasing (now 20% of breaches), with organisations taking a median of 32 days to remediate and only ~54% fully patched, leaving significant exposure windows.*

*https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

There is a gap between the speed of software development and security teams' ability to evaluate security. With AI, this gap is widening.

Emerging threats

- **Identity and access management for AI Agents:** As organisations adopt AI agents, each function has a new type of identity that requires governance. The challenge is not just the volume of agents but the exponential complexity as they chain permissions or inherit access in unexpected ways.
- **AI-powered cyber risk:** Models trained to be proficient in code are inherently capable in cyber contexts. They are effective at identifying individual bugs, but more importantly, can chain together multiple vulnerabilities. Each vulnerability may pose limited risk in isolation, but models can combine sequences of three to five or more weaknesses to construct exploits that enable highly sophisticated end outcomes.*
- **Uncontrolled data exposure via GenAI usage:** As employees increasingly use GenAI tools in day-to-day workflows, sensitive corporate data is being input into external models without appropriate oversight. The risk is not just leakage, but loss of control over how that data is stored, processed, and potentially reused by third-party systems.

Emerging compliance capabilities

- **Pre-emptive data gating for AI (clean / avoid / remove):** Systematically classifying and controlling which data GenAI systems can access, ensuring only compliant, relevant datasets are used in training and retrieval.
- **End-to-end input transparency and traceability:** Tracking exactly which data sources and content fragments inform AI outputs, enabling auditability, root-cause analysis, and regulatory defensibility.**
- **Continuous AI-driven adversarial testing and remediation validation:** AI-powered red teaming platforms now execute persistent, automated offensive testing. These capabilities continuously identify vulnerabilities, track remediation efforts, and retest environments, generating auditable evidence of risk reduction rather than static compliance outputs.

*https://red.anthropic.com/2026/mythos-preview/

**https://www.parkerlawrence.co.uk/post/snog-marry-avoid-a-modern-data-governance-approach-for-genai-rollouts

Deep Dive: ESG

Subcategories

ESG Ratings: Platforms providing scores or evaluations of companies or financial instruments based on their ESG performance, using transparent methodologies, benchmarking, and industry standards.

ESG Reporting and Disclosures: Technologies supporting the accurate preparation and submission of ESG-related reports and disclosures, aligned with global frameworks and regulatory requirements.

ESG Risk Management: Solutions identifying, evaluating, and mitigating ESG-related risks impacting an organization or investment portfolio, utilizing risk assessments, scenario modeling, and control frameworks.

Climate Risk Quantification: Platforms quantifying financial exposure to climate-related risks, including physical and transition risks, through modeling, scenario analysis, stress testing, and financial impact assessments.

Vendor Snapshot

140+
products from 75+ providers

67%
of vendors expect financial institutions' related technology spend to increase in 2026

$93m
raised by ESG vendors in 2025, across 17 deals

RegTech adoption

	UK + Europe	North America	APAC	MENA
Core part of control environment	7%	7%	17%	10%
Scaled enterprise use	18%	25%	18%	8%
Functional use in some teams	28%	24%	33%	25%
Pilot/limited use	31%	22%	18%	35%
No meaningful use	16%	22%	13%	23%
Don't know/prefer not to say	-	-	-	-

ESG RegTech adoption remains materially lower than other domains, with only **9%** of firms embedding it as a core part of the control environment, reflecting structural challenges rather than simple market immaturity. ESG relies on fragmented, unstructured, and often unverifiable data, spanning global supply chains, carbon estimates, and qualitative metrics. Firms cannot industrialise controls without reliable, standardised inputs.

ESG regulation is relatively young compared to other domains, and regulatory pressure varies significantly across the globe. Technology adoption has, until recently, primarily been driven by stakeholder (customer or investor) pressure. Although Europe is often seen as the regulatory leader for ESG, a surprising **31%** of firms are still in the "Pilot/limited use" phase. It seems that while the laws exist, the technology to implement them at scale is still being tested, creating a significant opportunity for RegTech providers who can solve the data-verification puzzle.

Trends

Key pain points

- **Data fragmentation and value-chain opacity:** Organisations still struggle to obtain consistent, decision-grade ESG data across internal systems and third parties. Data availability, quality, and supply chain complexity remain the primary blockers to CSRD/ESRS readiness, compounded by the fact that supply-chain emissions can be ~26x larger than operational emissions.*
- **Regulatory fragmentation:** ESG compliance is driven by overlapping regimes (ESRS, ISSB, California laws, ratings methodologies, anti-greenwashing rules). Regulatory delays (e.g. EU stop-the-clock) are increasing divergence rather than reducing workload.
- **Weak linkage between ESG signals and operational risk:** Most organisations remain disclosure-focused rather than risk-focused. While ESG reporting alignment is improving, only a small minority conducts robust scenario analysis or risk exposure.

*https://www.bcg.com/press/25june2024-corporates-supply-chain-scope-3-emissions-higher-than-operational-emissions

Data centre demand is rising globally, creating a trade-off between productivity gains and sustainability impact.

Emerging threats

- **AI as both ESG enabler and sustainability burden:** Data centre demand is rising globally, creating a trade-off between productivity gains and sustainability impact. ESG teams must now track AI-related energy usage, procurement, and governance as part of their remit.
- **Ratings and scoring divergence creating market risk:** ESG ratings remain inconsistent across providers, with materially different scores driven by opaque methodologies. As regulation begins to formalise oversight (e.g. in the EU and UK), firms face a dual risk: (1) being penalised by markets or investors due to unfavourable ratings they cannot easily challenge, and (2) being required to explain and reconcile differences across multiple scoring frameworks.
- **Nature and biodiversity risk moving into scope:** Nature-related risks (biodiversity loss, water stress, ecosystem dependency) are entering regulatory and investor focus. These risks are harder to quantify, more location-specific, and less supported by mature data infrastructure.

Emerging compliance capabilities

- **Unified data layers for multi-framework reporting:** Moving towards a single, governed ESG data layer that can support multiple frameworks (ESRS, ISSB, California, questionnaires) from one source of truth. This disclosure graph approach enables reuse, consistency, and scalability as reporting requirements evolve.
- **Assurance-by-design architectures:** Embedding auditability directly into workflows, including data lineage, controls, approvals, and evidence management. This aligns with emerging assurance standards (e.g. ISSA 5000) and regulatory expectations for financial-grade supervision of ESG disclosures.
- **Decision-grade ESG risk intelligence with controlled AI:** Integrating ESG data with scenario analysis, geospatial risk modelling, and financial impact assessment. AI is being deployed selectively to validate data, identify exposures, and accelerate evidence collection under human oversight.

RegTech Market Map

Note: This market map is not a complete representation of the RegTech vendor landscape. It captures only ~10% of the vendors in our database and only includes vendors once, in what we deem their *primary* category. In reality, many of these vendors have multiple products spanning multiple regulatory domains.

* The underlying taxonomy for this report includes AI Governance within Resilience, alongside other subcategories such as Enterprise Risk Management, reflecting the broader and wider-reaching impacts of AI across modern organizations.

Appendix

Financial Institution Survey Demographics

Region

Country					
UK	France	US	Australia	Singapore	UAE
20%	13.33%	33.33%	10%	10%	13.33%

Company Subsector

Financial Subsectors					
FinTech (inc. Crypto)	Retail Banking	Investment Banking	Payments	Asset Management	Insurance
23.67%	35%	29.67%	29.67%	21.67%	23.33%

Company Size

No. Of Employees						
50 - 249	250 - 499	500 - 999	1,000 - 4,999	5,000 - 9,999	10,000 - 19,999	20,000 +
15.33%	18.33%	20.33%	23%	15.67%	6%	1.33%

Job Titles

Job Title						
Chief Compliance Officers	Director/VP of Compliance	Head of Compliance	Compliance Manager or Compliance Specialist	Chief Risk Officer	Chief Information Security Officer (CISO)	Head of Financial Crime/MLRO (Money Laundering Reporting Officer)
13.67%	14.33%	15.67%	16.33%	13.33%	13.33%	13.33%

RegTech Vendor Survey Demographics

Region

Country (HQ)							
United Kingdom	United States	Australia	Germany	Belgium	France	Singapore	Other (14 countries)
33.80%	26.76%	4.23%	4.23%	2.82%	2.82%	2.82%	22.54%

Company Size

No. Employees		
Under 50	50-249	250+
63.38%	28.17%	8.45%

About This Research

The Global State of RegTech is a new annual research initiative by Parker & Lawrence Research and RegTech Analyst.

The Global State of RegTech is a new annual research initiative by Parker & Lawrence Research and RegTech Analyst, as part of a shared mission to support compliant and efficient financial services markets through the adoption of technology. The research explores the evolving role of RegTech across risk and compliance domains and their underlying use cases, bringing together all sides of the market through greater awareness and deeper understanding.

About Parker & Lawrence Research

Parker & Lawrence Research is a market research firm focused on AI, risk and compliance. It supports the responsible adoption of emerging technologies by delivering market intelligence that informs the decisions of senior risk and compliance professionals. The team has tracked the RegTech market since 2017, developing proprietary taxonomies, databases and methodologies. During this time, it has worked across the market, supporting global regulators with technology strategy and market intelligence, advising financial institutions on gap analysis and vendor selection, and producing thought leadership with technology vendors.

About RegTech Analyst

RegTech Analyst is the world's leading provider of RegTech information services, B2B media products and industry events. The company informs, connects and advances a network of over 60,000 compliance professionals from financial institutions, technology innovators, investors, and advisory firms. From breaking market intelligence and deep-dive analysis to world-class industry events, RegTech Analyst gives the people shaping the future of financial compliance the information, relationships and analysis they need to move faster and make better decisions.

Acknowledgements

A special thanks to the experts who contributed their perspective and feedback on the themes contained in this report:

Sholthana Begum - Senior Director, Technology and Digital Intelligence at Competition and Markets Authority

Kelly Letsiou - Financial Crime and Technology at Baringa

Parker & Lawrence
Research

REGTECH ANALYST

Contact

Mariyan Dimitrov, Head of Business Operations, FinTech Global
mdimitrov@fintech.global

Michael Lawrence, Co-founder, Parker & Lawrence Research
michael@parkerlawrence.co.uk

Nathan Parker, Co-founder, Parker & Lawrence Research
nathan@parkerlawrence.co.uk