UNIVERSITY OF CAMBRIDGE Judge Business School | Cambridge Centre for Alternative Finance

CAMBRIDGE SUPTECH LAB

IN COLLABORATION WITH

DIGITAL TRANSFORMATION SOLUTIONS

State of SupTech Report 2025

4th Edition

WITH SUPPORT FROM

Gates Foundation

PARTNERS & CONTRIBUTORS

abhi
ACBF
ADB
ASBA
ASSAL
CCSBSO
DeNederlandscheBank EUROSYSTEEM
Ecomonitor
EU Supervisory Digital Finance Academy
EUI
FCA
Nasdaq
Superintendencia Financiera de Colombia
Reserve Bank of India

About the State of SupTech Report 2025

The State of SupTech Report 2025 provides an updated, critical view of how financial supervisory authorities are navigating digital transformation in an environment shaped by AI, cloud, data-driven finance, and rising expectations of public accountability. It examines how supervisors are redefining their mandates and operating models as financial systems become more technology-intensive, interconnected, and exposed to new forms of risk and misconduct.

As a collaborative resource for the global ecosystem, the report offers evidence and comparative intelligence to help align efforts, identify systemic gaps, and understand recurring challenges and emerging practice. It is designed to support supervisors, policymakers, providers, and partners in advancing a more coherent and outcome-driven approach to suptech and related data and technology investments.

By engaging with the findings, stakeholders can work together to accelerate the adoption of suptech applications and realise their potential to modernise supervisory practices, strengthen market integrity, and support transparency, inclusion, sustainability, and resilience across economies.

The responsible use of technology in financial supervision is now central to maintaining trust in both financial systems and the public institutions that oversee them. When financial authorities apply technology with fairness, accountability, and citizen-centric governance, they do more than improve risk detection or operational efficiency — they reinforce democratic values, enhance the robustness of financial systems, and bolster confidence in the public institutions that safeguard societies.

This year's edition is also connected to GovSpace, the digital platform developed by Digital Transformation Solutions (DTS) and prototyped through the Cambridge SupTech Lab. Through GovSpace, agencies can explore interactive benchmarks, compare their journeys with peers, access curated resources and case studies through dedicated Spaces, and participate in an ongoing, practice-driven conversation that supports continuous improvement, institutional capacity building, and more effective deployment of suptech and adjacent govtech solutions.

How to use this report

- Identify your baseline and compare it with peers using survey results and benchmarks.
- Explore case studies, examples, and thematic deep dives to guide decision-making.
- Use insights as inputs for strategic planning, capability development, and technology investment.
- Refer to GovSpace Spaces for additional resources, tools, and follow-on discussions.

Engage on GovSpace

- Access the State of SupTech 2025 Space for supporting materials and to download the charts.
- Join topic-based communities to exchange experiences with peers.
- View interactive dashboards and explore your agency's diagnostic insights in the Digital Twin.
- Receive updates on emerging practices, datasets, and implementation guidance.

GOVSPACE
powered by
DIGITAL TRANSFORMATION SOLUTIONS

Practical Data Science for Financial Supervision
Digital Transformation Solutions Training

Scan to learn more

Suggest Citation

Cambridge SupTech Lab and Digital Transformation Solutions (2025), State of SupTech Report 2025, Cambridge: University of Cambridge Center for Alternative Finance (CCAF) and Digital Transformation Solutions (DTS).

Available at www.cambridgesuptechlab.org/SOS.

The mention of specific companies, manufacturers or software does not imply that they are endorsed or recommended by the Cambridge Suptech Lab in preference to others of a similar nature that are not mentioned.

Authors

Maryeliza Barasa
Insights Manager,
Digital Transformation Solutions

Simone di Castri
CEO, Digital Transformation Solutions, and
Co-Head, Cambridge SupTech Lab

Matt Grasser
CTO, Digital Transformation Solutions, and
Co-Head, Cambridge SupTech Lab

Design

Emily Duong

Contents

Acknowledgments

The Cambridge SupTech Lab and Digital Transformation Solutions team extends its deepest gratitude to the colleagues from the 148 financial authorities who participated in this year’s survey.

We also wish to thank our partners who contributed to bringing this year’s report fruition, with special acknowledgement to: Hernán Colmán and María José Baqueiro (Association of Supervisors of Banks of the Americas), Olga Salashina and Carlos Javier Chaparro (Association of Insurance Supervisors of Latin America), Karina Velásquez (CCSBSO), Lisette Cipriano (Asian Development Bank), Nico Lauridsen (European University Institute & EU Supervisory Digital Finance Academy), and Rodolphe Bance (The African Capacity Building Foundation). These technical partners were instrumental in extending the survey’s reach, enabling us to gather one of the most comprehensive and diverse datasets on suptech from financial authorities to date.

We are also grateful to Ruben ten Berge, Sebastian Kavelin, and Friso van der Meyden (De Nederlandsche Bank), Ejaz Anwer, Ahmad Butt, and Burat Ahmed (Abhi), Dr. Jugnu Ansari, Geetha Giddi, and Vijay Singh Shekhawat (Reserve Bank of India), Fatima Abukar, Steve Hall, Zac Lovell, and Sid Samant (UK Financial Conduct Authority), Tatiana Lorena Chaparro Pineda, Mauricio Chaparro Benavides, and Francisco Javier Duque Sandoval (Financial Superintendency of Colombia), Min-Si Wang and Marios Kargarlis (Ecomonitor), and Ed Probst (Nasdaq) for their valuable contributions to the case studies included in the report.

In addition to the authors, several colleagues at the Cambridge SupTech Lab contributed to the questionnaire design, dataset analysis, case study research, and content review, including Elia Resch, Kyriakos Christofi, Wenbin Wu, Samir Kiuhan-Vásquez, Kalliopi Letsiou, and Lara Sousa Faria. Their support has been invaluable in shaping the final report.

Thank you all for making this year’s edition possible.

Executive Summary

The **State of SupTech Report 2025** offers a comprehensive global analysis of supervisory technology (suptech), examining its adoption across key dimensions: the supervisory use cases it enables, the blockers and enablers linked to digital infrastructure and underlying technologies, and the change-management processes shaping agencies' digital transformation journeys. It also reviews the approaches and strategies supervisory authorities use to develop and deploy suptech applications, along with the practical challenges and risks they face. In addition, the report presents both year-over-year (YOY) comparisons and a longitudinal view grounded in data from the State of SupTech Surveys conducted in 2022, 2023, 2024, and 2025.

This edition is built on a robust four-year dataset, drawing insights from **312 financial authorities across 172 countries and six continents.** In 2025 alone, **148 authorities from 105 countries** contributed to the survey, providing an exceptionally global and time-consistent perspective on how suptech is evolving worldwide.

Respondents represent the full spectrum of financial-sector public institutions — including central banks, securities and capital-market regulators, conduct authorities, pension and insurance supervisors, and other regulatory and supervisory bodies. This breadth ensures a holistic understanding of how suptech is reshaping financial oversight across jurisdictions.

The analysis is further strengthened by data from **GovSpace** Discover, the dynamic and AI-powered intelligence hub that maps suptech and govtech providers, code, solutions, and real-world applications across the globe.

Highlights From the State of SupTech Report 2025

SupTech Adoption and Strategic Development

- **Global suptech adoption accelerates.** The number of authorities with operational suptech deployments (Generation 2–4) has more than tripled since 2022, reaching 197 agencies across 140 countries in 2025, demonstrating the growing centrality of digital tools in contemporary financial supervision.
- **Persistent maturity divide.** Surveyed financial authorities in advanced economies show much deeper deployment (43% operate over ten applications) compared to their peers in emerging markets and developing economies (EMDEs) (only 11% operate over ten applications), underscoring a global capability gap shaped by strategy and governance, skills, infrastructure, and budget constraints.
- **Suptech activity rebalances across supervisory domains.** The 2025 data show a landscape confident in advanced supervisory technologies for traditional areas, while also expanding and experimenting into high-risk, rapidly evolving domains. AML/CFT/CPF leads at 53%, followed closely by licensing and authorisations (52%) and consumer protection (51%), while prudential supervision declined from 66% in 2022 to 48%, with signals of maturation in emerging areas including AI oversight (37%), digital assets (29%), and climate risks (28%).
- **Suptech value realized.** 18% of agencies rate their suptech applications as very effective, and large number classify them as moderately (33.5%) or somewhat effective (34%). The primary value is consistently realised through improving internal supervisory performance (e.g., time savings, data integration, and analytical accuracy). The perceived effectiveness for external supervisory outcomes, such as influencing regulated-entity behaviour or enabling real-time supervision, remains demonstrably lower.

Technologies and the Data Journey

- **Steady mordenisation continues.** Supervisory authorities are currently pursuing steady, deliberate modernisation, and still rely on foundational tools, even though they express strong demand for advanced analytics and AI. Adoption remains cautious and deliberate, prioritising data quality, infrastructure, and governance, yet the sharp gap between current use and ambition for capabilities such as predictive analytics, advanced BI, and generative AI underscores a sector poised for transformation once core enablers are in place.
- **AI (including GenAI) is reshaping financial supervision, but maturity remains low.** AI is rapidly enhancing supervisory capabilities, from large-scale text analysis and predictive modelling (each used by 23% of authorities) to automated reporting (17%) and enhancing real-time decision making (11%). Yet maturity remains limited, 26% of agencies in initial exploration stages, and only 7% reporting widespread or fully integrated deployment. Advanced economies are significantly ahead, with 24% reporting widespread deployment compared with less than 1% in EMDEs.
- **Key AI adoption barriers shift to trust and human factors.** The principal constraint on the use of AI by supervisory authorities is consistently data protection, privacy, and security concerns (30%), but the overall barrier landscape has shifted from initial technical issues to operational and human factors. This is evidenced by the prominence of staff skills and employment issues (22%) and technical integration barriers (20%), deficits that pose greater hurdles than computational limitations.

Enablers and Challenges

- **Uneven but advancing strategic planning.** Strategic planning for digital transformation, data governance, suptech, and AI is progressing, but frameworks remain uneven and only partially integrated. While operational and technical elements are prioritised, cross-framework alignment, governance, and sequencing are limited.
- **Strategies enable sustained innovation.** Authorities with coherent strategies report smoother implementation, higher data quality, and broader suptech deployment, highlighting the link between integrated planning and effective supervisory innovation. Advanced economies show higher maturity, while EMDEs demonstrate strong intent but slower institutionalisation.
- **Suptech adoption continues to encounter significant obstacles, though financial authorities are taking active measures to overcome them.** Progress in design is primarily constrained by poor data quality (49%), shortages of specialised talent (43%), and lengthy production cycles (42%), while implementation efforts are further hindered by resource-intensive deployment (52%), cost-related pressures (43%), and limited internal IT capacity (40%). More than one-third of the authorities report having no dedicated budget for suptech or digital transformation (36%), and this challenge

is even more acute for advanced technologies, with nearly two-thirds lacking explicit budgets for AI and GenAI (63%). To narrow capability gaps, most authorities are investing in external (66%) and internal (61%) training and strengthening cooperation through bilateral partnerships (62%) and peer-learning forums (61%).

- **Suptech procurement remains formal, structured, and cautiously innovative.** Financial authorities overwhelmingly rely on traditional procurement including Requests for Proposal (60%) and tenders (45%), reinforced by cross-departmental evaluation committees (57%). Innovation methods such as tech sprints (29%) and regulatory sandboxes (30%) are used but remain secondary. Advanced economies pair formal procurement with higher innovation uptake (tech sprints 57%), while EMDEs depend more heavily on RFPs (61%), underscoring differing innovation capacities.
- **Internal teams drive suptech, with targeted external support.** In 2025, suptech development is led by internal teams - IT departments (60%), business units (44%) - while vendors (44%) and consultants (35%) provide specialised support. Advanced economies rely more on internal resources and consultants, whereas EMDEs balance internal IT (56%) with vendors (44%) and greater use of donor-funded programmes (23% vs. 7% in AEs).

Foreword

From Michael Hsu, Past Acting Controller of the Currency, U.S. Office of the Comptroller of the Currency, Fellow, Aspen Institute, and Chair of the Advisory Board, Digital Transformation Solutions

Financial supervision has always had to adapt and evolve. Today, though, the pace and complexity of change – driven by artificial intelligence, shifting market structures, and the digitization of financial services – is pushing supervisors to fundamentally rethink how they operate.

The State of SupTech Report 2025 arrives at a critical time. As supervisors worldwide confront the twin challenges of rapid technological advancement and resource constraints, this report provides an evidence-based picture of where we stand and what lies ahead. It is both a benchmark and a roadmap.

This year's edition reflects the expanding scope of supervisory responsibilities. The report includes a substantially expanded section on strategies — examining how authorities are moving from isolated pilots to coherent, institution-wide approaches to technology adoption. Readers will also find new sections addressing some of the most pressing frontiers in supervision: AI oversight, open banking and open finance, and operational risks. Additionally, the report introduces new analysis on gender data in financial inclusion, an area where better measurement can drive better outcomes.

I am particularly encouraged by the report's strengthened treatment of data governance. Sound data architecture is the foundation upon which all supervisory technology rests. The expanded discussion of ISO 20022 underscores how structured, interoperable financial messaging directly strengthens supervisory capacity, enabling real-time monitoring, pattern recognition, and cross-border coordination that enhance our ability to detect misconduct and emerging risks.

While suptech adoption has been accelerating, meaningful gaps persist: between advanced and emerging economies, between strategy and execution, and between technological capability and institutional readiness. Closing these gaps will require sustained investment, global cooperation, and a willingness to learn from peers.

I commend the Cambridge SupTech Lab and Digital Transformation Solutions for their continued leadership in this space. They have helped build the shared vocabulary and collaborative networks that supervisors need to succeed. In a world where financial risks increasingly cross borders and sectors, that kind of collective intelligence is indispensable.

The responsible application of technology in financial supervision is ultimately about trust — trust that markets are fair, institutions sound, and public authorities equipped to fulfil their mandates. This report helps advance that trust by showing what is possible when supervisors embrace innovation with rigor and purpose.

About Cambridge SupTech Lab

The Cambridge SupTech Lab accelerates the digital transformation of financial supervision to foster resilient, transparent, accountable, sustainable, and inclusive financial sectors.

The Lab catalyses the integration of innovative technologies and data science into supervisory processes to address enduring and emerging challenges in the rapidly evolving financial landscape. Through the Lab, financial authorities have championed the adoption of advanced suptech solutions to address pressing issues such as financial crime, fraud, exclusion, climate change enablers, consumer protection, artificial intelligence biases, and the supervision of fintech and digital assets.

Our global, multidisciplinary team partners with financial authorities' executives, supervisors, and data scientists to craft solutions across the entire innovation lifecycle — from data governance to AI-powered strategies, from the initial design to the full-scale deployment and scaling of cutting-edge suptech applications.

The Lab is implemented by the Cambridge Centre for Alternative Finance (CCAF) in collaboration with Digital Transformation Solutions (DTS), and supported by Fii.

We invite you to find out more at:

🌐 www.cambridgesuptechlab.org

Cambridge SupTech Lab

Introduction

Reimagining financial supervision in the age of intelligent technology

The State of SupTech Report 2025 takes stock of how financial supervisory authorities are progressing on their digital transformation journeys in a year when artificial intelligence, cloud, data-intensive finance, modern messaging standards (including ISO 20022), and digital public infrastructure have moved to the core of financial regulation and supervision. It examines four interrelated questions that now define the trajectory of modern supervision:

1. How far authorities have moved from pilots and isolated experiments to institutionalised, system-wide use of data and technology;
2. How these capabilities are being deployed in practice;
3. What effectiveness they are achieving across supervisory outcomes; and
4. What structural, organisational, and environmental barriers continue to constrain progress.

Building on a growing longitudinal dataset of 312 financial authorities across regions and income groups, this edition provides a structured, data-driven view of trends, gaps, and emerging practice in the digital transformation of financial supervision. It enables authorities to benchmark themselves against peers, understand which combinations of organisational choices and investments are associated with measurable results, and identify where progress is slowing or stalled. Participating agencies can use these insights — including tailored benchmark views — to prioritise the capabilities, processes, and partnerships that matter most for their context.

Reflecting the evolution of supervisory mandates, the 2025 edition expands the SupTech Taxonomy to incorporate three emerging areas of supervisory focus: Oversight of AI use by regulated firms, open banking and open finance supervision, and operational risks supervision.

Ultimately, the State of SupTech Report 2025 reaffirms a clear message: suptech is no longer a peripheral experiment but a core pillar — and enabler — of modern financial supervision.

From experimentation to institutionalisation

Since the inaugural State of SupTech Report in 2022, financial authorities worldwide have progressed from early experimentation to more systematic implementation of digital supervisory applications. As highlighted in the 2024 edition, the suptech movement has reached a clear inflection point: a shift from isolated pilots to more institutionalised adoption across both advanced and emerging-market jurisdictions, closely correlated with the rise of formal digital and data strategies within supervisory agencies. Building on those insights, the 2025 edition provides the most comprehensive global view yet of how suptech is reshaping financial oversight.

This transformation is occurring against a backdrop of profound structural change. Supervisors are not merely adapting to innovation; they are helping shape a new financial order defined by digital assets, tokenised deposits, programmable money, distributed ledger technologies, and highly interoperable data ecosystems. In this context, suptech stands at the centre of system-wide adaptation. Through advanced analytics, natural-language processing, and predictive modelling, it enhances authorities' capacity to detect vulnerabilities, enforce compliance, and preserve financial stability.

Yet building a future-ready supervisory system demands more than technology. It requires global coordination, sound governance, effective change management, strong data foundations, modernised operational processes, and sustained investment in skills and organisational capabilities — all anchored in a shared commitment to trust, accountability, transparency, and inclusion.

Global momentum among international standard-setters and financial institutions

In parallel with national efforts, 2025 marked a significant acceleration in suptech leadership from global institutions. The Bank for International Settlements (BIS) Innovation Hub announced a renewed work programme emphasising AI-enabled supervision, data architectures, and digital public infrastructures, signalling that supervisory technology has moved firmly into the mainstream of central banking innovation.

The International Monetary Fund (IMF) published AI Projects in Financial Supervisory Authorities: A Strategic Toolkit (2025), offering one of the first comprehensive methodologies for safe, effective, and governance-aligned adoption of AI in supervisory agencies. The Fund also warned that uneven adoption could create "tiered supervision," in which digital and analytical disparities widen gaps between jurisdictions. The IMF's Toolkit reinforces many of the principles embedded in the methodological approach of the State of SupTech report. Its emphasis on governance, data readiness, multidisciplinary teams, and iterative development mirrors the frameworks used in GovSpace Strategize.

A transformed supervisory environment

Insights in this subsection draw in part on Starling's Supervisors on Supervision report.

The supervisory environment entering 2025 is considerably more complex than in previous years. Supervisory leaders emphasise five structural realities that now frame their work:

- **Resilience under uncertainty** — geopolitical fragmentation, macro-financial volatility, and increasingly frequent cyber and operational disruptions require supervisory agility and rapid escalation mechanisms.
- **Data-centric supervision** — high-frequency, high-granularity data is now essential for timely detection, forward-looking analysis, and effective intervention.
- **Cross-border coordination** — financial activity, data flows, and third-party dependencies are global; supervisory responses must be as well.
- **Workforce transformation** — demand is rising for hybrid skills in engineering, analytics, behavioural insight, and AI validation, with institutional culture emerging as a decisive enabler of adoption.
- **Expansion of the supervisory perimeter** — supervisors must now oversee AI-driven decisioning models, BigTech infrastructure, digital service providers, and complex outsourcing chains.

These insights, underscored by supervisory leaders globally, reinforce that the challenges facing authorities are no longer episodic or localised; they are systemic, continuous, and increasingly intertwined.

Foundational shifts in supervisory data architecture

The shift toward AI-enabled supervision places new emphasis on AI-readiness – the extent to which supervisory datasets possess the structure, granularity, metadata richness, and interoperability required for machine-learning models to function reliably at scale. Suptech adoption is increasingly constrained or enabled by this underlying data architecture. Global moves toward structured messaging standards, machine-readable reporting, and privacy-preserving data-sharing are therefore foundational to the next stage of supervisory transformation.

A central driver of this shift is the global migration to ISO 20022, the structured messaging standard now used across major payment systems, including TARGET2 (ECB), CHAPS (Bank of England), and the Fedwire (Federal Reserve) transition. ISO 20022 replaces legacy free-text formats with highly structured, machine-readable fields – such as detailed party identifiers, purpose codes, and transaction metadata – creating datasets that are more consistent, interoperable, and analytically valuable. For supervisors, this standardisation supports automated data ingestion, anomaly detection, behavioural analytics, and network-based systemic-risk assessments drawn directly from high-frequency transaction flows.

Parallel advances in API-based reporting architectures are reshaping how supervisors access, validate, and process firm-level data. Instead of batch submissions in static templates, APIs enable continuous, event-driven, or request-response reporting, improving timeliness, reducing manual validation, and allowing supervisors to query specific data objects at the required granularity. Several authorities – including the BOE, Bank of Lithuania, and the Australian Prudential Regulation Authority (APRA) – are now exploring or piloting machine-readable reporting frameworks that link legal obligations to data models and technical specifications, enabling end-to-end automation from regulatory text to data submission.

At the same time, privacy-enhancing technologies (PETs) and secure cloud environments are becoming integral to supervisory architecture. Homomorphic encryption, secure multiparty computation, and federated learning increasingly allow authorities to analyse sensitive datasets without requiring centralised access. This is particularly relevant for cross-border supervision, where legal and confidentiality constraints traditionally limit data mobility. PET-enabled designs feature prominently in global innovation initiatives, including the BIS Innovation Hub's Project Aurora (financial crime analytics) and Project Aperta (consent-based, privacy-preserving data sharing for open finance).

Developments in instant account-to-account (A2A) payment systems also carry supervisory implications. Platforms such as Brazil's Pix, India's UPI, and the European Union's emerging SEPA Instant framework generate high-volume, structured, real-time data useful for liquidity monitoring, fraud detection, and behavioural analysis. As A2A systems expand into programmable payments and merchant use cases, supervisors face increasing overlap between payment-system oversight, open-finance data governance, and broader market-conduct supervision.

Despite these advances, two persistent structural constraints limit supervisors' ability to fully leverage modern data architectures. Cross-border data flows remain hindered by localisation requirements, confidentiality provisions, and inconsistent regulatory gateways, restricting supervisors' capacity to monitor global risks despite increasingly interconnected financial activity. Fragmented internal data landscapes also pose material barriers: many authorities continue to operate legacy databases without common identifiers, taxonomies, or ontologies, making integrated analytics difficult even when external reporting standards are improving.

These developments collectively represent a decisive shift in the supervisory data environment. Supervisors now operate within infrastructures capable of delivering higher-frequency, higher-granularity, and more interoperable data flows – an essential foundation for automated controls, AI-enabled analytics, early-warning systems, and more adaptive forms of supervision. Yet realising these benefits will require sustained investment in governance, interoperability, and organisational capability to ensure that data architecture becomes an enabler rather than a constraint.

A complex and mounting risk landscape

The State of SupTech Report 2025 emerges at a time when the global financial markets appear relatively stable amid ongoing trade tensions and geopolitical uncertainty. Yet, the International Monetary Fund's October 2025 Global Financial Stability Report cautions that beneath this apparent calm lies 'shifting ground', with stretched asset valuations, rising sovereign debt pressures, and complex interconnections between banks and non-bank financial institutions (NBFIs) that could exacerbate vulnerabilities if left unaddressed.

The World Economic Forum's Global Risks Report 2025 similarly underscores the convergence of geopolitical fragmentation, technological disruption, and macro-financial instability as defining pressures on public institutions. Structural forces such as technological acceleration, demographic shifts, climate risks, and geostrategic fragmentation continue their inexorable march, creating an environment characterised by heightened uncertainty, eroding trust, and persistent vulnerability.

The 2025 edition of the State of SupTech Report sits within this broader context. These pressures demand stronger surveillance capabilities and more adaptive oversight frameworks. To safeguard financial stability, policymakers and supervisors need to strengthen stress testing, enhance scenario analysis, and improve their ability to assess interactions between emerging risks. In this environment, resilience and effective risk management are essential for both financial institutions and the authorities that oversee them.

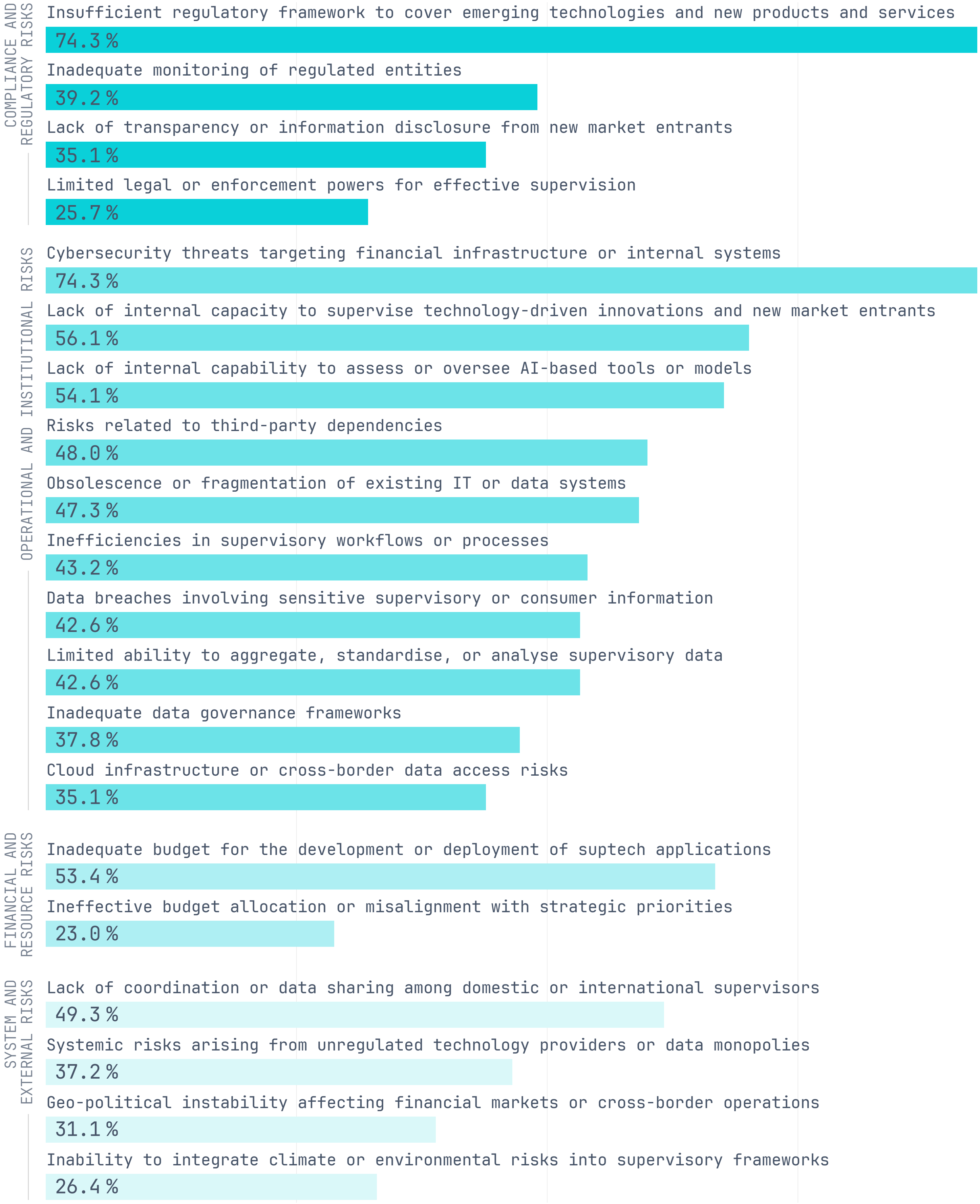
Survey responses for 2025 confirm that the supervisory risk environment has intensified (Figure 1). Authorities identify insufficient regulatory frameworks for emerging technologies and cybersecurity threats as their most pressing concerns, each cited by 74% of respondents. Operational capacity constraints remain acute: 56% report limited internal capacity to supervise technology-driven innovations, while 54% indicate insufficient capability to assess or oversee AI-based tools and models. Authorities also highlight third-party dependencies (48%), outdated or fragmented IT infrastructure (47%), and persistent weaknesses in data governance (38%) — including limited ability to aggregate or standardise data (43%), data breach risks (43%), and cloud or cross-border data access concerns (35%).

Resource limitations and systemic pressures compound these challenges. Inadequate budget for suptech development is noted by over half of respondents (53%), and lack of coordination or data sharing among domestic supervisors remains a significant friction point (49%). Systemic risks arising from unregulated technology providers are reported by 37%, while geopolitical instability affecting financial markets or cross-border operations concerns 31% of responding agencies.

Risk priorities diverge sharply across income groups and regions. Advanced economies emphasise cybersecurity threats (68%), insufficient regulatory frameworks for emerging technologies (54%), and operational vulnerabilities relating to data breaches, third-party dependencies, cloud infrastructure,

FIGURE 1.

Risks Identified by Financial Authorities



and technology obsolescence (each around 50%). AEs also express greater concern about geopolitical instability (43% versus 28% in EMDEs), reflecting their deeper exposure to cross-border interdependencies and critical infrastructure risk (Figure 2).

Emerging-market and developing economies face consistently higher pressures across almost all categories. Their leading risks include insufficient regulatory frameworks (80%), cybersecurity threats (76%), and inadequate budgets for suptech development (59%). Capacity gaps are more acute: EMDEs report significantly greater difficulty in assessing AI/ML models (59% versus 32% in AEs) and highlight persistent weaknesses in domestic data-sharing mechanisms. Financial constraints are also more pronounced (59% versus 36%), underscoring the need for targeted technical and financial support to prevent widening disparities in supervisory capability.

Beyond the common concerns of cybersecurity and insufficient regulatory frameworks, distinct risks emerge across regions, highlighting specific operational, financial, and institutional vulnerabilities. EAP and SSA face major gaps in supervisory capacity for technology driven innovations, and some of the most acute financial constraints. LAC and South Asia similarly face broad operational weaknesses, including limited capability to oversee AI-based tools and inadequate internal capacity to supervise tech-driven innovations. ECA contends with legacy systems, third-party dependencies, data breaches and cloud-related risks, while NA highlights data breaches, workflow inefficiencies, financial pressures and exposure to geopolitical instability. The MENA region also struggles with weak data aggregation and coordination, alongside capacity gaps in overseeing emerging technologies (Figure 3).

Taken together, these findings describe a supervisory landscape that is evolving but increasingly strained — one that requires faster responses, more flexible operational models, and sustained investment in technological, institutional, and human-capital resilience. Yet amid this turbulence lies opportunity: massive expansion in access to high-quality, timely data and advanced analytical tools now offers the potential to augment human judgement and enable more adaptive, forward-looking supervision.

Several factors make this transformation both possible and necessary. The COVID-19 pandemic demonstrated the sector's capacity for rapid digital adoption, turning remote examinations and electronic onboarding into standard practice. A new generation of digitally native leaders is assuming influence, while generative AI (GenAI) and distributed ledger technologies (DLT) are reaching maturity for mainstream supervision.

Authorities are deploying AI-driven analytics, automated reporting and licensing systems, market intelligence tools, and advanced surveillance applications. These capabilities improve the timeliness and quality of supervisory judgement — provided they are built on robust foundations of data governance, legal clarity, operational resilience, and ethical oversight.

Supervisory priorities in 2025 reflect this shift. Prudential supervisors are intensifying vigilance through enhanced stress testing, incident reporting frameworks, and international coordination amid a volatile environment. Cyber and operational resilience remain top priorities, driven by sophisticated cyber-attacks, dependence on third-party providers, and growing digitalisation. AI commands sustained policy attention, with emphasis on responsible innovation, risk management, and supervisory capacity-building. Regulation of digital assets continues to expand, particularly for stablecoins and institutional participation, driven by varied national priorities and a notable pro-crypto stance by the United States.

AML/CFT initiatives are evolving to cover new business models and digital assets, while consumer-protection frameworks are being updated to address rising fraud, online misconduct, and the influence of finfluencers. Payments infrastructure digital public infrastructure, and climate-related financial risk remain central to supervisory agendas.

Crucially, suptech in 2025 is increasingly harnessed to bolster regulatory effectiveness across these fronts. Authorities are using advanced AI-driven analytics, automated workflows, and integrated intelligence platforms to strengthen data quality, fraud detection, market surveillance, licensing processes, and operational oversight. These innovations underpin more proactive, transparent, and resilient supervision in an evolving financial ecosystem.

This report provides evidence on how authorities worldwide are navigating this balance, including their successes, challenges, and the conditions enabling effective suptech implementation. In a world of mounting complexity and persistent uncertainty, the intelligent deployment of suptech will determine not only supervisory effectiveness but the resilience of the financial systems authorities are charged with safeguarding.

From report to practice: Connecting with GovSpace

The State of SupTech Report 2025 is designed not only as an analytical publication but as part of a living, practice-driven environment. This edition is integrated with GovSpace — a digital platform that enables authorities to explore interactive benchmarks, access curated resources and case studies, and engage with peers in dedicated Spaces.

Through GovSpace, agencies can situate their own journeys within the global picture presented in this report, translate findings into concrete diagnostic and planning exercises, and participate in an ongoing community of practice focused on strengthening supervisory capabilities and accelerating the digital transformation of financial oversight.

The chapters that follow provide evidence, comparative intelligence, and practical insights to help financial authorities navigate the next phase of the suptech journey — one defined by greater complexity, higher expectations, and unprecedented opportunities for smarter, more resilient supervision.

FIGURE 2.

Risks and Threats Identified by Financial Authorities by Economic Classification

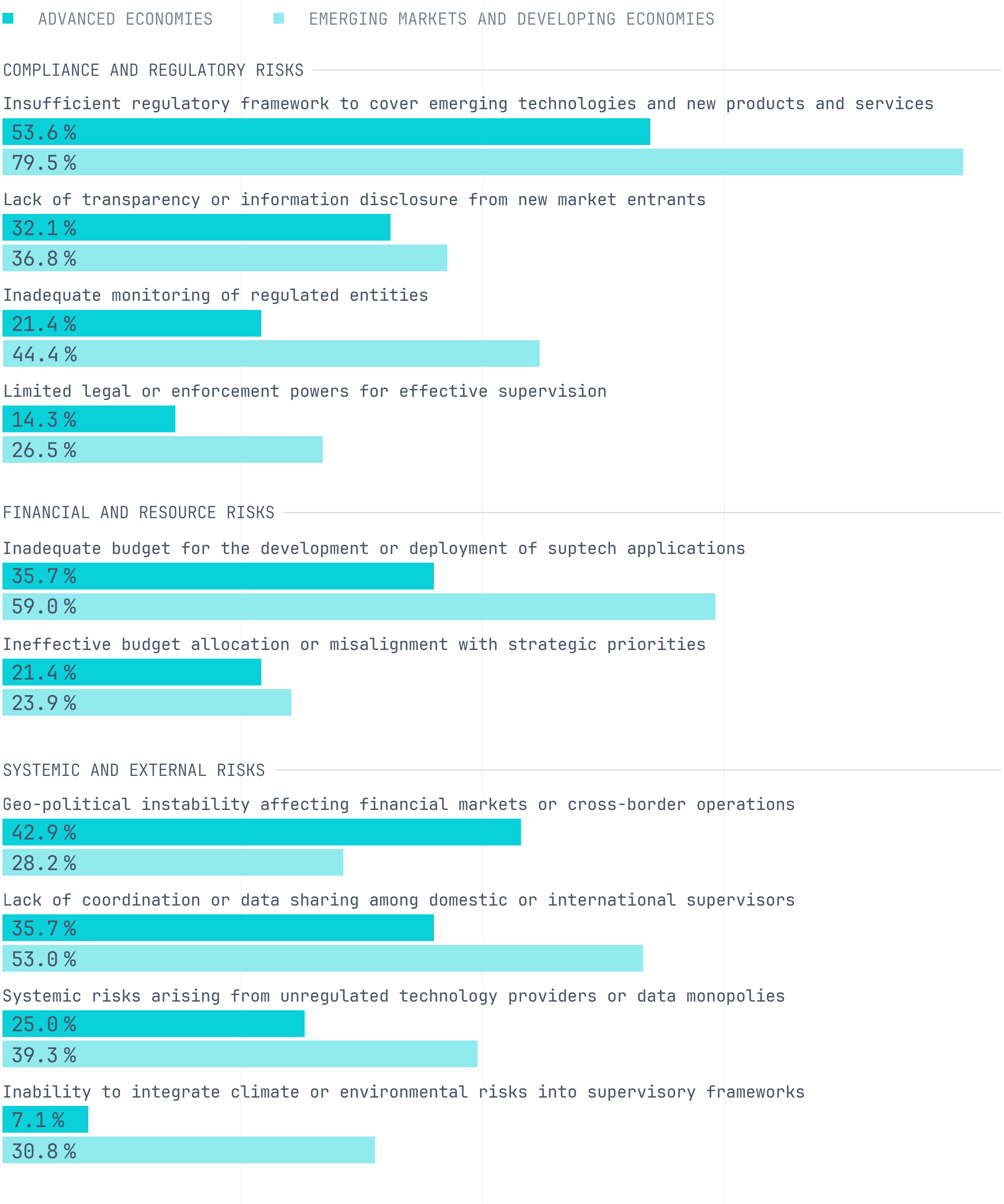


FIGURE 2. (CONTINUED)

Risks and Threats Identified by Financial Authorities by Economic Classification

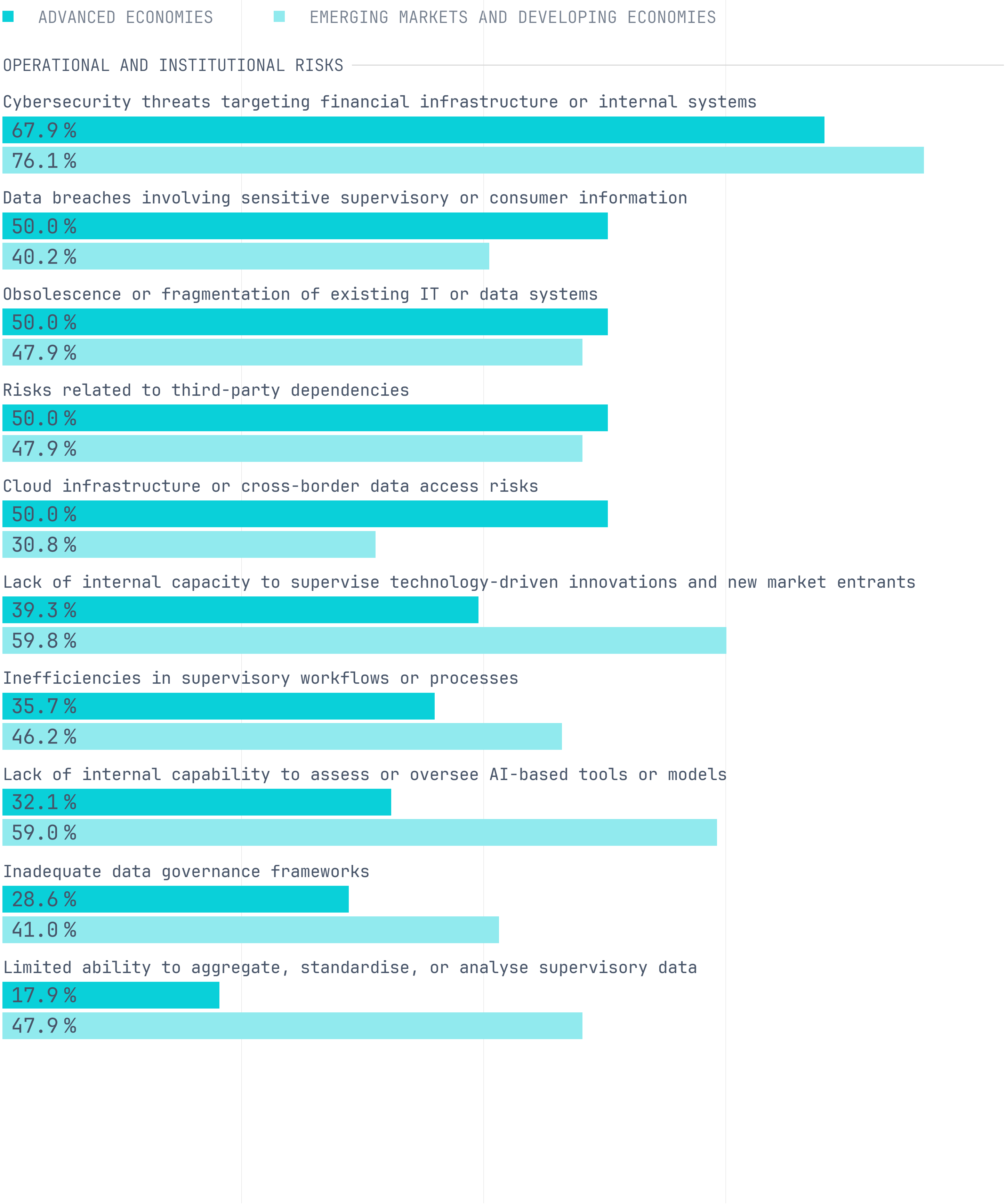


FIGURE 3.

Risks Identified by Financial Authorities
By Regional Classification

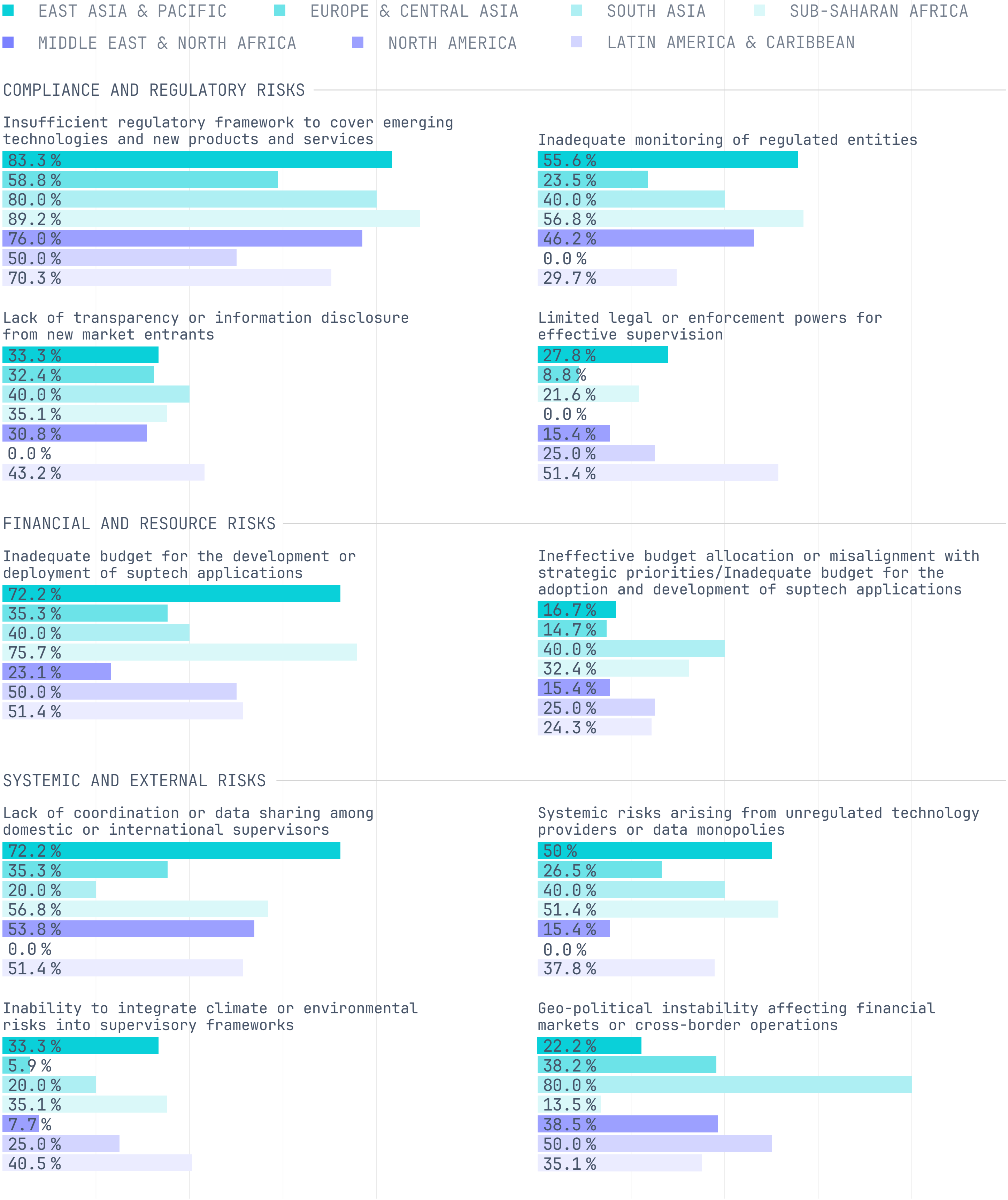
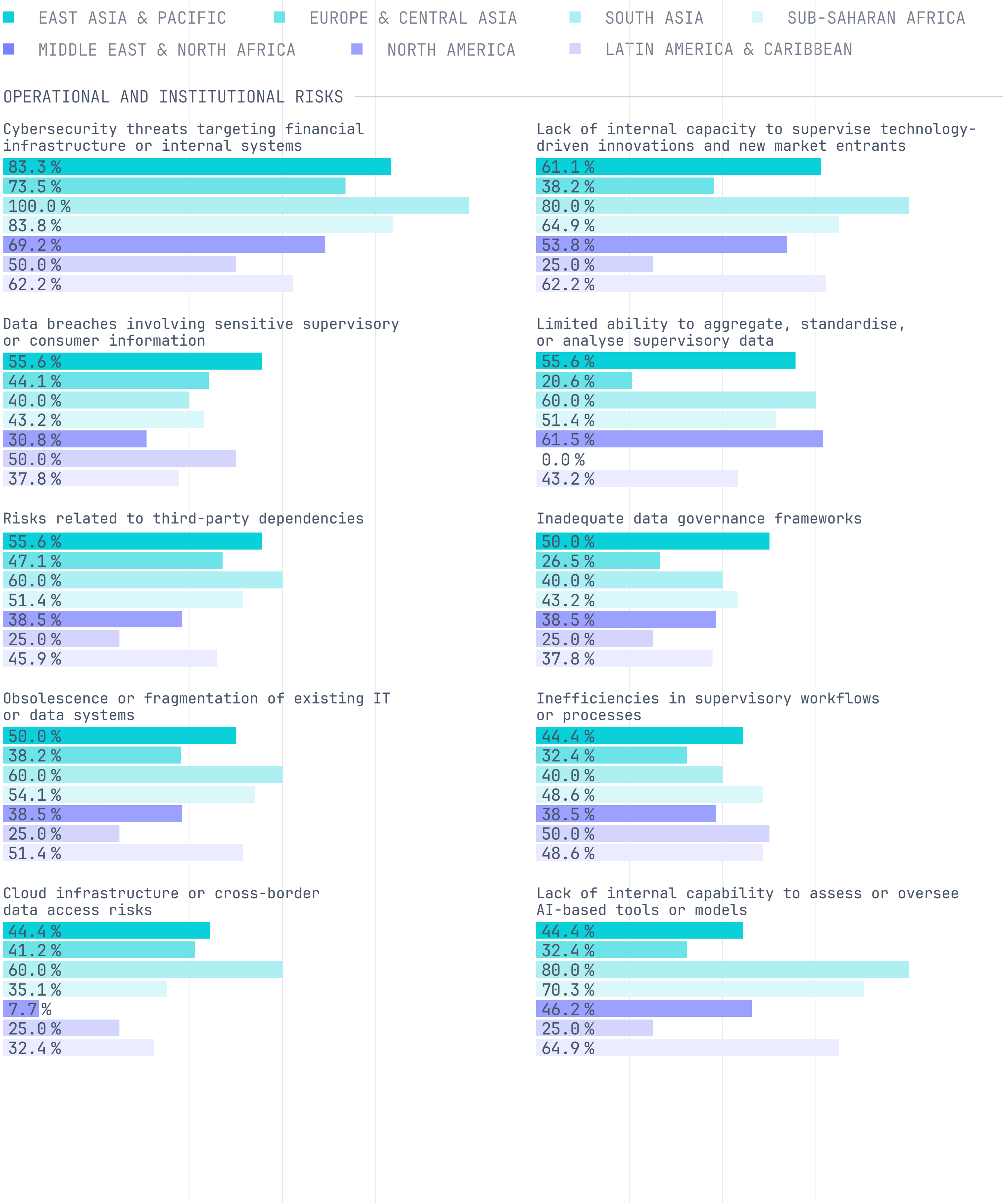


FIGURE 3. (CONTINUED)

Risks Identified by Financial Authorities
By Regional Classification



Survey Scope and Methodology

SupTech definition and generations framework

Supervisory technology, or suptech, refers to the application of technologies and data analysis solutions to augment financial authorities' capacity to oversee financial markets and optimise the use of supervisory data to improve outcomes for market participants. By facilitating access to timely, granular, and reliable information, suptech applications strengthen decision-making processes, enhance operational efficiency, and reinforce overall market integrity.

The suptech journey encompasses both the digital transformation of established supervisory processes and the adoption of "suptech-first" methodologies that harness artificial intelligence, machine learning, big data analytics, and distributed ledger technologies.

Consistent with the approach adopted in 2024, the State of SupTech Report 2025 applies a definition that excludes manual (Generation 0) and first-generation (Generation 1) tools, concentrating instead on advanced solutions classified within Generations 2, 3, and 4 of the SupTech Generations 2.0 framework. This focused scope aligns with contemporary supervisory priorities and represent substantive innovation beyond basic digitisation.

FIGURE 4.

SupTech Generations 2.0

	0G Manual	1G Minimal Tech	2G Digital	3G Advanced	4G Big Data & AI
Data Products	MINIMAL STATISTICAL SUMMARIES	DIGITAL, FILE-BASED REPORT GENERATION	MINIMAL STATIC CHARTS AND METRICS	INTERACTIVE VISUALIZATIONS	ADVANCED BUSINESS INTELLIGENCE TOOLS +GENERATIVE AI
Analytics	NO ADDITIONAL ANALYSIS	STATISTICAL SUMMARIES	DESCRIPTIVE/ DIAGNOSTIC ANALYTICS TOOLS	PREDICTIVE ANALYTICS TOOLS	PRESCRIPTIVE ANALYTICS TOOLS
Access Controls	INDIVIDUAL ACCESS ONLY	TEAM ACCESS ONLY	DEPARTMENT ACCESS ONLY	LIMITED AGENCY-WIDE ACCESS	AGENCY-WIDE ACCESS
Storage	PHYSICAL MEDIA	DIGITAL FILE-BASED STORAGE	DATABASES	CONSOLIDATED STORAGE PLATFORMS	ADVANCED STORAGE (DATA LAKES)
Validation + Processing	MANUAL OR NO VALIDATION RULES AFTER RECEIPT OF DATA	TEMPLATE-BASED VALIDATION	AUTOMATED VALIDATION	TASK AND PROCESS AUTOMATION APPLICATION	ADVANCED PROCESSING (IMAGE, TEXT, DOCUMENT, BIG DATA)
Collection	MANUALLY SUBMITTED	FILE SERVER	WEB PORTALS OR OTHER DOCUMENT MANAGEMENT	PROGRAMMING INTERFACES (API)	ADVANCED COLLECTION (AI-BASED, STREAMING, SCRAPING)

The SupTech Generations 2.0 framework delineates the progression from manual and minimally digital systems towards intelligent, AI-enabled environments that integrate automation and data across supervisory functions. It illustrates how suptech maturity advances through successive stages of digitalisation, culminating in fully data-driven, scalable, and adaptive supervisory ecosystems capable of continuous risk sensing and evidence-based intervention. For comprehensive definitions of key terms, technologies, and concepts referenced throughout this report, please refer to Appendix 3.

Report structure

The State of SupTech Report 2025 is structured to mirror the typical suptech lifecycle, from strategic planning through to operational deployment and continuous refinement. The report examines the evolving suptech ecosystem across the following thematic areas:

1. **Suptech landscape and strategies:** A comprehensive overview of global suptech adoption trends and financial authorities' strategic readiness, organisational setup, and digital transformation maturity.
2. **Suptech applications and development:** Detailed analysis of existing solutions, development methodologies, and stakeholder involvement.
3. **Supervisory areas and use cases:** Structured categorisation of functional applications across supervisory domains using the Cambridge SupTech Lab's SupTech Taxonomy.
4. **Effectiveness, risks, and challenges:** Insights into the suptech outcomes, benefits realised, and implementation obstacles.
5. **AI and GenAI adoption and maturity:** Analysis of AI deployment, from established machine learning to emerging generative AI.
6. **Data governance and data-journey essentials:** Policies, frameworks, and practices governing data throughout its lifecycle.
7. **Suptech enabling factors:** Tools, technologies, and architectures supporting suptech, structured using the DataStack framework and SupTech Generations 2.0.
8. **Capacity-building and collaboration:** Skill-building initiatives, inter-agency engagement, and partnerships supporting suptech deployment.
9. **Organisational structures and governance models:** Examination of team structures, roles, responsibilities, and governance arrangements enabling effective suptech deployment.

To complement the analysis, this year's report features six detailed case studies from leading financial authorities and ecosystem actors: De Nederlandsche Bank (Netherlands), Financial Conduct Authority (United Kingdom), Financial Superintendency of Colombia, Nasdaq, and Reserve Bank of India, and one central bank that requested anonymity. These case studies provide practical insights into the challenges, approaches, and outcomes associated with implementing specific suptech solutions across diverse institutional and jurisdictional contexts.

Survey sample

The State of SupTech Survey 2025, conducted between September and October 2025 by the Cambridge SupTech Lab and Digital Transformation Solutions team, drew participation from 148 financial authorities across the globe, providing an unprecedented breadth and depth of insight into suptech practices. The 2025 questionnaire introduced new questions on gender and sex-disaggregated data, elements of selected strategies, open data initiatives, and privacy-enhancing technologies (PETs).

The survey responses provide strong global representation, including authorities from regions that are typically underrepresented in discussions on the modernisation of financial supervision (Figure 5). Using the International Monetary Fund's World Economic Outlook classification, Emerging Market and Developing Economies (EMDEs) make up the majority of respondents with 81% of authorities, while 19% of the authorities are from Advanced Economies (AEs).

Based on the World Bank's income classification, 37% of agencies are from high-income countries, 28% from upper-middle-income, 30% from lower-middle-income, and 5% from low-income countries. The limited participation from low-income jurisdictions reflects the slower uptake of suptech solutions, as observed in data from the GovSpace Discover database.

FIGURE 5.

Distribution of Respondents by Region

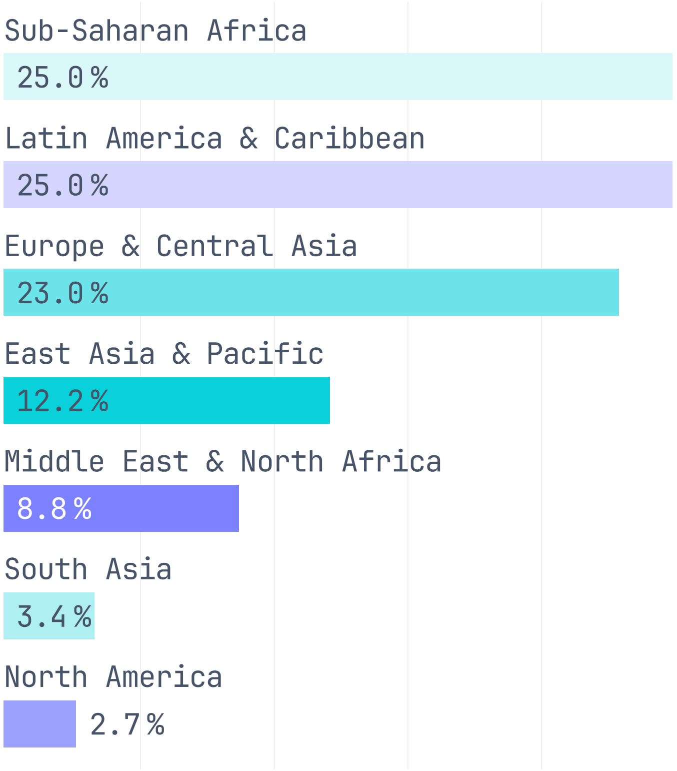
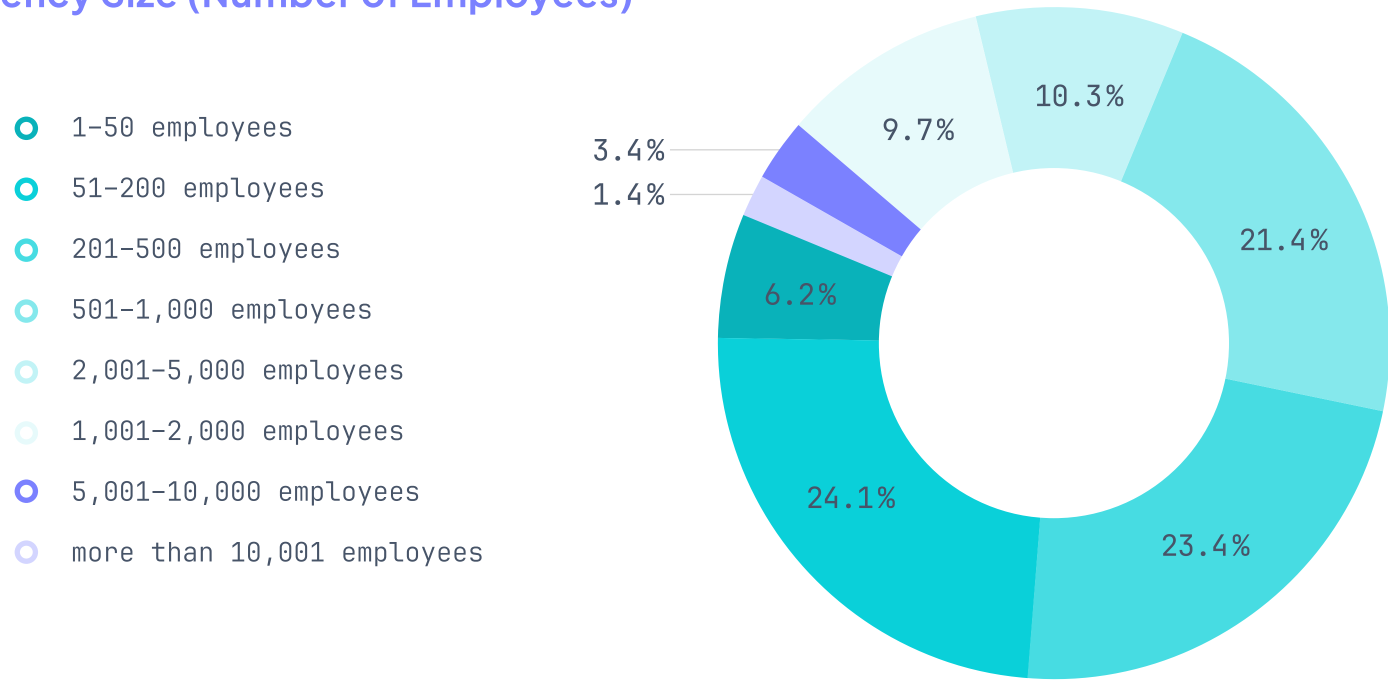


FIGURE 6.

Agency Size (Number of Employees)



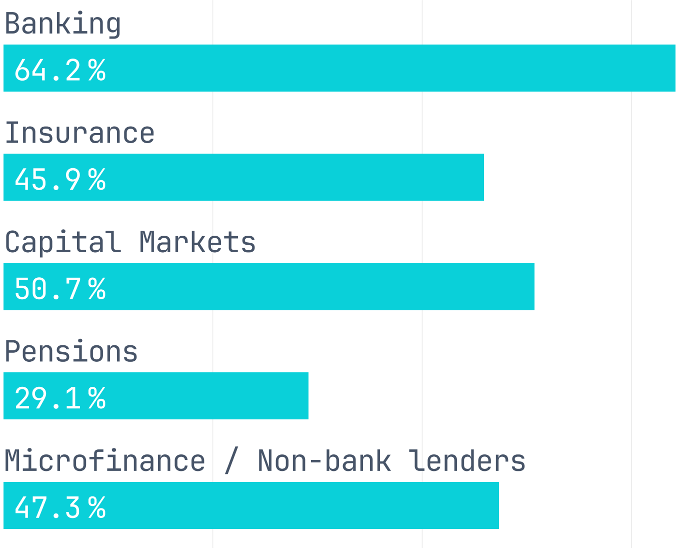
The size of respondent agencies varies widely. Small authorities with 1–50 employees represent 6.2% of the sample. Agencies with 51–200 employees (24.1%), 201–500 employees (23.4%), and 501–1,000 employees (21.4%) are the most common. Mid-sized institutions with 1,001–2,000 employees account for 9.7% of respondents, while 2,001–5,000 employees represent 10.3%. Only a small share of authorities have more than 5,000 staff: those with 5,001–10,000 employees represent 3.4%, and authorities with more than 10,000 employees account for 1.4% (Figure 6).

The majority of respondent agencies supervise multiple sectors, with banking (64%), capital markets (51%), and microfinance/non-bank lenders (both 47%) being the most common (Figure 7). Nearly half also oversee insurance (46%), while around 29% supervise pensions and 32% supervise other sectors such as fintech, payments, and crypto-assets.

Almost half of agencies (48%) operate under an integrated supervisory model, while 25% share mandates with other authorities and another 27% do not operate under an integrated model.

FIGURE 7.

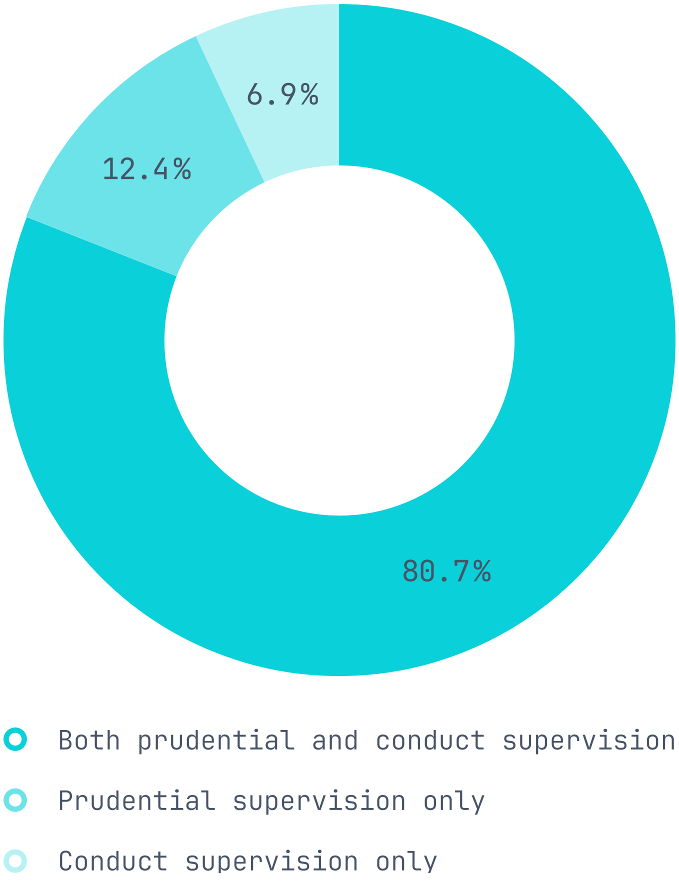
Sectors Supervised by Financial Authorities



The majority of respondent agencies (81%) report having both prudential and conduct responsibilities (Figure 8). A further 12% focus solely on prudential supervision — a mandate that typically encompasses stability and prudential activities such as macroprudential surveillance, crisis management, recovery and resolution, liquidity and solvency oversight, financial market infrastructure (FMI) supervision, stress testing, and system-wide risk monitoring. The remaining 7% are dedicated exclusively to conduct supervision, which in many jurisdictions may include areas such as anti-money laundering and countering the financing of terrorism (AML/CFT), consumer protection, and cybersecurity.

FIGURE 8.

Primary Focus Areas of Agency Supervision



Suptech taxonomy

The State of SupTech Survey employs a structured classification system known as the SupTech Taxonomy, which provides a common language for describing supervisory functions, use cases, technologies, and data architectures across jurisdictions. The taxonomy enables meaningful cross-country comparability, guides strategic and technical planning, and supports solution design by systematically mapping how supervisory challenges translate into specific digital and analytical capabilities.

Digital Transformation Solutions applies this taxonomy throughout its intelligence and transformation platform, GovSpace, where it underpins diagnostic modules, benchmark visualisations, and the mapping of applications and architectures. By aligning survey data with the same taxonomy used in GovSpace, the State of SupTech Report contributes to a shared ecosystem-wide framework that improves data harmonisation, strengthens coordination among authorities and providers, and accelerates the development of interoperable, scalable suptech applications.

First introduced in the State of SupTech Report 2022, the taxonomy distinctly separates supervisory dimensions from technology dimensions, enabling systematic identification of supervisory needs and more deliberate alignment of digital solutions to those needs:

- The **supervisory dimension** comprises 16 areas, including three newly added ones:

    - Supervisory oversight of artificial Intelligence (AI) use by regulated firms
    - Open banking and open finance supervision
    - Operational risks supervision.

  These are subdivided into **163 use cases**, an expansion from 101 in the previous year. This hierarchical structure organises use cases according to activities performed by supervisory functions.

- The **technology dimension** categorises tools according to their application within **five layers of the suptech data stack** (see section 4.2).

Together, the supervisory and technology dimensions form an integrated framework that underpins the analytical approach in this report. The taxonomy shapes the structure of subsequent chapters, informs cross-country comparisons, and supports the detailed mapping of suptech applications highlighted in the case studies and annexes.

THE STATE OF SUPTECH

1.

Suptech Adoption and Effectiveness

1.1 The global expansion of suptech: Tracking adoption and growth

Suptech adoption has expanded significantly across jurisdictions. The number of authorities with at least one 2G–4G deployment has tripled since 2022, reaching 197 agencies across 140 countries in 2025. Adoption is broadening, but depth varies: 60% of surveyed authorities now use suptech, with 44% operating more than five applications and 19% operating more than ten. Advanced economies report significantly higher deployment maturity, with 85% using suptech and 43% deploying more than ten applications, compared with 53% and 11% respectively in EMDEs.

Suptech uptake has accelerated markedly over the past four years (Figure 9). In 2022, 54 authorities reported at least one Generation 2, 3, or 4 live suptech application. This increased to 79 in 2023, followed by a significant jump in 2024 when 171 authorities had operational deployments. By 2025, the total reaches **197 authorities across 140 countries** — more than a threefold increase since 2022, highlighting the increasing role of digital tools in contemporary financial supervision.

FIGURE 9.

Financial Authorities With One or More SupTech Applications Deployed

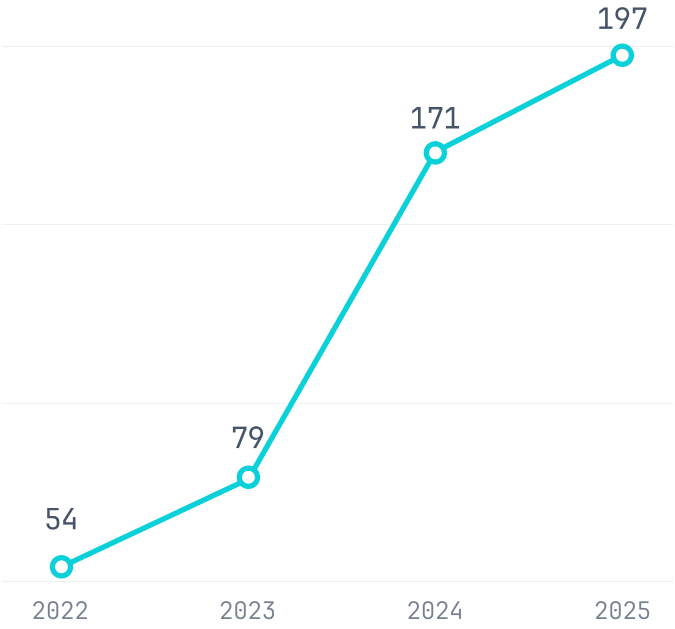


Figure 10 shows the global distribution of these deployments, reflecting a broad-based expansion of supervisory digital transformation.

This global count combines self-reported data from the four editions of the State of SupTech survey with additional authorities identified through GovSpace Discover as having deployed 2G–4G applications, providing a broader and more up-to-date picture of worldwide adoption.

In 2025, 60% of surveyed financial authorities reported actively using suptech applications (Figure 11). Among these agencies, deployments vary considerably: 22% operate a single application, 34% have implemented between two and five, and 44% report using more than five suptech applications, with 19% indicating they operate more than ten.

These findings show that suptech adoption is becoming more widespread, but the depth and sophistication of implementation differ widely across jurisdictions. While many authorities remain at an early stage — operating only one or a few applications — a significant and growing cohort is scaling portfolios across multiple supervisory functions. The fact that 44% of active users now operate more than five applications, and nearly one in five operates more than ten, indicates that suptech is increasingly suggests that suptech is being applied across a broader set of supervisory processes, rather than limited to isolated pilots. These patterns reflect variations in strategy maturity, digital readiness, data infrastructure, governance arrangements, and organisational capacity.

FIGURE 10.

Global Suptech Adoption:
Countries with one or more suptech applications deployed

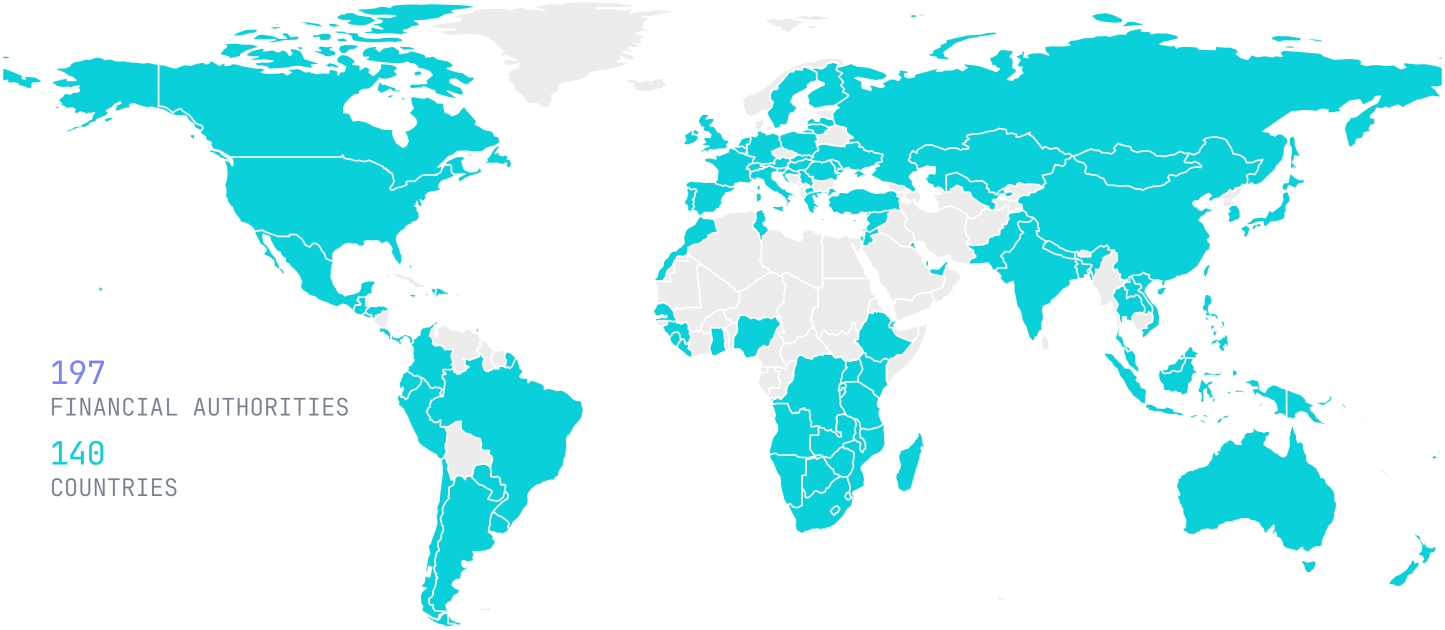
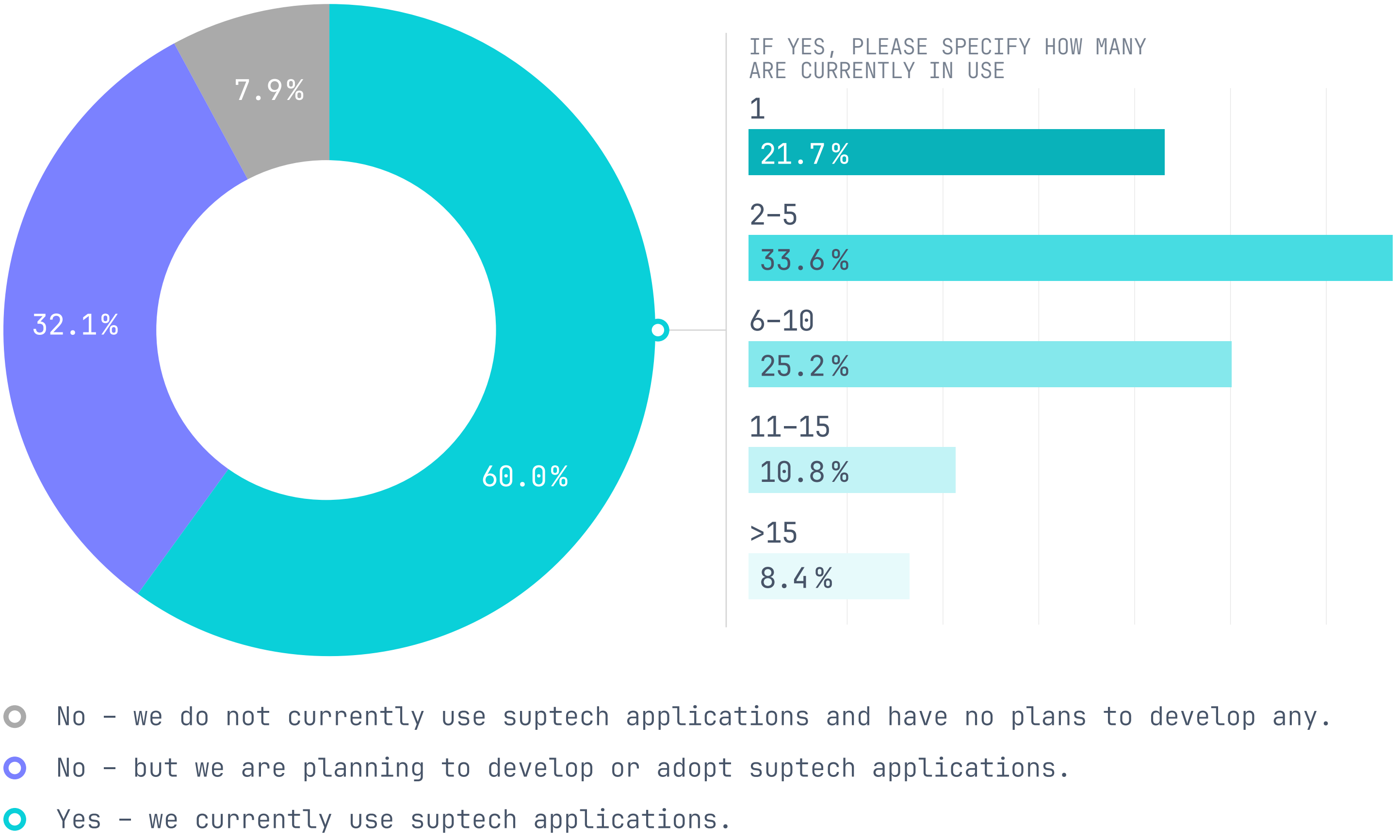


FIGURE 11.

Number of SupTech Application Deployed



Beyond current users, 32% of financial authorities plan to develop or adopt suptech applications, while around 8% report no immediate plans to do so. This underscores the uneven maturity landscape and highlights the need for continued collaboration, knowledge exchange, and the sharing of reusable code, architectures, and assets to support more consistent and inclusive progress across jurisdictions.

The adoption of suptech continues to be significantly higher in advanced economies (AEs), where 85% of agencies report using applications and 15% indicate plans for future deployment. In contrast, in EMDEs just over half of authorities currently use suptech (53%), while 37% plan to adopt and 10% report no plans. This highlights a clear adoption gap and persistent implementation hurdles for EMDEs.

Maturity levels also differ markedly. In AEs, 43% of agencies have deployed more than ten applications, compared with only 11% in EMDEs (Figure 12).

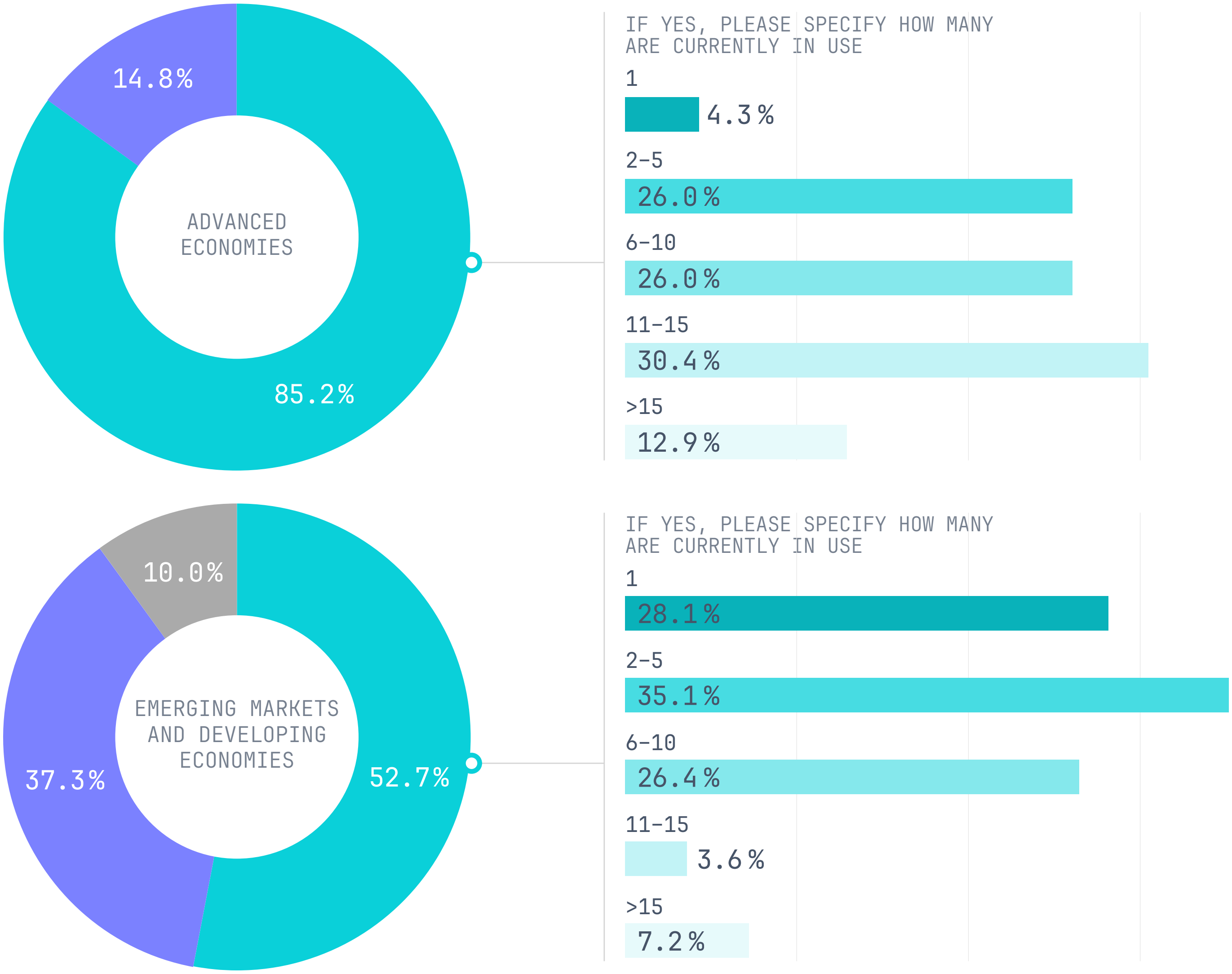
FIGURE 12.

Status of SupTech Application Deployment by Economic Classification

○ No – we do not currently use suptech applications and have no plans to develop any.

○ No – but we are planning to develop or adopt suptech applications.

○ Yes – we currently use suptech applications.



1.2 Effectiveness of suptech solutions

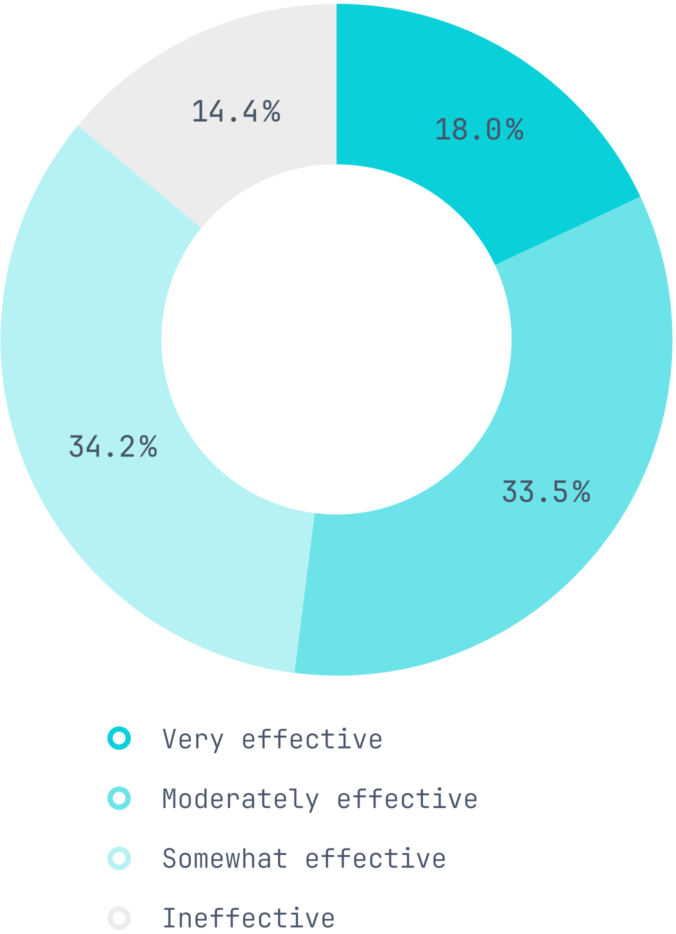
Financial authorities continue to view suptech as beneficial, but assessments in 2025 are more calibrated. While 18% of agencies rate their applications as very effective, most classify them as moderately effective (33.5%) or somewhat effective (34.2%), and 14.4% consider them ineffective. Effectiveness is strongest for internal supervisory performance, including time savings, data integration, analytical accuracy, and support for data-driven decision-making. External supervisory outcomes, such as influencing regulated-entity behaviour or enabling real-time supervision, receive lower ratings. Perceived effectiveness varies by economic classification: EMDEs report higher gains in time and cost efficiency, while advanced economies report stronger results in data integration and interoperability.

Financial authorities continue to view suptech as a valuable asset, but the 2025 survey shows a more measured and discerning assessment of effectiveness. his shift may reflect maturing expectations and more rigorous assessments as deployments become more established.

While 18% of authorities rate their applications as very effective, the largest share (33.5%) considers them *moderately effective* and 34.2% *somewhat effective*, bringing the majority of agencies to acknowledge meaningful — though uneven — benefits. A smaller proportion (14.4%) considers current solutions *ineffective* (Figure 13).

FIGURE 13.

Effectiveness of SupTech Applications

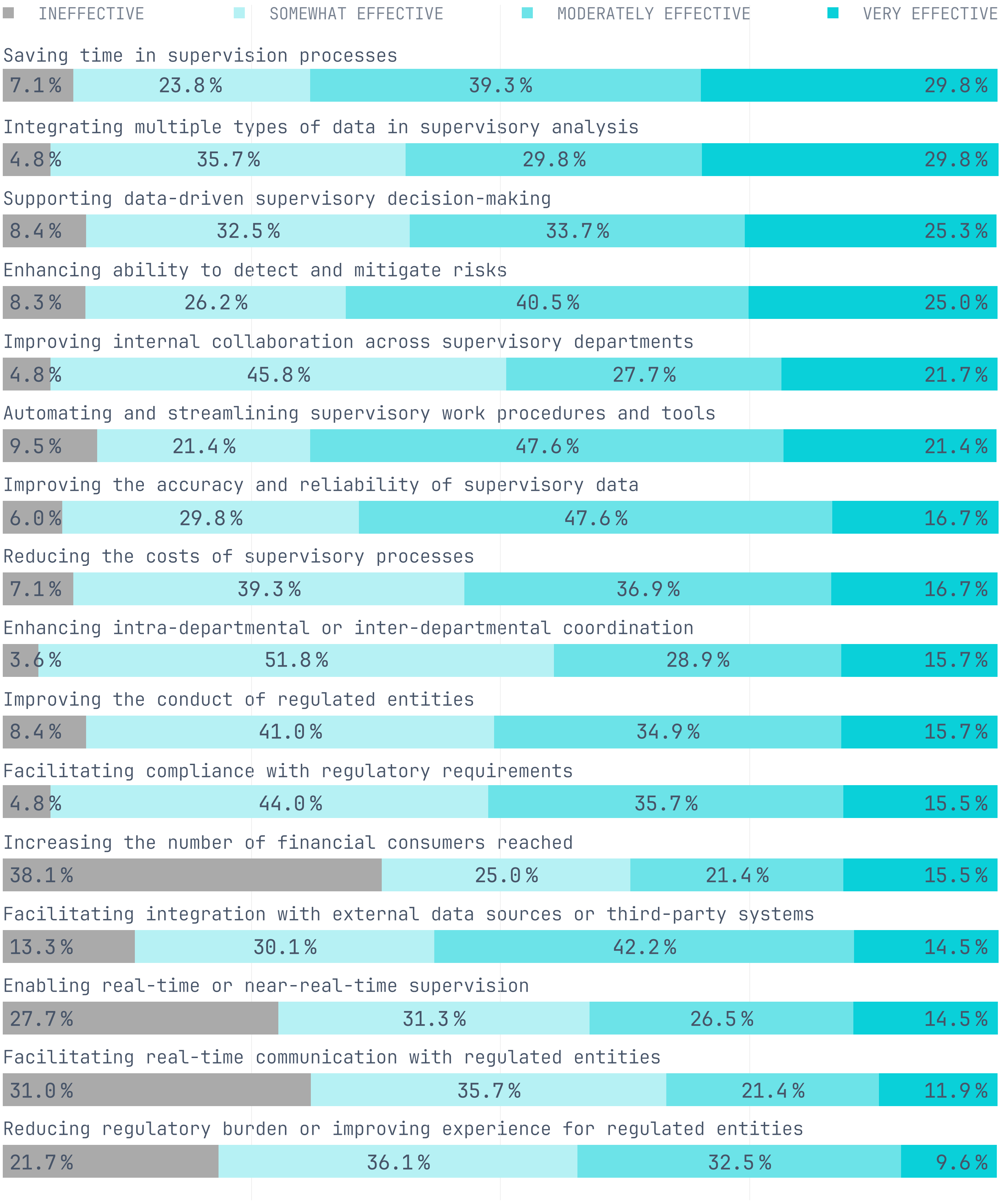


A number of factors may help explain why effectiveness assessments appear more measured in 2025. While the survey does not directly capture respondents' underlying reasoning, several developments observed across supervisory practice could influence how authorities evaluate their applications:

- **Evolving expectations as deployments mature.** As suptech moves from pilots into routine supervisory workflows, authorities may be developing a clearer understanding of what constitutes effective performance and assessing solutions against more complex, real-world use cases.
- **More structured measurement frameworks.** Compared with earlier years, authorities increasingly report using KPIs, outcome frameworks, and longitudinal assessments. These tools naturally lead to more calibrated evaluations than the enthusiasm-driven

FIGURE 14.

Effectiveness of SupTech Applications



assessments that often accompany early-stage innovation.

- **Greater visibility of institutional constraints.** As deployments scale, issues related to data quality, governance, change management, and system interoperability become more evident. This may enable authorities to differentiate more clearly between limitations rooted in technology and those stemming from institutional processes.
- **Expansion into technically demanding domains.** Suptech is increasingly applied to areas such as AI model oversight, real-time market monitoring, behavioural analytics, and operational-risk supervision. These domains inherently require more sophisticated data, infrastructure, and organisational readiness, which may temper perceived effectiveness.uShift from novelty to operational integration. As applications become part of day-to-day supervisory work, their value is assessed less on innovation and more on reliability, scalability, and alignment with established supervisory processes.

These factors may contribute to the more nuanced effectiveness ratings observed in 2025, reflecting a supervisory community that is assessing suptech within the realities of operational use rather than early-stage experimentation.

Effectiveness varies significantly across supervisory KPIs. Suptech applications continue to deliver the clearest benefits where performance is measured through internal operational indicators — such as workflow optimisation, data integration, time savings, and analytical quality. These areas show the highest levels of perceived effectiveness across all response categories. By contrast, KPIs linked to external supervisory outcomes — including influencing regulated-entity behaviour, supporting real-time supervision, and improving market or consumer outcomes — exhibit more mixed and often modest ratings.

The strongest perceived impact lies in improving internal supervisory performance. The highest very effective ratings are concentrated in time savings (30%), integration of multiple data types (30%), support for data-driven decision-making (25%), improvement in analytical accuracy and reliability (17%), and enhanced ability to detect and mitigate risks (25%). When combining *very effective* and *moderately effective*, these core internal functions consistently fall within the 64–75% range. These results suggest that suptech delivers its most immediate and measurable gains in data integration, workflow efficiency, and analytical depth.

This strength in data handling can support supervisory judgement by improving the availability and quality of analytical inputs. Approximately 60% of respondents rate suptech as at least *moderately effective* in enabling data-driven supervisory decision-making and in improving risk detection. These contributions are relevant for prudential and conduct oversight and underscore the value of suptech as a force multiplier for supervisory analysis.

Efficiency benefits are reflected in the positive ratings reported by agencies. A combined 69% of agencies report positive effects in saving time in supervisory processes, and 69% report improvements in automating and streamlining supervisory procedures and tools. However, financial efficiencies lag behind operational efficiencies: only 54% view suptech as effective in reducing the costs of supervisory processes, and just 17% consider it very effective. This gap suggests that while process automation is accelerating workflows, institutional cost savings remain longer-term and depend on broader operational restructuring, staff redistribution, and legacy system rationalisation.

Progress on organisational coordination and collaboration is more limited. Only 49% rate suptech as effective in improving internal collaboration across departments, and 45% in improving intra- or inter-departmental coordination. These weaker results reflect a common trend: survey responses suggest that technology alone does not resolve organisational coordination challenges without accompanying changes in governance, incentives, and culture.

External-facing supervisory outcomes show the most modest levels of effectiveness. Ratings for influencing regulated-entity behaviour, facilitating compliance, improving external communication, or supporting real-time or near-real-time supervision are sharply lower. For example, enabling real-time supervision has only 15% *very effective* and 27% *moderately effective* ratings, while 28% rate it *ineffective*. These results indicate that some supervisory activities, particularly those requiring real-time data or behavioural insights, remain more challenging to digitise. Some of these limitations also reflect an organisational dynamic explored later in this report: advanced analytical outputs are not yet routinely used by senior leadership, constraining the strategic uptake of suptech insights (see section 2.3.2).

Taken together, this evidence points toward two recurring patterns:

1. Suptech delivers its strongest value where data, internal processes, and analytical workflows are central.
2. More complex supervisory outcomes — especially those requiring behavioural change by regulated entities or real-time oversight — demand deeper institutional reform, stronger data foundations, and more advanced operational models than most authorities currently possess.

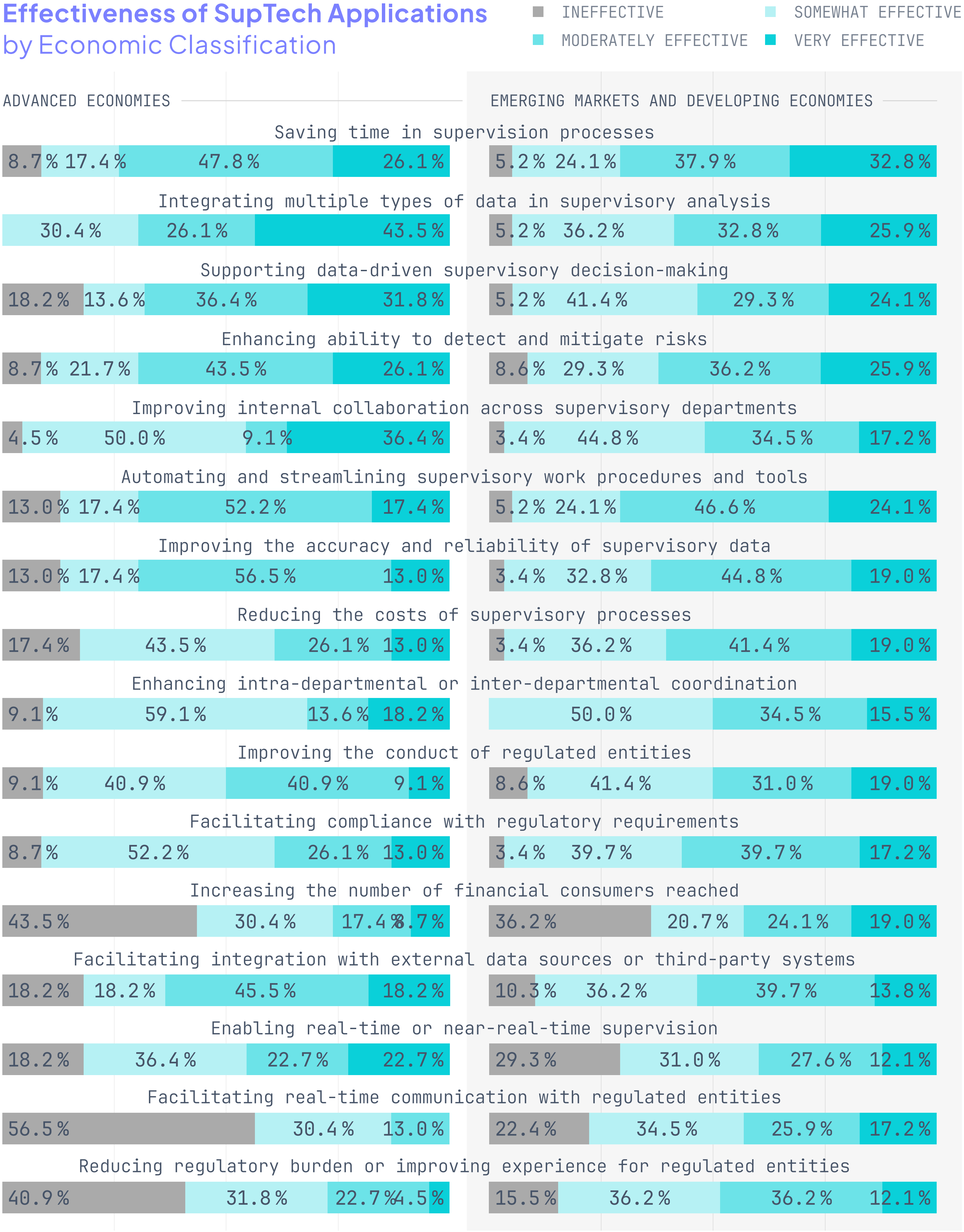
The segmentation of results by economic classification (Figure 15) highlights meaningful differences in perceived effectiveness. Authorities in emerging markets report higher effectiveness in saving time (71% combining very and moderately effective) and reducing supervisory costs (60% versus 39% in AEs), likely reflecting substantial efficiency gains from digitising previously manual or paper-based processes. However, EMDEs lag in more technologically demanding areas, such as enabling real-time or near-real-time supervision (40% versus 45% in AEs), pointing to differences in underlying infrastructure, data availability, and analytical expertise.

Authorities in advanced economies tend to report stronger effectiveness in data-related capabilities. Perceived effectiveness is slightly higher for integrating multiple types of data (70% versus 59% in EMDEs) and for facilitating integration with external data sources or third-party systems (64% versus 54%), reflecting the presence of more mature data ecosystems, more harmonised reporting infrastructures, and higher adoption of interoperability standards.

Across both groups, somewhat effective remains the dominant rating in many categories, indicating that most agencies experience partial but incomplete benefits. This reinforces the conclusion that while suptech is creating measurable value, many applications have not yet reached their full potential and would benefit from deeper integration, more robust data foundations, and stronger organisational enablers.

FIGURE 15.

Effectiveness of SupTech Applications by Economic Classification



1.3 Cross-cutting challenges in digital transformation, suptech, data governance, and AI adoption

Financial authorities face a consistent set of cross-cutting obstacles across strategy, suptech, data governance, and AI adoption. Commonly reported constraints include limited internal capacity, fragmented organisational structures, persistent data-quality and interoperability issues, and governance or trust concerns. Resource and procurement limitations further slow implementation. Although the 2025 survey expands the analysis beyond previous editions, the results strongly reinforce long-standing patterns: digital transformation is progressing, but remains uneven and constrained by foundational institutional bottlenecks.

Across all dimensions of digital transformation — from strategy formulation to application development, data governance, and AI deployment — financial authorities face a persistent and interconnected set of challenges. Although each domain presents distinct obstacles, the 2025 survey reveals four systemic patterns that cut across all areas: capacity constraints, organisational fragmentation, foundational data and infrastructure weaknesses, and governance or trust-related barriers. These challenges shape the conditions under which supervisory modernisation is progressing.

This year's analysis expands significantly on the challenge framework used in the 2024 edition. Despite this broader scope, the results broadly echo the trends observed in previous editions of this report.

More detailed analysis of each challenge domain appears in:

- Section 2.2.3 — Strategy-related design and implementation constraints
- Section 2.4.5 — Design and deployment challenges for suptech applications
- Section 4.1 — Data management, governance, and data-quality bottlenecks
- Section 5.2 — Barriers to AI deployment and evolution of supervisory AI challenges

Capacity limitations remain the most pervasive constraint across all domains

Limited internal capacity — both in digital expertise and available specialised staff — is the most consistently reported challenge.

- **Strategy development:** Nearly half of authorities cite a lack of internal capacity or experience in digital strategy design (48%).
- **Suptech applications:** Talent shortages (43%) and gaps in product-design skills (41%) are major barriers.
- **Data management:** Authorities struggle to manage high-volume, dynamic data (57%) and rely heavily on manual cleaning (45%).
- **AI:** Skills gaps are a major constraint (22%).

Across all areas, these patterns confirm that digital transformation is constrained more by human capital and institutional readiness than by technology availability.

Organisational fragmentation and weak coordination impede both design and execution

Cross-departmental and cross-agency coordination problems appear prominently across the survey.

- **Strategy:** Difficulty achieving cross-departmental input (33%) and silo issues during implementation (46%).
- **Suptech**: Coordination challenges between agencies or shared data access limitations (22%).
- **Data management:** Inconsistent data standards and identifiers (24–26%).
- **AI:** Integration challenges with existing workflows (20%) and governance or accountability gaps (17%).

These findings suggest that organisational fragmentation is a significant barrier to scaling digital transformation.

Data quality, interoperability, and legacy infrastructure present structural bottlenecks

Data-related weaknesses are widely reported across all dimensions of digital transformation.

- **Strategy:** Limited availability of relevant data and diagnostics (23%).
- **Suptech:** Data quality issues are the top design-stage barrier (49%).
- **Data management:** Integrating diverse and legacy data sources (64%), ensuring validated submissions (60%), enabling interoperability (40%).
- **AI:** Data protection and privacy (30%), explainability and transparency concerns (18%), and foundational data quality risks (11%).

Legacy IT systems exacerbate these issues, hindering interoperability and complicating the deployment of modern technologies.

Resource constraints and procurement barriers slow implementation and limit scalability

Resource pressures consistently limit implementation progress.

- **Strategy implementation:** Budget constraints or misaligned procurement cycles (37%).
- **Suptech:** Cost pressures (43%), resource-intensive deployment (52%), procurement constraints (39%).
- **Data:** Resource limitations restrict infrastructure upgrades (37%).
- **AI:** High implementation costs and compute requirements (17%).

Even where strategic intent is strong, execution remains vulnerable to fiscal constraints and rigid procurement practices.

Governance, trust, and ethical concerns increasingly shape technology adoption

Governance and trust have become decisive factors across all digital transformation domains.

- **Strategy:** Securing leadership sponsorship remains a challenge (17%).
- **Suptech:** Organisational culture not aligned with innovation (38%).
- **Data:** Lack of clarity on accountability for data quality (32%).
- **AI:** Privacy/security concerns (30%), explainability and “black box” risks (18%), reputational concerns (11%).

These factors point to the growing importance of responsible use, transparency, and risk management in digital transformation efforts.

2.

Pathways to Suptech Adoption

Strategies, governance, and operational enablers

2.1 Strategic, governance and operational responses to implementation challenges

Financial authorities are taking a wide range of actions to strengthen their digital transformation and suptech programmes. The most common steps focus on building skills, expanding peer learning, and developing institution-wide strategies. Many agencies are also updating legacy systems, revising internal guidelines, and strengthening talent and training frameworks. Technology exploration and ecosystem engagement are increasingly typical, including technology scouting, cloud adoption, and collaboration with multilaterals and regulated entities. While both AEs and EMDEs prioritise upskilling and strategy development, AEs place greater emphasis on modernising core infrastructure, whereas EMDEs focus more on technology discovery, external support, and direct collaboration with industry.

Financial authorities are actively advancing their digital transformation agendas by taking a wide range of actions to mitigate the risks highlighted in the Introduction and to address the challenges identified in Section 1.3. These measures aim to enable smarter supervision — that is, supervision that is more data-driven, anticipatory, timely, and proportionate, supported by enhanced analytical depth and operational agility.

The distribution of actions reported (Figure 16) shows a strong emphasis on capability building, modernising legacy systems, and reinforcing cross-institutional cooperation, supported by targeted efforts to improve digital readiness and supervisory effectiveness.

Human capital development and peer exchange as primary levers

Across all response categories, skills and capability enhancement emerge as the dominant focus. The largest share of authorities engaged in external training programmes (66%), closely followed by internal training programmes (61%) and participation in peer-learning forums or technical workshops (61%). These findings highlight the central role of people and institutional culture in enabling suptech adoption. The fact that bilateral collaboration is the second most common overall action (62%) further underscores how strongly supervisors rely on peer networks and knowledge exchange as accelerators of transformation.

Strategic alignment and institutional commitment

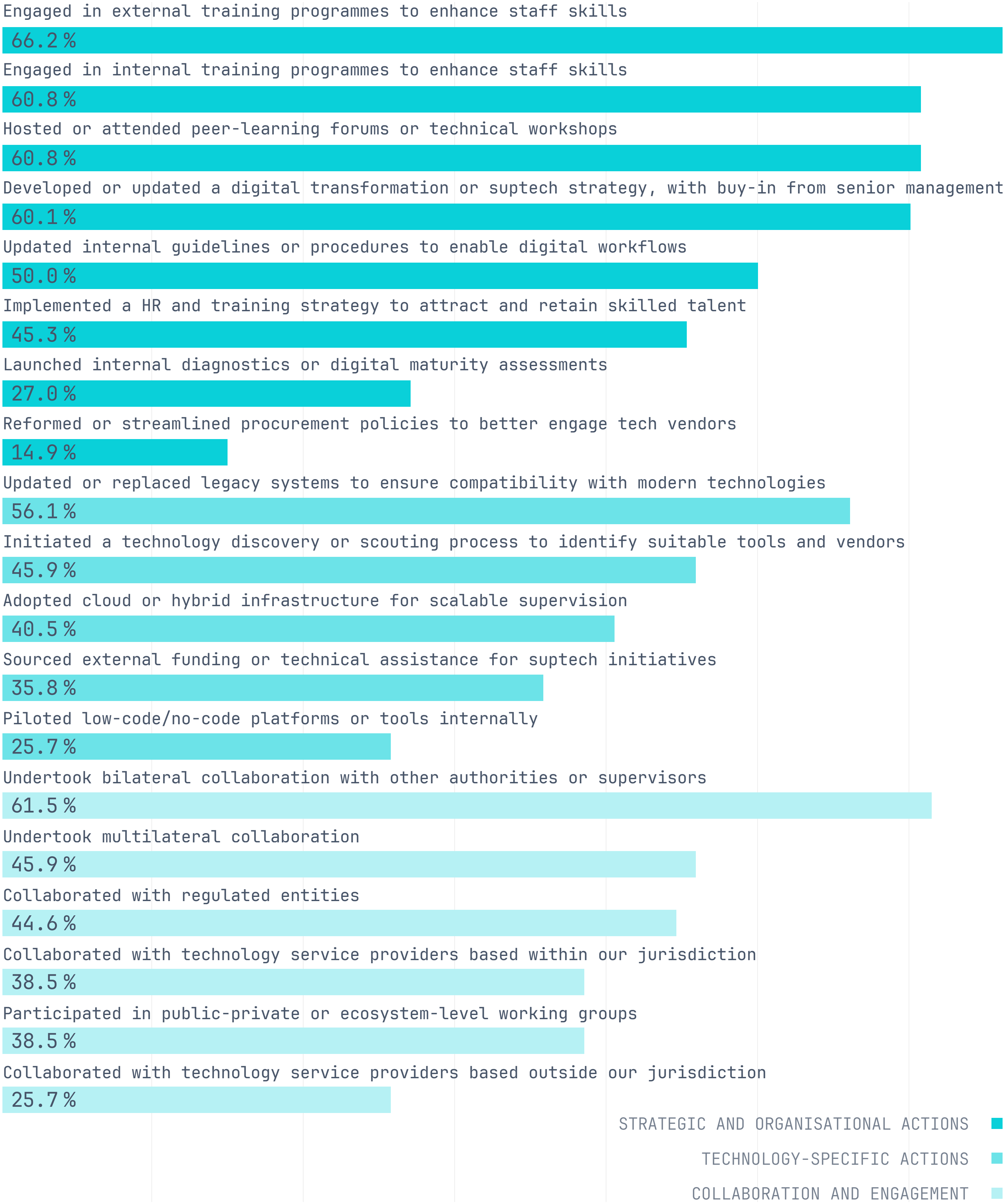
A notable proportion of authorities are shifting from reactive or tool-specific deployments to coherent institutional strategies. 60% developed or updated a digital transformation or suptech strategy with explicit senior-management endorsement. This evolution signals strengthening organisational commitment and internal alignment. These developments provide the foundation for the deeper analysis presented in Sections 2.2, 2.3, and 2.4, which examine how agencies formalise strategies, structure governance, and operationalise transformation.

Operational readiness: systems, guidelines, and talent

Operational enablers also feature prominently. Half of the respondents reported updating internal guidelines or procedures to support digital workflows (50%), and more than half updated or replaced legacy systems to ensure compatibility with modern technologies (56%). Efforts to attract and retain skilled talent were also substantial, with 45% implementing HR or training strategies.

FIGURE 16.

Actions Taken by Agencies to Address Digital Transformation and SupTech Challenges



Despite widespread recognition of procurement as a barrier (see the 2024 edition for the perspective of suptech providers and the 2022 edition for detailed analysis of procurement pathways), only 15% reported implementing procurement reforms. This remains one of the most significant gaps between perceived importance and concrete action, and continues to serve as a critical bottleneck for scalability and innovation.

Technology engagement and multi-stakeholder collaboration

Authorities also pursued a range of technology-focused and partnership-based approaches. Many initiated technology discovery or scouting processes to identify suitable tools and vendors (46%), adopted cloud or hybrid infrastructure to support scalable supervision (41%), or piloted low-code/no-code platforms (26%).

FIGURE 17.

Actions Taken by Agencies to Accelerate SupTech

By Economic Classification

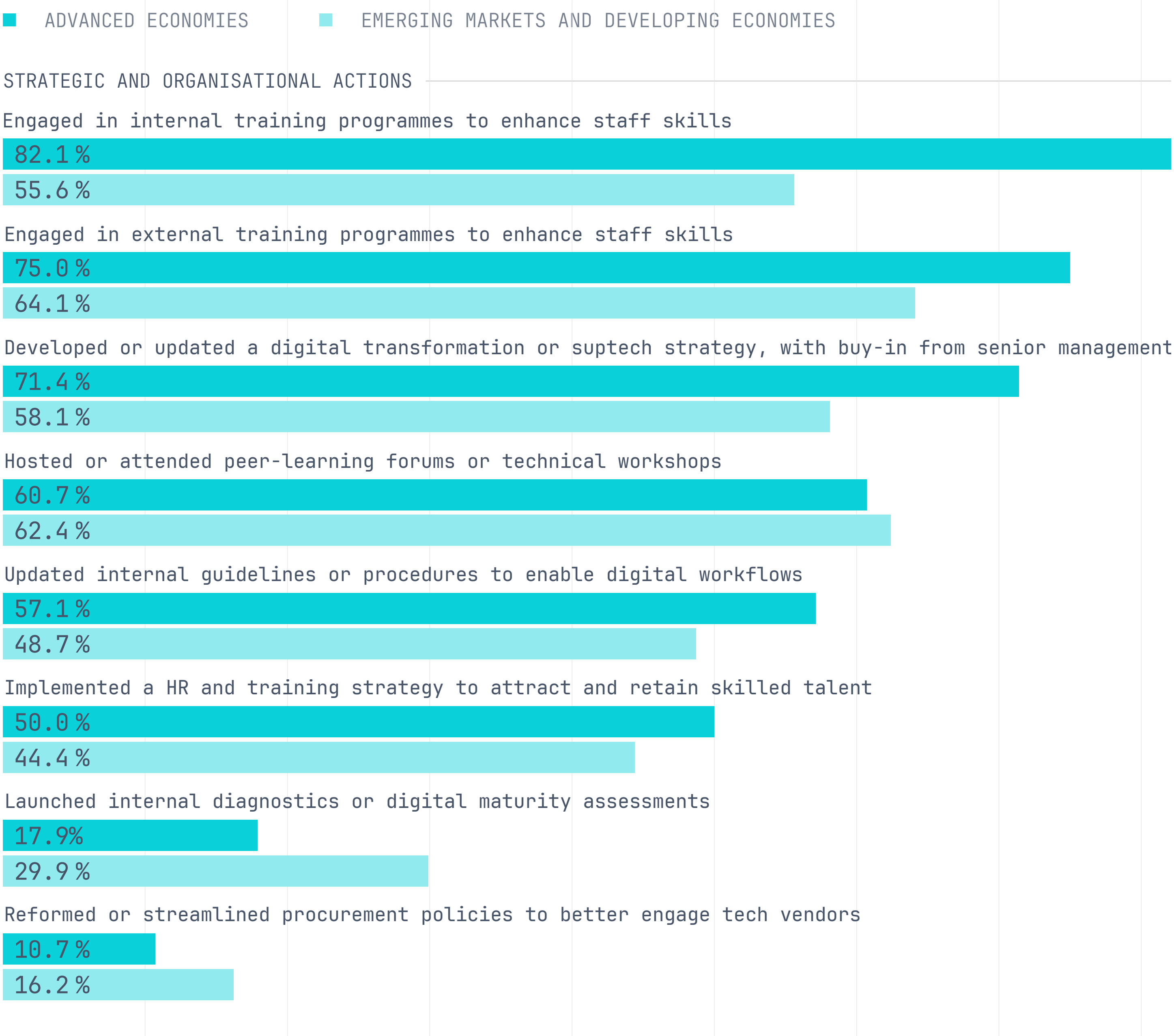
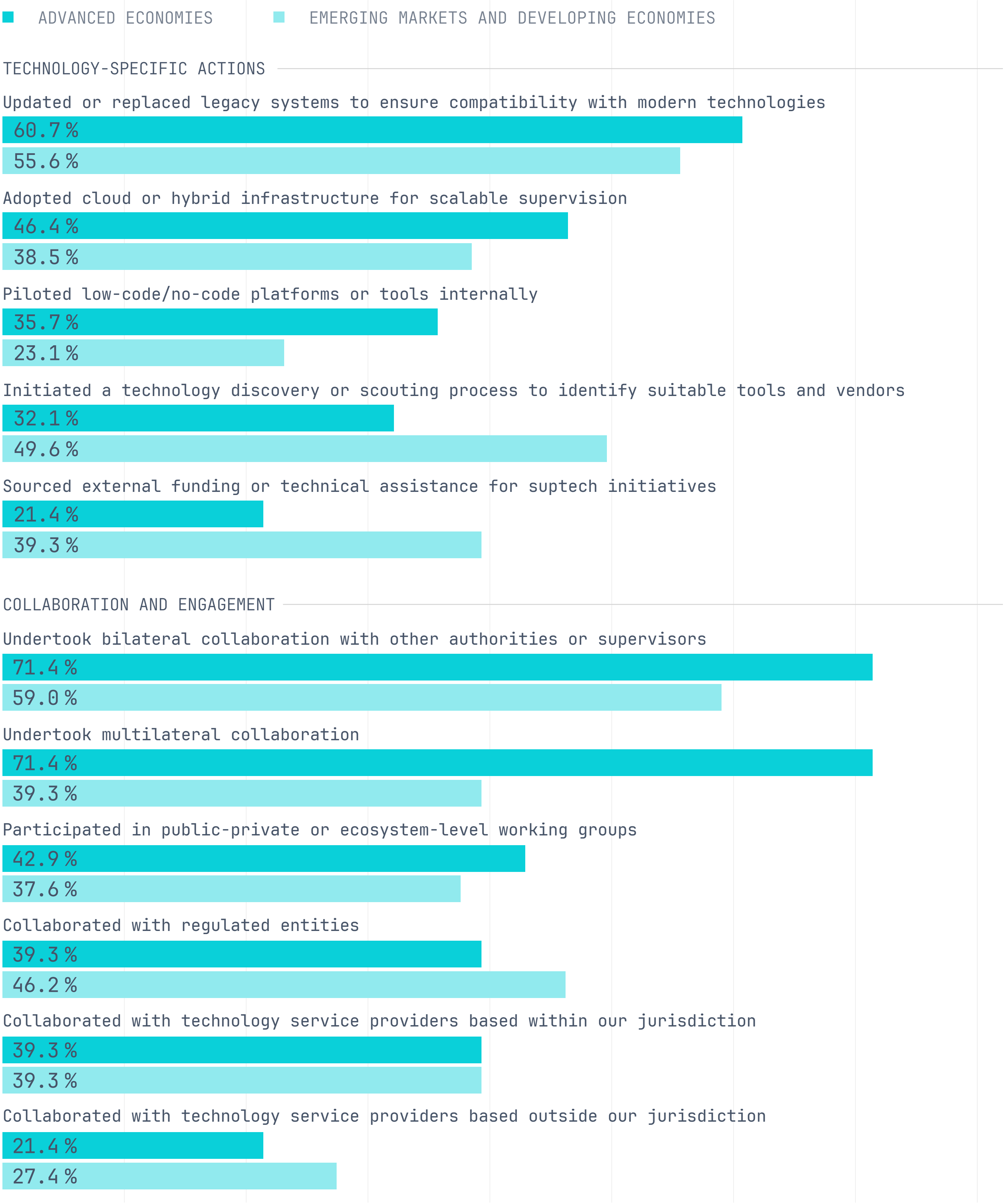


FIGURE 17. (CONTINUED)

Actions Taken by Agencies to Accelerate SupTech

By Economic Classification



Collaboration across the ecosystem was equally prominent: multilateral engagement was reported by 46% of authorities, while 45% collaborated with regulated entities through pilots or sandboxes. These actions signal a growing openness to experimentation, ecosystem engagement, and modern architectures, although uneven adoption across regions reflects differences in resources and digital maturity.

Both AEs and EMDEs prioritise internal upskilling and strategic alignment (Figure 17). A clear majority of AEs focus on internal (82%) and external (75%) training programmes, alongside developing or updating a digital transformation or suptech roadmap (71%). EMDEs similarly rely on external training (64%) and institution-wide strategy development (58%), but place slightly greater emphasis on peer-learning, with 62% hosting or attending peer-learning forums. This indicates a global recognition that human capital and strategic clarity are the most critical first steps in overcoming implementation hurdles.

In terms of direct technological and system-focused actions, AEs concentrate on modernising core infrastructure: 61% updated or replaced legacy systems and 46% adopted cloud or hybrid infrastructure. EMDEs also prioritise legacy system upgrades (56%), but their technology strategy leans more towards exploration and external support. Nearly half (49.6%) have initiated a technology discovery or scouting programme (compared with 32% of AEs), and 39% have sourced external funding or technical assistance, reflecting a greater need for external resources and validation to drive technological change.

Patterns of external engagement differ meaningfully. AEs prioritise multilateral cooperation, with both bilateral and multilateral collaboration reported by 71% of agencies, and 43% also engaged in public–private or ecosystem-level working groups. While EMDEs also report high levels of bilateral collaboration (59%), their second most common action is collaboration with regulated entities (46%), exceeding participation in multilateral forums (39%). This suggests that EMDEs place particular emphasis on close, operational interaction with the supervised industry and direct peer-to-peer exchange to enable practical adoption of new technologies.

Together, these patterns show that while authorities across income groups share a common focus on skills, strategy, and system upgrades, the pathways they prioritise reflect differences in institutional maturity, resource availability, and ecosystem dynamics.

Taken together, these actions show that financial authorities are not only responding tactically to immediate operational challenges but are beginning to embed digital transformation within broader institutional frameworks. However, the effectiveness and sustainability of these efforts depend on the strength of the underlying strategies that guide them. Section 2.2 therefore examines how authorities are developing and formalising the strategic foundations of digital transformation — including suptech, data governance, and digital transformation strategies — and assesses the extent to which these frameworks provide coherence, prioritisation, and institutional alignment for the actions described above.

NOTE ON STRUCTURE AND TERMINOLOGY

This report uses the terms ‘strategy,’ ‘roadmap,’ and ‘blueprint’ interchangeably to reflect real-world practice, as financial authorities often combine long-term vision, institutional priorities, and implementation pathways into a single guiding framework.

For analytical clarity, the report distinguishes three interdependent layers of institutional preparedness:

- Section 2.2 analyses the existence and features of strategic frameworks that establish direction, set priorities, and guide the sequencing of actions (the 'what' and the 'how').
- Section 2.3 examines governance frameworks, detailing the internal structures, roles, and processes that support execution and ensure accountability.
- Section 2.4 looks at the practical implementation of these strategies and frameworks, highlighting how financial authorities operationalise institutional plans and translate them into deployed applications and scalable innovations.

This layered approach provides a coherent framework for understanding institutional capacity, despite the diversity in planning terminology.

2.2 The interplay of financial authorities' strategies

The analysis across Section 2.2 shows that financial authorities are advancing strategic planning for digital transformation, data governance, suptech, and AI, but their frameworks remain uneven in scope, content, and institutional integration. Most strategies prioritise operational and technical elements, while cross-framework alignment, governance foundations, and coherent sequencing are used far less consistently. Digital transformation and data governance serve as the primary anchors of institutional modernisation, yet their linkages with suptech and AI are often implicit rather than systematically designed. Emerging domains such as gender-responsive supervision and digital public infrastructure remain peripheral.

Authorities with more developed and better-aligned strategies report fewer obstacles — particularly around data quality, interoperability, and internal coordination — and are more likely to deploy multiple suptech applications. While causality cannot be established, the survey indicates a clear association: coherent strategic planning reduces institutional friction and enables broader supervisory innovation. The findings highlight the value of strategy portfolios that are both comprehensive and integrated, supporting the organisational, data, and technological foundations needed for scalable, intelligence-driven supervision.

Strategic frameworks are increasingly important to how financial authorities organise digital transformation, data use, and supervisory innovation. They provide a shared vision, clarify roles and responsibilities, and help align investments in technology, data, and people. Robust data governance, in particular, plays a key role in underpinning the quality and interoperability of information on which scalable suptech adoption depends.

When strategies are coherent and connected, they are associated with stronger governance and operational coordination, better support for human capital development, and improved technological readiness. When they are absent or fragmented, suptech initiatives are more likely to be ad hoc, underutilised, or difficult to scale.

The subsections that follow examine the content, coverage, and use of six types of strategic frameworks: digital transformation, data governance, suptech, AI, digital public infrastructure (DPI), and gender equality or gender-responsive supervision. They explore how these strategies overlap or complement one another, how widely they are adopted across jurisdictions and regions, what challenges authorities face in developing and implementing them, and how they relate to suptech deployment.

2.2.1 Content and complementarity of strategic frameworks

A review of strategy content across digital transformation, data governance, suptech, AI, gender-responsive supervision, and DPI reveals strong operational focus but limited integration. DX, DG, and ST strategies emphasise digitalisation, system integration, and tool development, yet they seldom cross-reference one another or articulate shared governance or sequencing. AI strategies remain exploratory and only lightly connected to data or supervisory frameworks. Gender and DPI strategies are the least developed and often remain peripheral to core transformation plans. Across domains, governance, resource planning, and monitoring mechanisms appear inconsistently, reducing opportunities for strategies to reinforce each other.

A comparative review of the content of financial authorities' digital transformation, data governance, suptech, AI, gender-responsive supervision, and digital public infrastructure (DPI) strategies points to three broad patterns: (i) strong emphasis on operational and technical elements; (ii) limited cross-referencing and integration between frameworks; and (iii) very selective treatment of gender and DPI. While each strategy reflects its own institutional logic, their contents often overlap or remain disconnected from other domains on which they rely.

FIGURE 18.

Elements of Financial Authorities' Digital Transformation Strategies

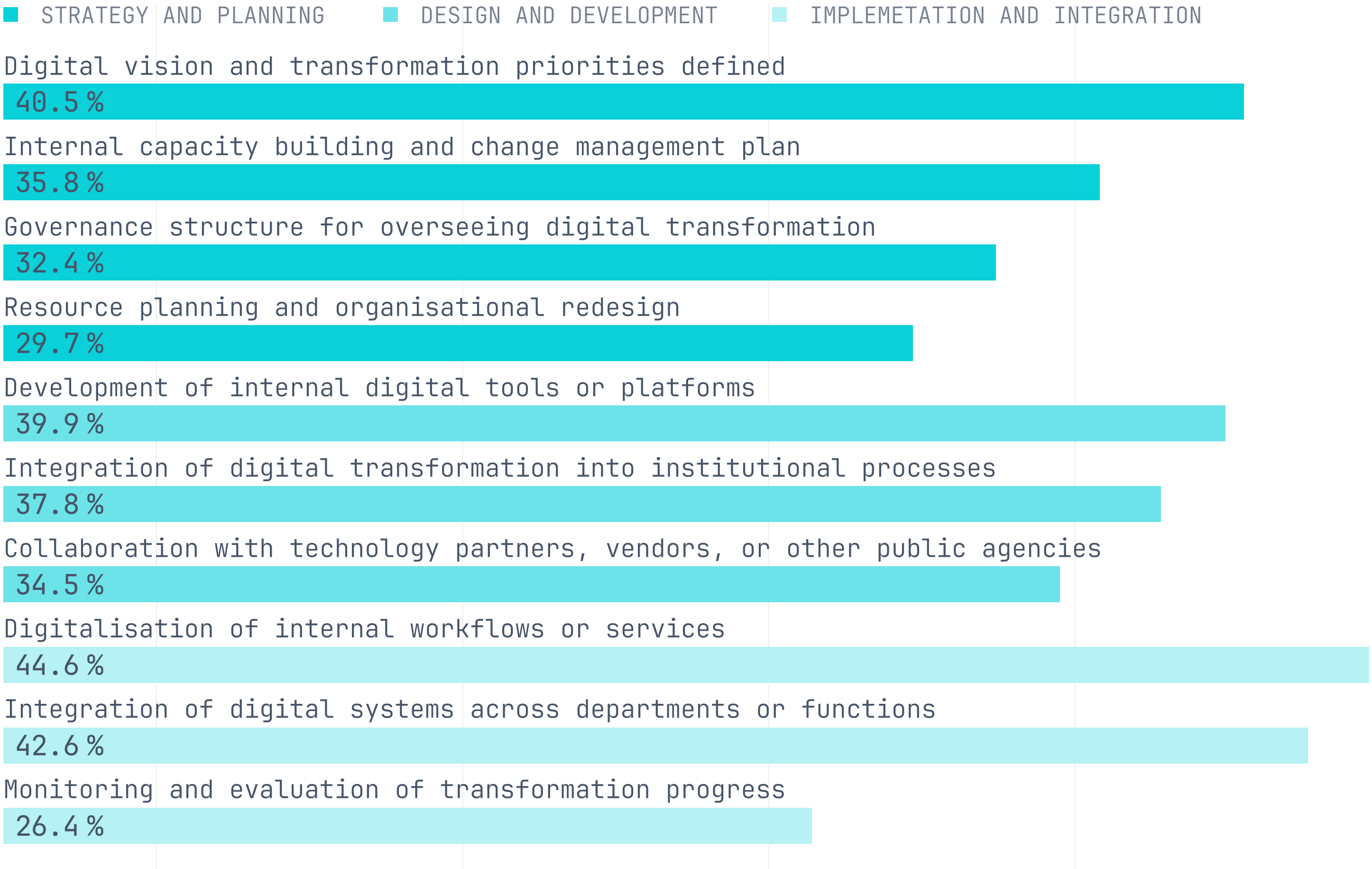
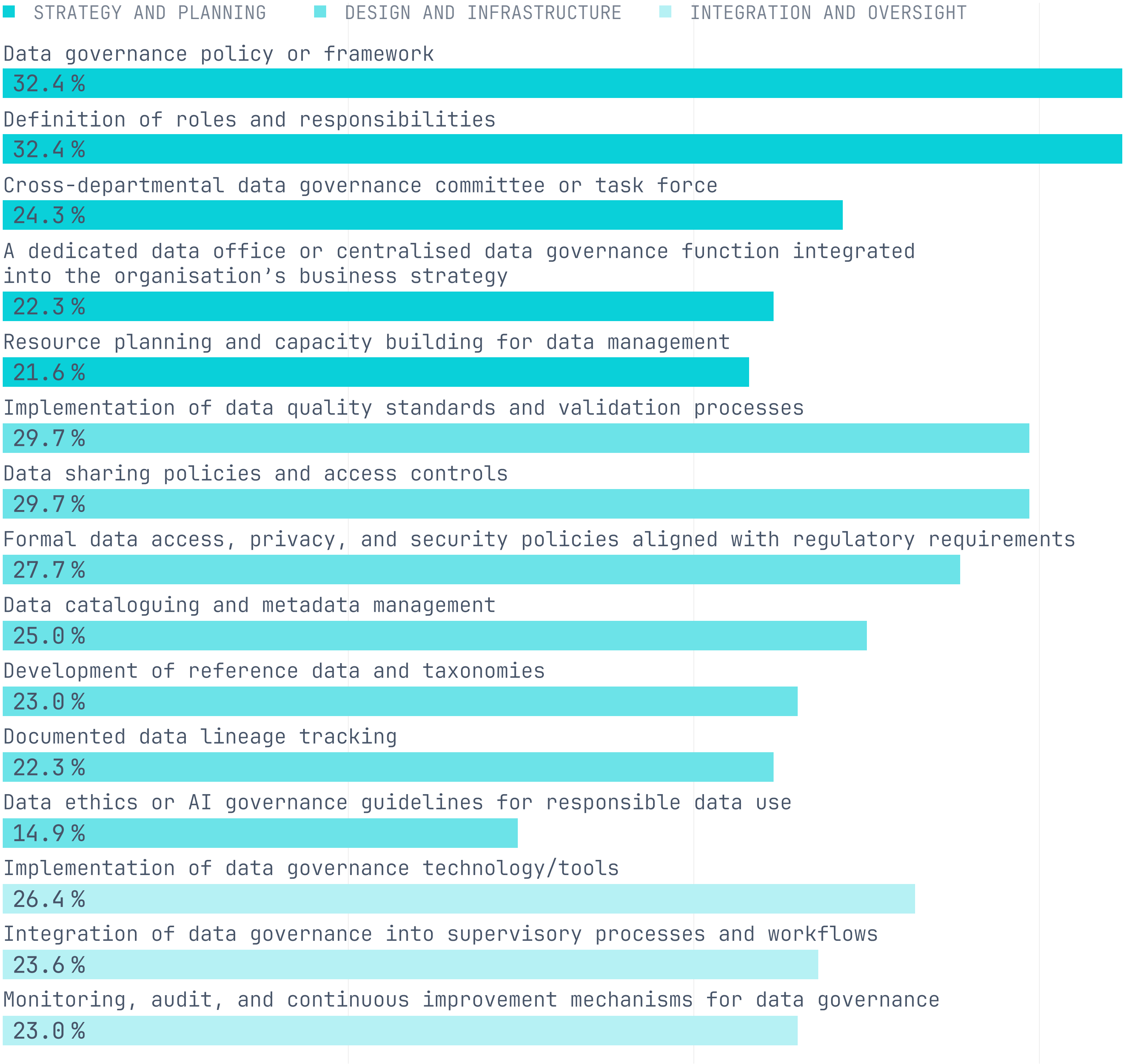


FIGURE 19.

Elements of Financial Authorities' Data Governance Strategies



DIGITAL TRANSFORMATION STRATEGIES

Digital transformation strategies place strong emphasis on execution. Common elements include the definition of a digital vision and priorities, capability development, governance arrangements, and alignment of organisational design and resources. Technical development focuses on internal tool building and collaboration with partners. Implementation centres on workflow digitalisation and system integration, while monitoring mechanisms appear infrequently (Figure 18).

DATA GOVERNANCE STRATEGIES

Data governance strategies often contain selected operational and policy elements—such as data standards, access controls, metadata management, and sharing protocols—but tend to lack comprehensive frameworks that combine policy, accountability, technical infrastructure, and oversight. Many include fragments of data practices without fully articulated governance architecture (Figure 19).

SUPTECH STRATEGIES

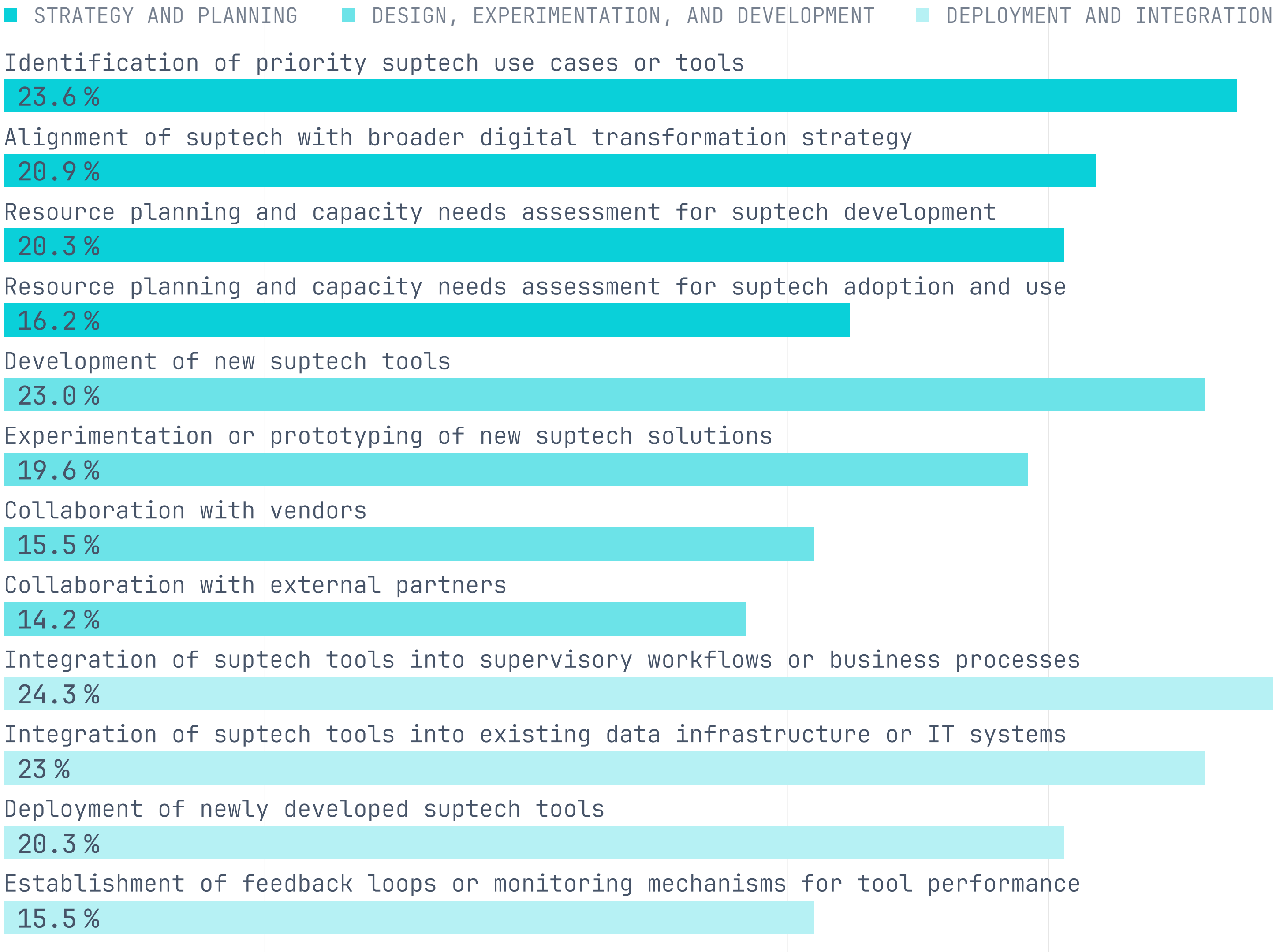
Suptech strategies usually cover a narrow subset of planning, design, and integration elements. Some authorities prioritise use-case selection, prototyping, and collaboration with vendors; others focus on integrating suptech applications into supervisory workflows or existing data infrastructure. Few strategies describe an authority-wide approach, explicit linkages to digital transformation or data-governance frameworks, or detailed mechanisms for feedback and iteration (Figure 20).

AI STRATEGIES

AI strategies are generally exploratory. They reference pilots, model experimentation, and early use cases such as anomaly detection or document processing. Some include elements of governance—internal policies, oversight bodies, or risk management frameworks—

FIGURE 20.

Elements of Financial Authorities’ SupTech Strategies



but these are limited. Connections to data governance, workflow integration, or supervisory functions remain sparse (Figure 21).

GENDER-RESPONSIVE SUPERVISION STRATEGIES

Gender strategies are limited in scope. Elements such as gender-disaggregated data, focal points, capacity building, or gender KPIs appear only occasionally. Gender considerations are present in some financial inclusion strategies but rarely embedded across supervisory planning or data governance (Figure 22).

DIGITAL PUBLIC INFRASTRUCTURE STRATEGIES

Digital public infrastructure refers to foundational digital systems — such as digital identity, payment platforms, and data-exchange layers — that are secure, interoperable, and built on open standards to support the inclusive delivery of public and private services at scale (Figure 23). By enabling seamless integration, paperless processes, and lower transaction costs, DPI accelerates digital transformation across both government and market ecosystems.

FIGURE 21.

Elements of Financial Authorities' AI Strategies

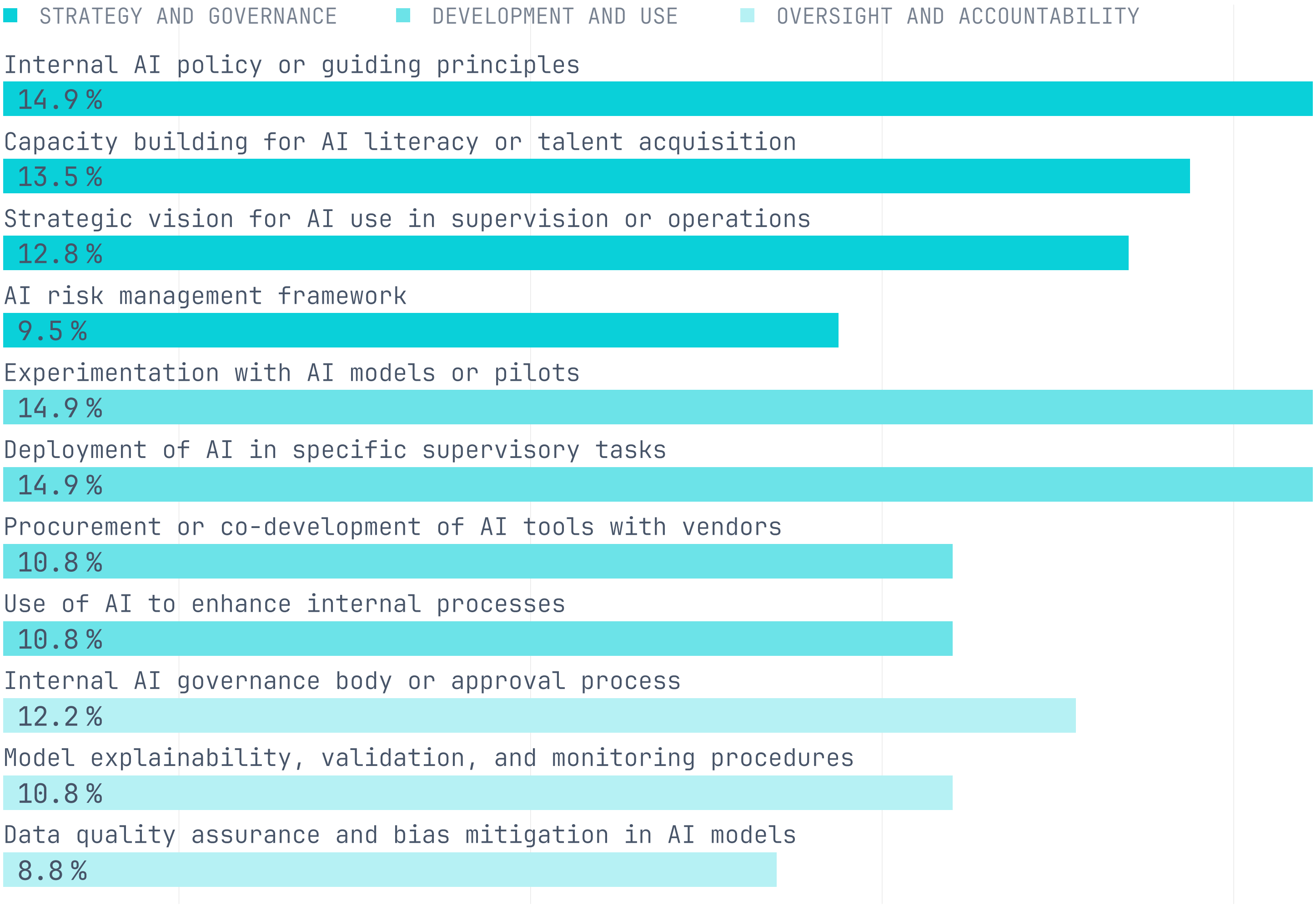
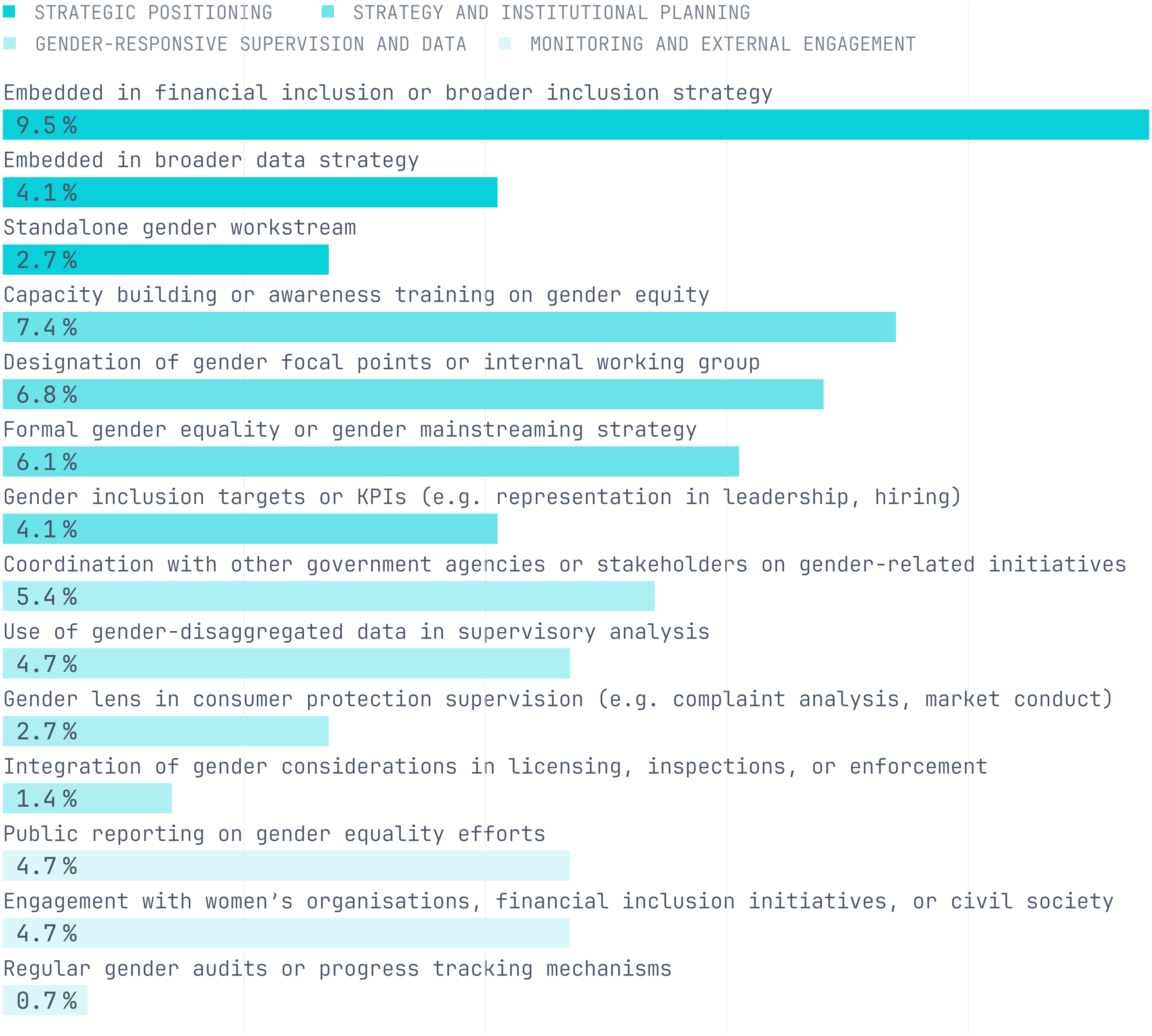


FIGURE 22.

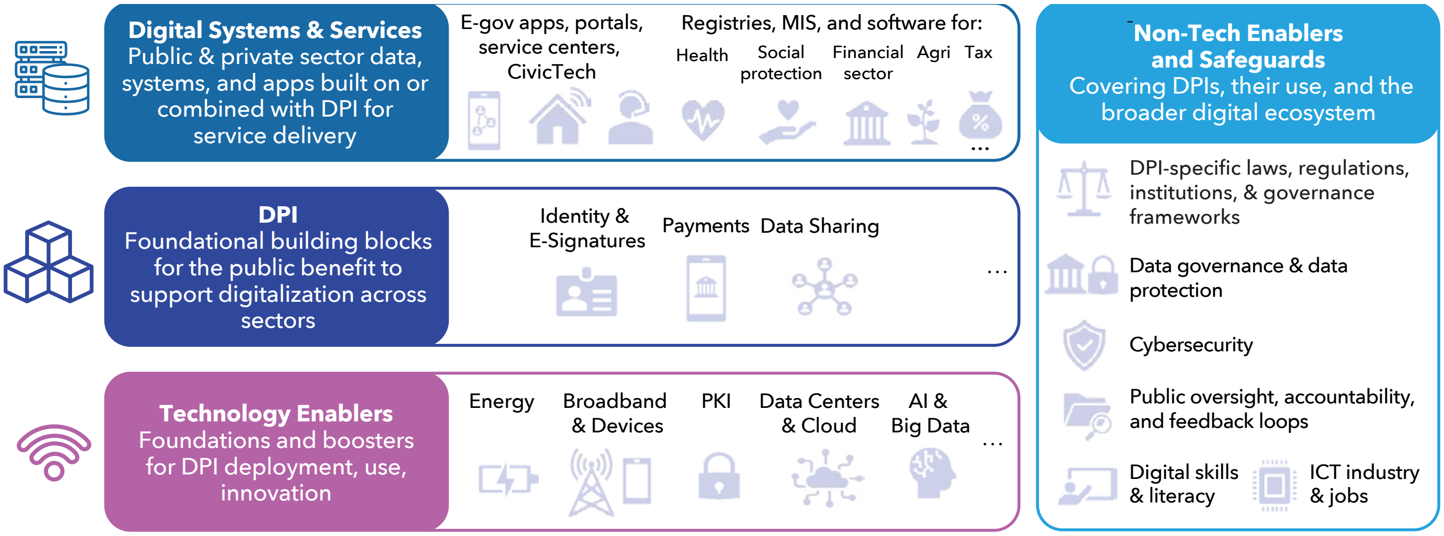
Elements of Financial Authorities' Gender-Responsive Supervision Strategies



For financial authorities, DPI is increasingly relevant to supervision. Secure and portable digital identity supports e-KYC and real-time verification. Interoperable data-exchange layers enable automated reporting, cross-agency intelligence flows, and more reliable risk monitoring. Modern payment infrastructures generate high-frequency transaction data essential for AML/CFT, fraud detection, consumer-protection oversight, and financial inclusion analysis. In this sense, DPI forms a foundational layer that directly affects the granularity, timeliness, and reliability of the datasets upon which suptech depends. Global policy agendas — including the World Bank's 2025 DPI guidance — increasingly frame DPI as a public good that strengthens regulatory capacity and financial-integrity systems by improving traceability, data quality, and cross-institutional interoperability.

FIGURE 23.

Broader DPI Ecosystem


Digital Systems & Services
Public & private sector data, systems, and apps built on or combined with DPI for service delivery
E-gov apps, portals, service centers, CivicTech
Registries, MIS, and software for:
Health
Social protection
Financial sector
Agri
Tax
...
DPI
Foundational building blocks for the public benefit to support digitalization across sectors
Identity & E-Signatures
Payments
Data Sharing
...
Technology Enablers
Foundations and boosters for DPI deployment, use, innovation
Energy
Broadband & Devices
PKI
Data Centers & Cloud
AI & Big Data
...
Non-Tech Enablers and Safeguards
Covering DPIs, their use, and the broader digital ecosystem
DPI-specific laws, regulations, institutions, & governance frameworks
Data governance & data protection
Cybersecurity
Public oversight, accountability, and feedback loops
Digital skills & literacy
ICT industry & jobs

SOURCE: WORLD BANK, 2025

DPI strategies remain highly selective, focusing on capacity building, engagement with national DPI initiatives, or identifying supervisory roles. Operational references to identity systems, payment infrastructure, or data exchange platforms are present but limited. Few strategies articulate how DPI should support supervisory data flows, reporting, or verification processes (Figure 24).

The analysis below examines how the substance of these strategies aligns — or fails to align — across transformation efforts. There several overlaps and complementarities across strategic frameworks:

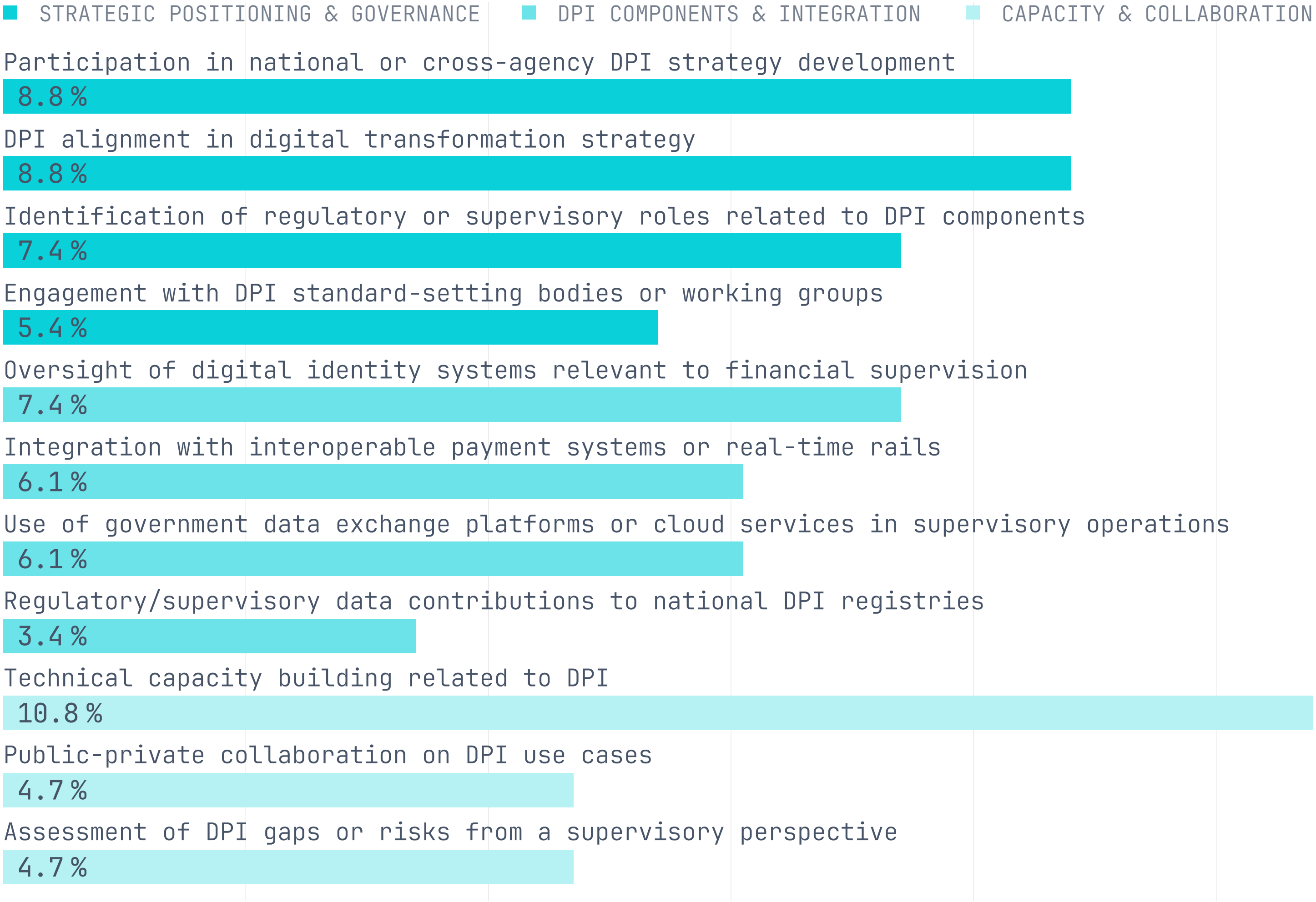
Strong operational overlap across core strategies. Across digital transformation (DX), data governance (DG), suptech (ST), and AI strategies, authorities repeatedly emphasise technical delivery: digitalising workflows, integrating systems, developing tools, or piloting applications. This pattern is consistent across domains and suggests that authorities tend to approach strategy through a technology-first lens. While this supports rapid implementation, it also increases the risk of fragmented efforts when technical development is not anchored in shared governance, standards, or sequencing frameworks.

Complementarity between DX, DG, and ST is conceptually strong but weakly expressed. DX, DG, and ST strategies should reinforce one another: DX provides institutional alignment, DG establishes data quality and interoperability, and ST applies these enablers to supervisory practice. However, the content of strategies shows only limited cross-referencing. Few suptech strategies reference DX or DG; DX strategies seldom incorporate data governance as a foundational pillar; and DG strategies rarely articulate downstream implications for supervisory technology. The complementarities exist in principle but remain largely underused.

AI strategies depend on DG and ST but rarely connect to them. AI strategies reference pilots and experimentation, but seldom include the data governance, workflow integration, or supervisory use-case prioritisation on which AI deployment relies. Their content does not yet reflect explicit links to DG or ST strategies. Without these connections, there is a risk that

FIGURE 24.

Elements of Financial Authorities' DPI Strategies



AI initiatives develop in isolation, disconnected from the systems, data integrity, and supervisory objectives required for meaningful application.

Gender and DPI strategies remain peripheral and disconnected. Both gender-responsive supervision and DPI strategies contain few elements and demonstrate minimal integration with the main transformation domains. Gender considerations are only occasionally embedded in inclusion or data strategies, and DPI efforts rarely appear linked to DX, DG, or ST plans, despite their potential to support secure identity verification, automated reporting, and cross-agency data exchange. Their peripheral treatment may limit opportunities for broader impact.

Gaps in governance, sequencing, and monitoring appear to weaken complementarities. Across strategy types, governance structures, resource planning, and monitoring and learning mechanisms appear inconsistently. This lack of common building blocks reduces the potential for strategies to reinforce one another. Without shared governance, cross-domain coordination is limited; without sequenced planning, technical workstreams emerge independently; and without monitoring, institutions struggle to steer or course-correct their transformation efforts.

Taken together, the content of these strategies illustrates three overarching dynamics:

1. Operational overlaps are strong, especially in digitalisation and tool development.
2. Complementarities are present but underused, particularly across DX, DG, ST, and AI.
3. Peripheral domains — gender and DPI — remain disconnected, limiting their contribution to supervisory effectiveness.

The next step for many authorities is not merely to expand strategy content but to better align the building blocks across domains. More coordinated planning — supported by diagnostics, cross-departmental governance, and shared monitoring mechanisms — could help digital transformation, data governance, suptech, and AI strategies reinforce each other rather than evolve in parallel.

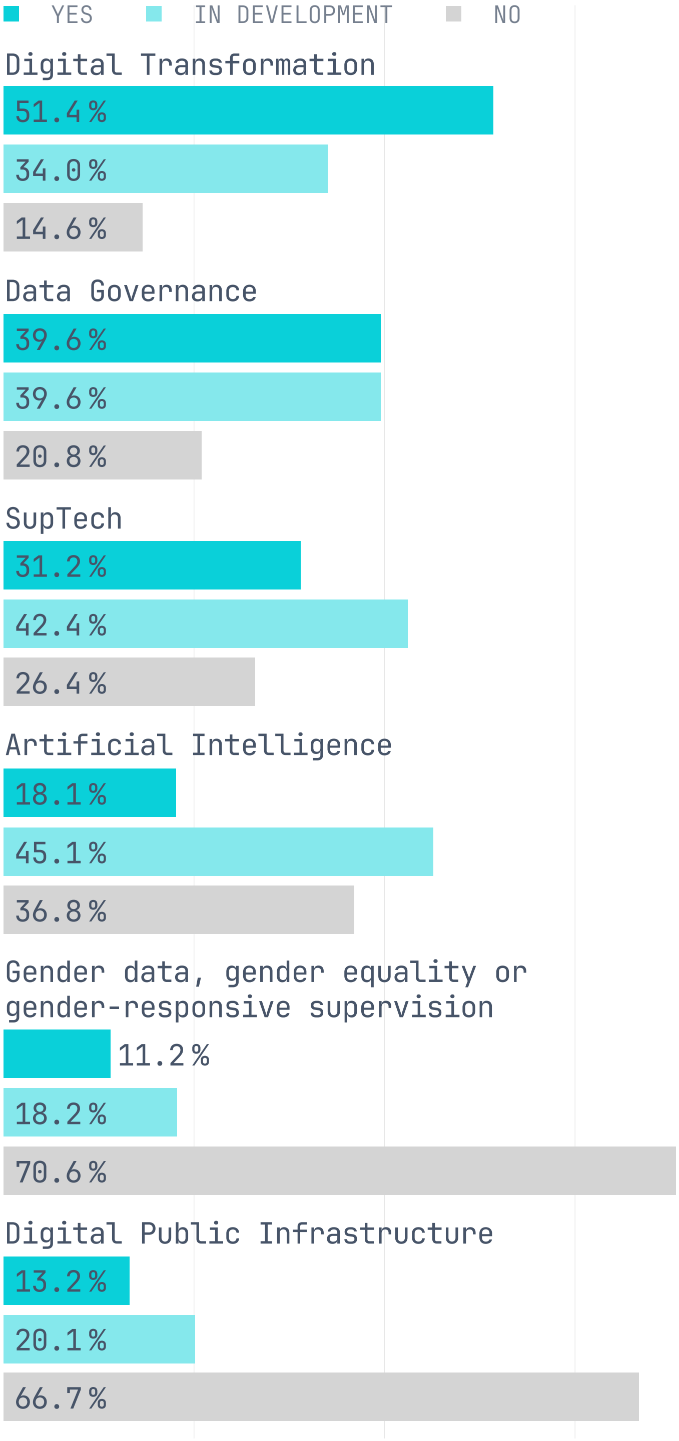
2.2.2 Maturity of strategic frameworks

Strategic planning for digital transformation is advancing, but maturity varies widely across frameworks. Digital transformation and data governance are the most established, with over half of authorities reporting operational strategies or roadmaps. Suptech strategies are progressing more slowly, with around one-third operational and a similar share still in development. AI governance remains at an early stage, and most authorities lack gender equality or DPI strategies. Across all frameworks, AEs report higher operational maturity, while EMDEs show strong intent but slower institutionalisation. Regionally, NA, EAP, and SSA demonstrate the strongest adoption of DX and DG frameworks, whereas SA and ECA show the highest shares without foundational strategies.

The 2025 survey shows that strategic planning is progressing, but maturity varies significantly across frameworks (Figure 25).

FIGURE 25.

Adoption of Core Strategic Frameworks Across Financial Authorities



SUPTECH STRATEGY

Financial authorities are developing structured, institution-wide plans to guide suptech adoption and enhance supervisory efficiency, effectiveness, and adaptability. These strategies define objectives linked to supervisory outcomes, establish governance arrangements, outline data integration and capacity-building requirements, and increasingly embed agile development and human-centred design principles. Alignment with broader data governance frameworks ensures interoperability, data quality, and institutional coherence.

In 2025, less than a third of surveyed authorities (31%) reported having an operational suptech strategy or roadmap. The largest group (42%) had a strategy in development, signalling strong near-term commitment to formalising their approach, while just over a quarter (26%) reported having no suptech strategy at all.

Historical comparison shows slow but steady progress: 23% of authorities had a suptech strategy or roadmap in 2022, rising to 29% in 2024 and 31% in 2025. These figures indicate recognition of suptech as a strategic priority, though formal institutionalisation remains uneven and gradual.

DATA GOVERNANCE STRATEGY

A data governance strategy provides a comprehensive framework to ensure the quality, security, accessibility, interoperability, and ethical use of data across all functions of a financial authority. Robust data governance underpins AI readiness and suptech deployment and typically incorporates data architecture, stewardship, access controls, quality assurance, and cybersecurity, often under the oversight of a senior executive.

In 2025, 40% of surveyed authorities reported having an operational data governance strategy or roadmap. A further 40% had a strategy in development, while only 21% reported having no formal framework.

Compared to 2024, when 37% had an adopted strategy and 39% were developing one, the data indicates steady progression toward operationalising data governance. Most authorities are now either implementing or actively building data governance frameworks, indicating its status as a key institutional priority.

DIGITAL TRANSFORMATION STRATEGY

A digital transformation strategy provides a high-level institutional roadmap guiding how financial authorities modernise their operations, infrastructure, and workforce to remain agile, responsive, and effective in an increasingly digital financial system. It often serves as an umbrella for more specialised frameworks, including suptech, data governance, and emerging AI governance protocols.

In 2025, just over half of surveyed authorities (51%) reported having an operational digital transformation strategy or roadmap, representing a significant rise from the previous year. A further 34% had a strategy in development, while only 15% reported having none.

This trend aligns with the 2024 results: that year, 39% of authorities reported an adopted digital transformation strategy, compared with 51% operational in 2025; and 41% were developing one in 2024, many of which subsequently entered operational status. The data suggests that digital transformation strategies are becoming increasingly institutionalised.

AI & ML GOVERNANCE STRATEGY

AI and ML governance is an emerging priority as supervisory tools increasingly rely on AI for risk scoring, fraud detection, market surveillance, and other analytical functions. These developments intersect closely with data governance to ensure quality, accountability, and ethical use.

In 2025, only 18% of surveyed agencies reported having an operational AI strategy or roadmap. A larger share (45%) had one in development, indicating growing attention to formal governance structures. Over a third (37%) reported having no AI strategy at all, confirming that AI governance remains at an early stage for many authorities.

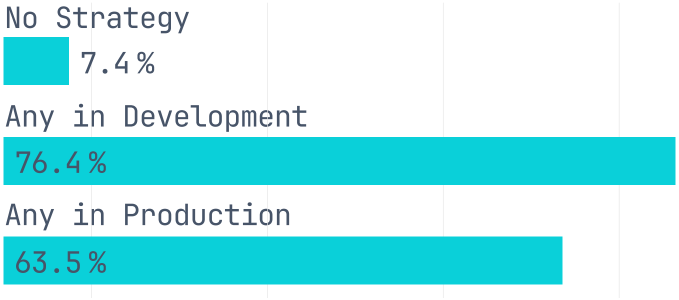
GENDER EQUALITY OR GENDER-RESPONSIVE SUPERVISION

Gender equality and gender-responsive supervision are increasingly recognised as important elements of inclusive financial oversight. Integrating gender considerations can help ensure that supervisory policies and outcomes are equitable and sensitive to differential impacts across demographic groups.

Despite this, formal frameworks remain limited: 71% of authorities reported no strategy or roadmap related to gender equality or gender-responsive supervision. Only 11% had an operational strategy, while 18% had one in development. The findings indicate that gender-responsive supervision has not yet become a mainstream strategic priority.

FIGURE 26.

Distribution of Authorities by Number of Adopted or Developing Strategies



DIGITAL PUBLIC INFRASTRUCTURE (DPI)

DPI remains the least mature strategic area within financial authorities in 2025. A clear majority (67%) report having no DPI strategy or roadmap, while 13% have an operational strategy and 20% are developing one. This gap may reflect the fact that DPI is typically led by central government digital agencies, rather than supervisors, even though financial authorities depend on DPI's robustness and interoperability for effective suptech deployment. As a result, the institutionalisation of DPI within supervisory strategies remains nascent.

As national DPI agendas expand, opportunities will grow for financial authorities to integrate more fully into unified digital ecosystems — environments where identity, payments, reporting, and data exchange operate seamlessly across the public and private sector. This deeper integration could, over time, provide the infrastructural uplift needed for more scalable, data-rich, and intelligence-driven supervision.

The distribution of strategies across financial authorities (Figure 19) reveals a landscape where most agencies have begun formalising their digital ambitions, yet adoption remains uneven and fragmented.

Across all strategic areas, 63.5% of financial authorities report having at least one operational strategic framework, and an even greater share, 76%, have at least one strategy in development (Figure 26). Only 7% of respondents report having no strategy of any kind, indicating broad recognition that structured planning is important for modern regulation and supervision. Notably, based on our analysis 26% of all authorities developing strategies are doing so for the first time, adding to the 35% identified last year. This points to a continuing wave of first-generation institutional formalisation, with a significant share of authorities only now establishing their foundational strategic frameworks.

FIGURE 27.

Combination of Adopted Strategic Frameworks

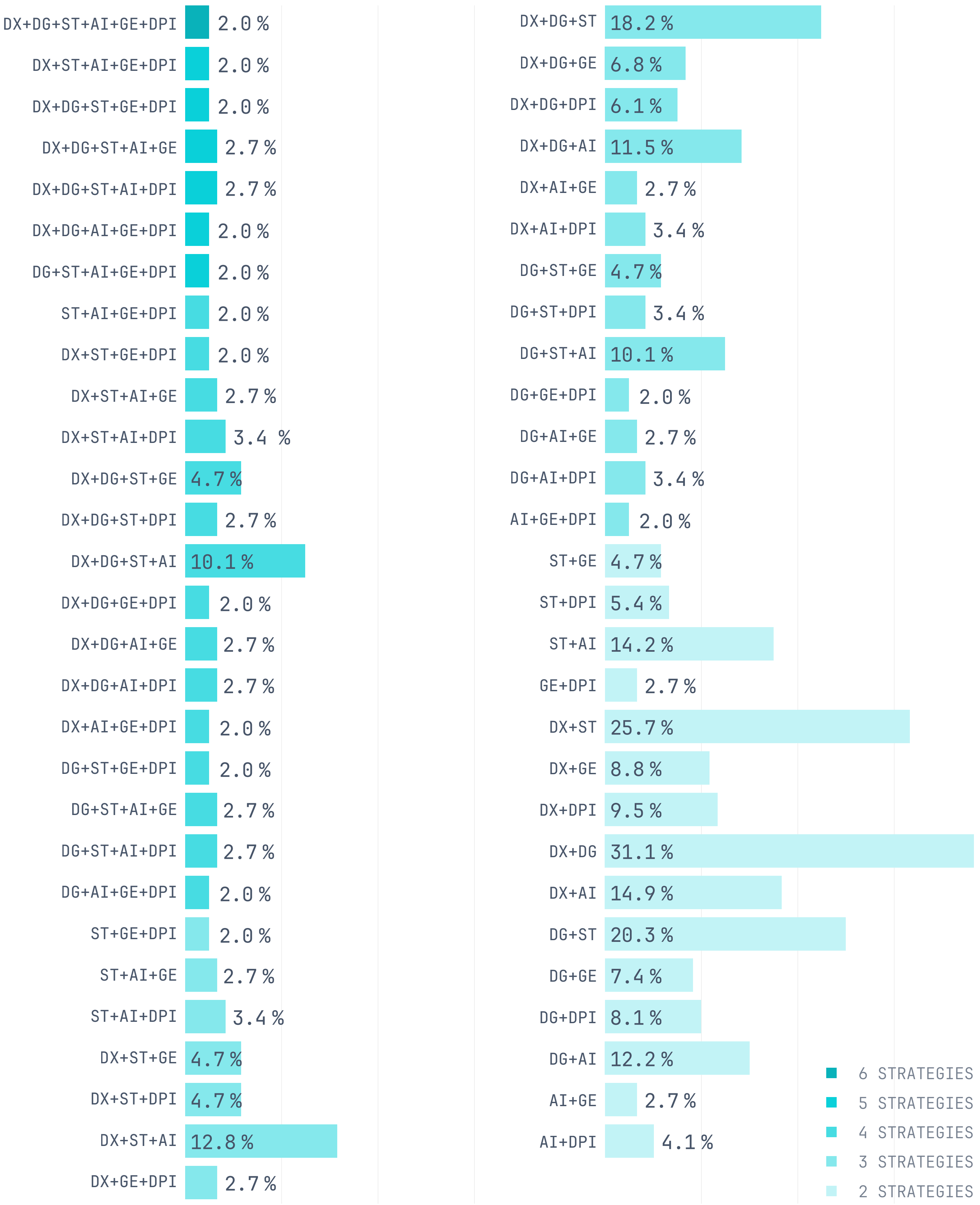


Figure 27 shows that strategic frameworks tend to cluster in predictable patterns. The most common combinations involve exactly two strategies, with digital transformation and data governance forming the backbone of most authorities' planning efforts. These core strategies appear in nearly all of the larger clusters, indicating that institutions typically establish organisation-wide digital priorities and data governance foundations before expanding into more specialised domains.

Three-strategy combinations represent the next major grouping, usually adding either suptech or AI on top of DX and DG. These patterns suggest that supervisory innovation frameworks are generally layered only after core organisational and data priorities are in place.

Combinations involving four or more strategies are less common and include gender equality and digital public infrastructure only in a small minority of cases. GE and DPI thus remain peripheral and are typically adopted only by authorities with already extensive strategic portfolios.

Overall, the chart highlights a common sequencing pattern: foundational strategies (DX and DG) appear first; operationally focused strategies (ST and AI) follow; and specialised or cross-cutting strategies (GE and DPI) are adopted only by a small group of authorities pursuing broad, multi-domain transformation.

The comparative analysis of strategic frameworks across AEs and EMDEs reveals notable differences in maturity, readiness, and strategic prioritisation (Figure 28). Overall, AEs demonstrate higher levels of operationalisation across core digital domains, while EMDEs show strong intent but face persistent capacity and resource constraints that slow implementation.

Across all strategic domains, the charts clearly show that AEs consistently demonstrate higher operational maturity, particularly in digital transformation and data governance. EMDEs exhibit high rates of strategies in development across most domains, signalling strong intent, but also face larger structural gaps, especially in AI and data governance. Suptech strategies are maturing slowly and in parallel across both groups, reflecting their growing importance yet still-limited institutionalisation. Gender equality and DPI remain the least developed areas in both AEs and EMDEs. The largest strategic divides appear in AI and data governance, where EMDE readiness lags significantly.

These patterns underscore the importance of sequencing strategic frameworks. AEs tend to establish data governance and digital transformation frameworks first, creating the foundations for AI and suptech institutionalisation. EMDEs often enter these domains simultaneously, which can dilute focus and stretch institutional capacity.

Digital transformation (DX): broad adoption but uneven maturity. Digital transformation is the most mature strategic area for both groups, although the gap in operational readiness is substantial. These results indicate that although EMDEs are progressing, they remain behind AEs in adopting institution-wide digital transformation frameworks capable of supporting scaled technological change.

- AEs: 67% have an operational DX roadmap, and only 11% lack any strategy.
- EMDEs: 48% operational and 37% in development, while 15% remain without a strategy.

Data governance (DG): widespread recognition but slower institutionalisation in EMDEs. Data governance is a core strategic priority across groups, yet AEs again show a significantly higher degree of implementation. The quarter of EMDE agencies lacking a DG roadmap may represent a structural vulnerability, given the foundational role of data quality, interoperability, and stewardship for both suptech and AI adoption.

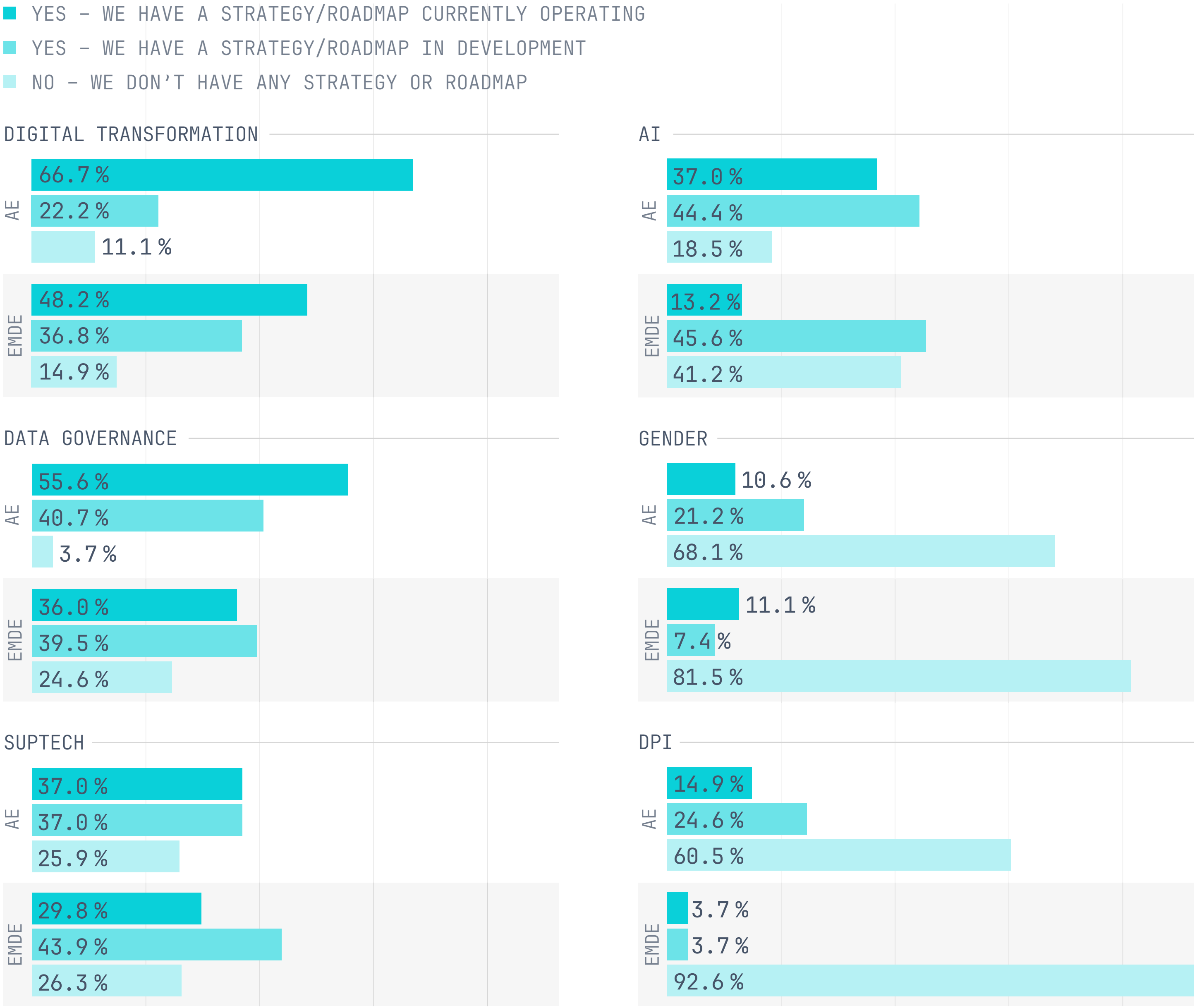
- AEs: 56% operational, 41% developing, and small number without any DG framework.
- EMDEs: 36% operational, 40% developing.

Suptech (ST): strong intent but slow global formalization. Suptech strategic planning remains moderate in both groups. The figures indicate growing recognition of suptech's importance, but also that institutionalisation remains a work in progress globally.

- AEs: 37% operational, 37% in development, and 26% without a strategy.
- EMDEs: 30% operational, 44% in development, and 26% without any strategy.

FIGURE 28.

Strategies By Economic Classification



Artificial intelligence (AI): rapidly emerging priority with wide gaps in readiness. AI strategy is the most uneven and fragmented domain across groups. The high share of EMDEs without an AI strategy points to substantial challenges in articulating and operationalising AI governance — challenges that pose direct constraints to AI-enabled suptech adoption.

- AEs: 37% operational, 44% in development.
- EMDEs: Only 13% operational, 45% in development, and almost half have no framework at all.

Gender equality (GE): minimal strategic integration globally. Strategic planning for gender equality or gender-responsive supervision is the least developed area overall. These data show that gender considerations remain highly under-institutionalised across supervisory frameworks, with only marginal differences between economic groups.

- AEs: 81.5% have no strategy, 11% developing one, and 7% operational.
- EMDEs: 68% no strategy, 21% developing, and 11% operational.

Digital public infrastructure (DPI): low engagement, mostly in EMDEs. DPI is the least mature strategic area for both groups, with extremely low adoption in AEs. EMDEs show more engagement, likely linked to national DPI initiatives.

- AEs: 93% have no DPI strategy; only 7% operational or in development.
- EMDEs: 60% have no strategy, 25% in development, and 15% operational.

Regional differences in strategic readiness reveal uneven progress across supervisory jurisdictions (Figure 29). While the overall global pattern mirrors the AE–EMDE divide, the regional breakdown provides a more nuanced picture of where strategic institutionalisation is advancing and where gaps remain.

Across regions, the data show a three-tier pattern of strategic maturity:

1. High maturity: North America, EAP, and Sub-Saharan Africa in DX and DG.
2. Mid-maturity: Latin America & the Caribbean and MENA, where strategies are primarily in development rather than operational.
3. Low maturity: South Asia and ECA, where large shares of agencies lack foundational DX or DG strategies.

DIGITAL TRANSFORMATION (DX) AND DATA GOVERNANCE (DG): STRONGEST IN NA, EAP, AND SSA

Digital transformation and data governance show the highest levels of operational adoption in NA and EAP, where a majority of respondents report operational roadmaps. Sub-Saharan Africa also records comparatively strong operational adoption of DX strategies, reflecting momentum in broader public-sector digitalisation across the region.

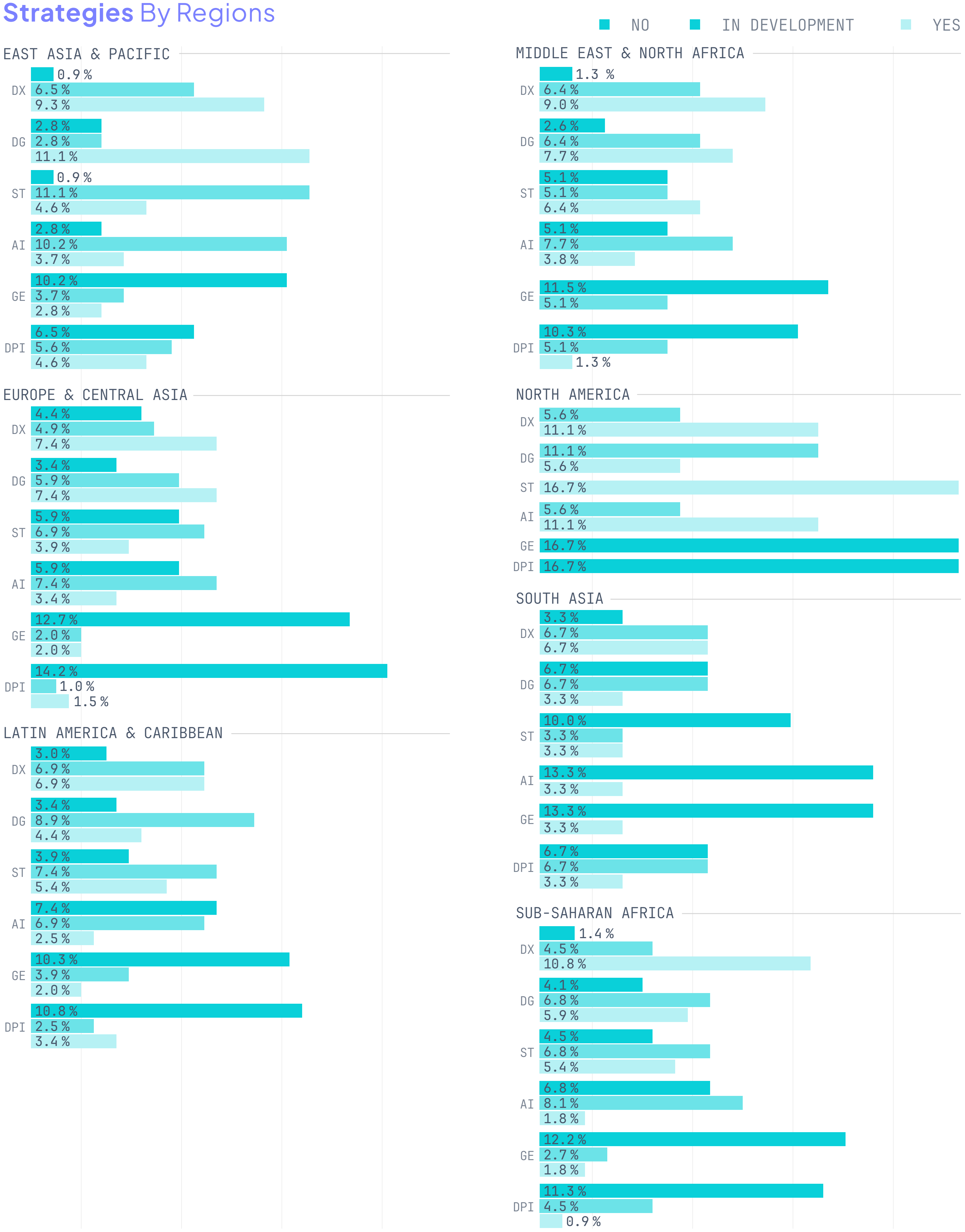
In contrast, ECA displays the highest share of agencies without a digital transformation strategy, while SA shows the largest percentage lacking a data governance framework. These gaps point to foundational weaknesses that may slow downstream implementation of suptech and AI.

SUPTECH (ST) AND ARTIFICIAL INTELLIGENCE (AI): WIDESPREAD INTENT, SLOWER EXECUTION

Suptech and AI strategies follow a similar pattern across regions:

FIGURE 29.

Strategies By Regions



- NA shows the strongest concentration of operational ST and AI strategies.
- SA displays the highest proportion of agencies without either strategy.
- LAC and MENA show moderate levels of strategies in development, signalling intent but slower institutionalisation.

Across all regions, the share of agencies with strategies in development is larger than the share with strategies fully operational.

GENDER EQUALITY (GE) AND DIGITAL PUBLIC INFRASTRUCTURE (DPI): LOWEST MATURITY GLOBALLY

Engagement with gender equality and DPI is uniformly low across all regions.

- NA reports no operational or in-development strategies for either GE or DPI.
- Most regions show only minimal activity, with "no strategy" overwhelmingly dominating GE and DPI categories.

These results indicate that GE and DPI remain the least institutionalised strategic domains within supervisory authorities globally, regardless of region.

2.2.3 Challenges in designing and implementing strategies

The 2025 survey shows that financial authorities face distinct challenges at both the design and implementation stages of digital transformation, data governance, suptech, and AI strategies. Strategy formulation is most affected by limited internal expertise and difficulties achieving cross-departmental alignment, alongside gaps in data, benchmarks, and leadership sponsorship. Implementation challenges are dominated by persistent siloed structures, budget and procurement constraints, and weak change-management and communication practices, with staff turnover and limited monitoring tools further complicating execution.

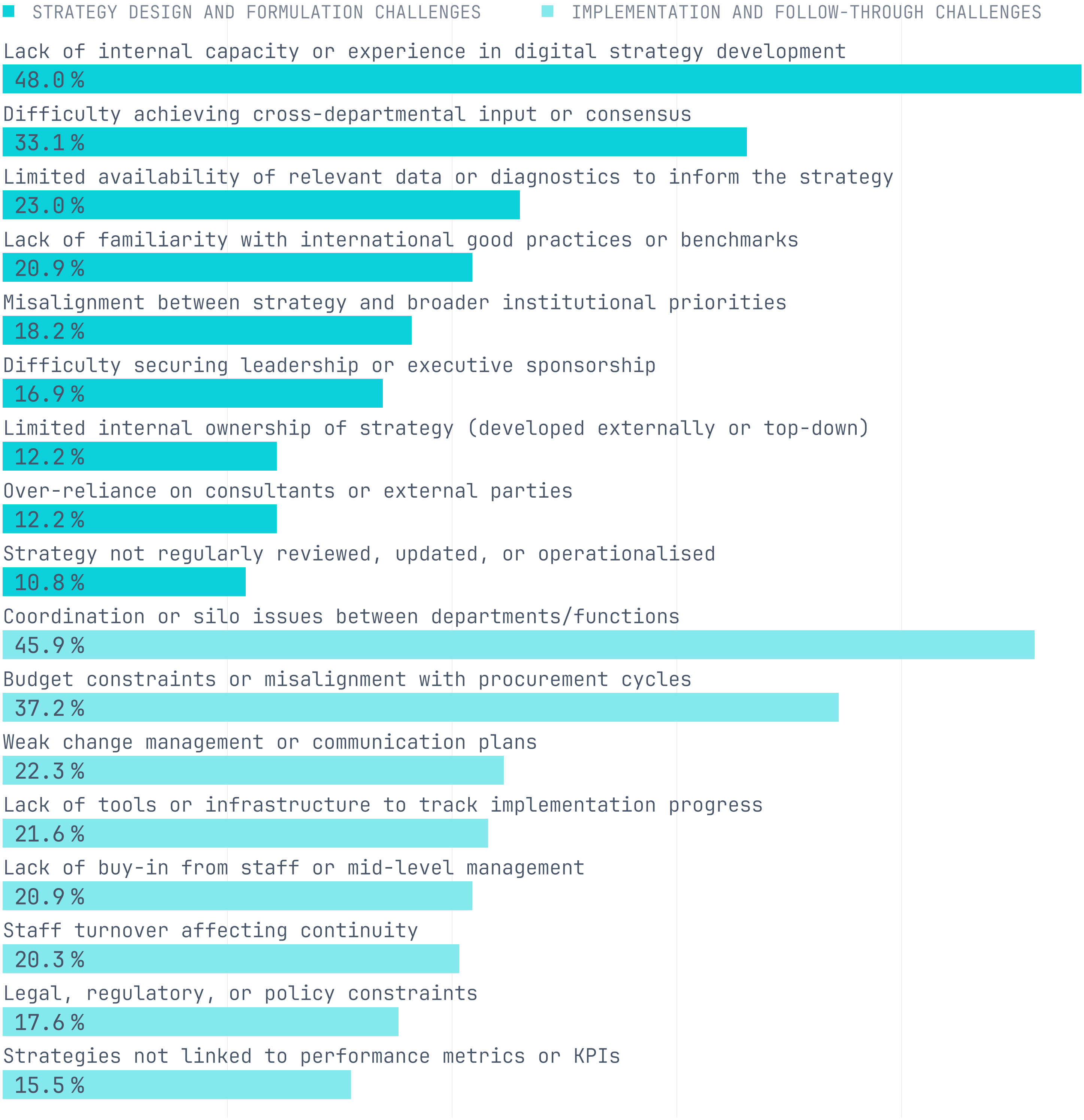
Financial authorities face significant challenges in both the design and implementation of digital transformation, data governance, suptech, and AI strategies (Figure 30). The most substantial barrier at the strategy design stage is the lack of internal capacity or experience in digital strategy development (48%). This skills gap is compounded by difficulty achieving cross-departmental input or consensus (33%), reflecting early coordination frictions. Other notable design-stage obstacles include limited availability of relevant data or diagnostics to inform strategic planning (23%), insufficient familiarity with international good practices or benchmarks (21%), misalignment between strategy and broader institutional priorities (18%), and challenges securing leadership or executive sponsorship (17%).

Once strategies are formulated, execution becomes significantly harder. The most persistent implementation barrier is inter-departmental fragmentation: 46% cite coordination or silo issues as the main impediment to follow-through. Financial constraints also loom large, with budget limitations or misaligned procurement cycles affecting 37% of authorities. Weak change-management and communication practices (22%) and a lack of tools or infrastructure to track implementation progress (22%) further hinder execution. Staff buy-in challenges (21%) and turnover (20%) add operational instability.

These findings highlight two core structural weaknesses: limited internal strategic expertise during design, and entrenched organisational fragmentation and resource constraints during execution. Without targeted improvements in

FIGURE 30.

Challenges in Designing and Implementing Strategic Frameworks



institutional capacity, governance, and cross-departmental coordination, even well-designed strategies risk stalling before they translate into meaningful transformation.

2.2.4 Strategy development

Financial authorities use several sequencing models to develop digital transformation, data governance, suptech, and AI strategies. The most common approach is diagnostics-first, followed by strategy-first planning and iterative, pilot-informed development. A smaller share aligns strategy work with wider government digital initiatives or adopts phased or budget-linked processes. Strategy formation is largely internally driven, with IT units, cross-departmental teams, and senior leadership playing central roles, complemented by targeted support from consultants, vendors, multilaterals, and peer institutions. Collaboration is widespread, relying on task forces, peer-learning networks, and self-assessments. Most authorities still use traditional documentation tools for strategy development, though some are beginning to adopt more integrated digital platforms.

How do authorities overcome the challenges outlined in the previous subsection and actually develop these strategies? Understanding the timing, processes, and institutional arrangements behind strategy formation is essential for interpreting both the maturity patterns observed across jurisdictions and the correlation between strategic planning and suptech deployment

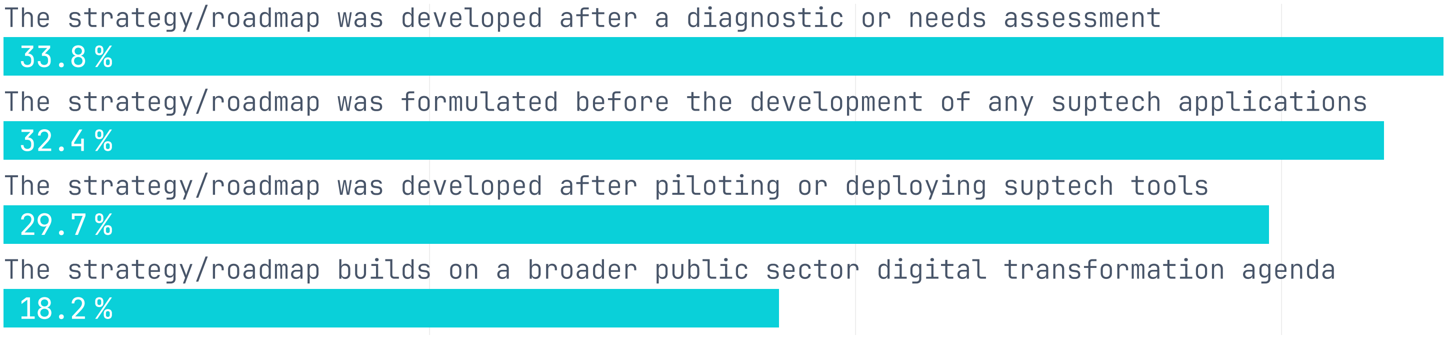
Financial authorities adopt diverse approaches to developing digital transformation, data governance, suptech, and AI strategies, with choices shaped by institutional maturity, leadership commitment, resource availability, and wider public-sector dynamics. The most common approach (34%) is **diagnostics-first**, where authorities design strategies after conducting assessments to identify capability gaps, risks, and priorities (Figure 31). This evidence-based sequencing helps anchor strategy in institutional reality and often results in clearer prioritisation and more credible implementation plans.

A slightly smaller share (32%) follows a **planning-first approach**, establishing strategies before pilots or projects. These frameworks typically set out high-level objectives, governance structures, and resource pathways, guiding subsequent operational decisions. This is often visible in authorities with established digital or data units.

Nearly 30% adopt an **iterative, experience-informed approach**, formulating strategies after pilots or proofs of concept. In these cases, experimentation provides practical insights that inform strategy design and help build internal

FIGURE 31.

Strategic Frameworks Development Timeline



buy-in. This model is common in authorities where early pilots are driven by specific supervisory needs or donor-funded initiatives.

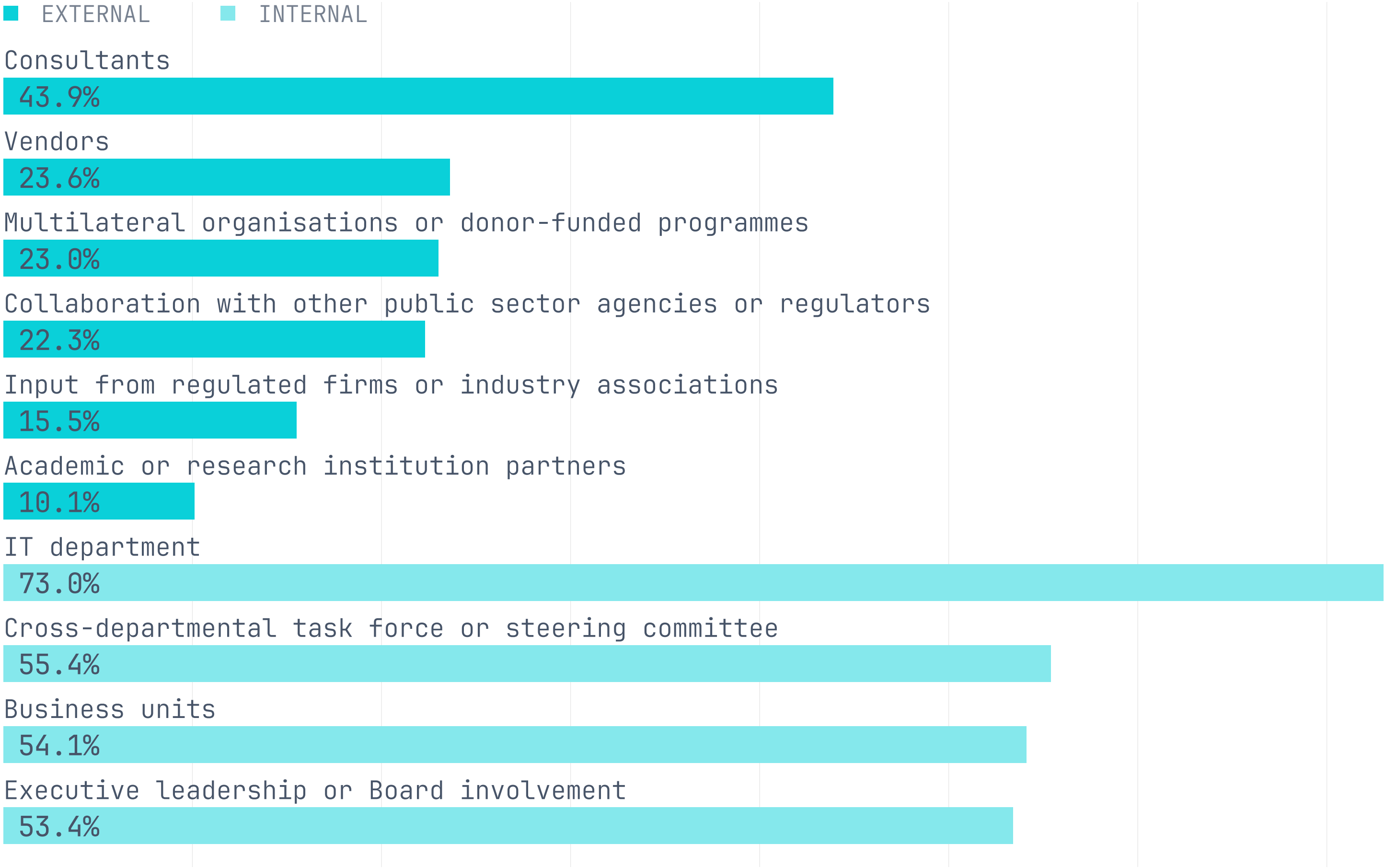
A smaller group (18%) align strategy development with broader public-sector digitalisation initiatives. This can bring advantages, like shared infrastructure and coordinated governance, but may limit sector-specific innovation if the financial authority has limited control over the overarching design.

An additional 8% report "other" approaches, including phased strategy development, staggered implementation linked to budget cycles, or incremental updates to earlier technology plans. These variations reflect differences in institutional culture, regulatory context, and the degree of urgency driving digital reform.

A few broad lessons emerge from the evidence. Authorities succeed through different sequencing models — diagnostics-first, strategy-first, or pilot-first — provided the approach remains coherent and execution is consistent. Strategies are most effective when aligned: digital transformation, data governance, and suptech frameworks reinforce one another and reduce fragmentation, whereas isolated planning often results in narrow or duplicated efforts. Ultimately, institutional capacity remains decisive. Even well-designed strategies struggle without sufficient human capital, strong data foundations, and effective governance. Continuous adjustment also proves important, as authorities refine strategies in response to institutional learning and evolving supervisory needs.

FIGURE 32.

Internal and External Actors Involved in Strategic Framework Development

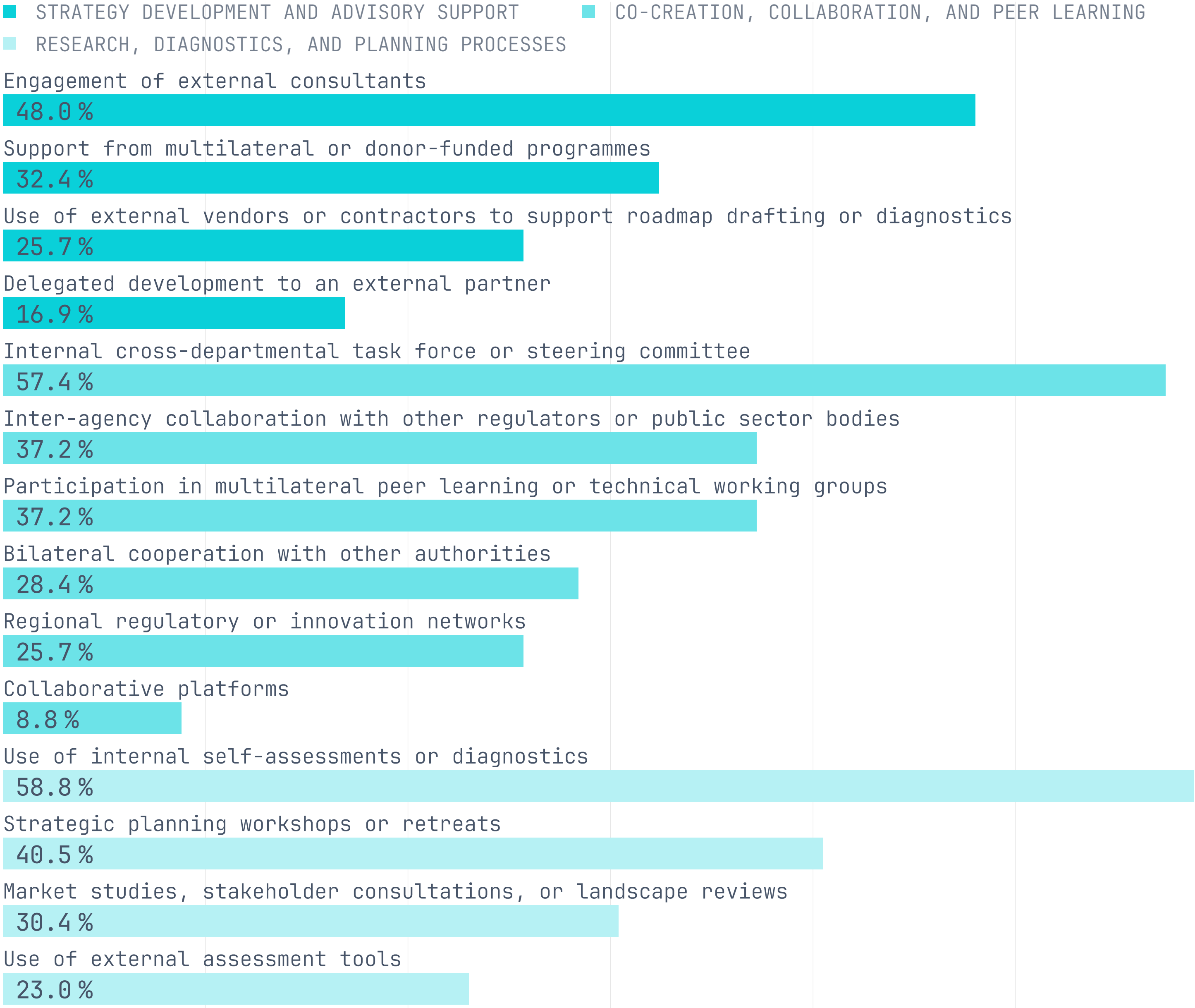


Financial authorities develop their digital transformation, data governance, suptech, and AI strategies through processes that are primarily driven from within the institution, but supported by targeted external expertise. The data shows that strategy formation is no longer treated as a purely technical exercise. Instead, it depends on broad internal ownership, cross-departmental collaboration, and selective engagement with consultants, vendors, and peer institutions (Figure 32).

Internal involvement is the dominant force shaping strategy development. IT departments play a central role, engaged in 73% of cases, reflecting the importance of data, architecture, and technology decisions in these frameworks. Strategy development, however, is not confined to technology teams. More than half of authorities also involve cross-departmental task forces, business units, and executive leadership, illustrating that these frameworks increasingly require enterprise-wide coordination and high-level commitment.

FIGURE 33.

Mechanisms Used to Engage Peers, Consultants, and Vendors in Strategy and Roadmap Development



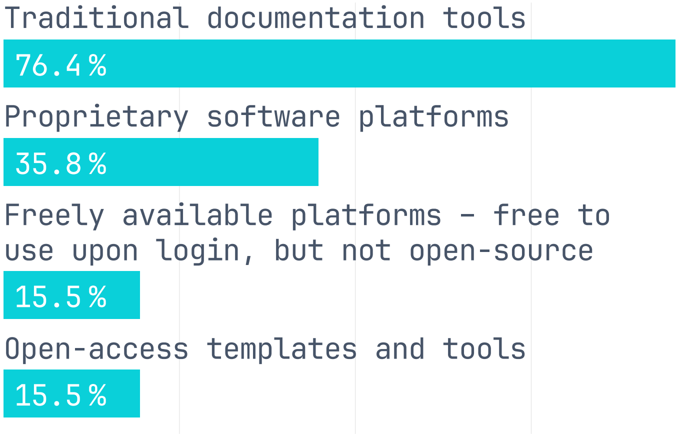
External actors complement internal leadership. Consultants are the most frequently engaged (44%), often providing specialised expertise, comparative assessments, or facilitation of diagnostics and planning workshops. Vendors, multilateral organisations, and other public-sector bodies offer targeted support, typically linked to specific technologies, capacity-building activities, or regional initiatives. Engagement with regulated firms, industry associations, and academic institutions is less common.

Strategy development is also supported by extensive internal and external collaboration (Figure 33). Internally, cross-functional task forces remain the backbone of coordination. Externally, many authorities participate in peer-learning groups, regional innovation networks, inter-agency working groups, or bilateral partnerships with other supervisors. These interactions help authorities benchmark their approaches, understand emerging supervisory practices, and adapt lessons from peers facing similar challenges. Underpinning these engagements is a strong reliance on internal self-assessments (59%), strategic planning workshops, market studies, and landscape reviews. The findings confirm that strategy development is both collaborative and evidence-based.

Despite this emphasis on collaboration, the tools used to support the development process remain relatively traditional. Figure 34 shows that three-quarters of authorities rely primarily on standard documentation tools. Enterprise software platforms are used in just over a third of cases, while freely available platforms and open-access templates each account for a modest 16%. A small group reports using more advanced or agile tools, such as internal collaboration platforms, mind-mapping software, or early applications of generative AI. This suggests that while strategic planning practices are evolving, the underlying toolset has not yet fully modernised.

FIGURE 34.

Tools and Platforms Used For Strategy Development and Coordination



Platforms such as GovSpace — used by 72 financial authorities and over 2,800 users during its MVP period, generating more than 30,000 diagnostic responses — illustrate how digital environments can support structured diagnostics, collaborative drafting, and cross-team alignment. While such tools are not yet mainstream, they provide a glimpse of how strategy development may evolve as authorities seek more integrated, data-driven planning methods.

2.2.5 How strategic frameworks mitigate institutional constraints

The distribution of challenges across authorities with 0–4 strategic frameworks (digital transformation, data governance, suptech, and AI) reveals a consistent pattern: agencies with no strategies in place report significantly higher difficulties across almost all categories, while those with multiple strategies tend to have lower rates of challenges, especially for core design, data, and implementation obstacles.

An examination of the challenges faced by authorities in designing and implementing suptech applications, operationalising effective data management, and deploying AI reveals a consistent pattern: the burden of challenges is highest among agencies with no strategic frameworks in place, and decreases markedly as authorities adopt two or more strategies related to digital transformation, data governance, suptech, and AI (Tables 1A–1C).

Across all domains, authorities without any strategy report the highest incidence of design, implementation, and data-management challenges. These include difficulties attracting talent, weak internal design capabilities, data quality issues, lack of interoperability, legacy IT constraints, and heavy reliance on manual processes. For example, data integration challenges are reported by 37% of authorities with no strategies, compared with 14% among those with three. Similar patterns appear for data quality issues (23% versus 9%) and resource-intensive deployment (22% versus 9%).

Adopting one strategy is associated with modest improvements, but challenge levels remain comparatively high. The most notable reductions occur among authorities with two or three strategies, where many core constraints become significantly less prevalent. At this stage, difficulties in data integration, design capacity, buy-in, and operational coordination fall sharply. Improvements are particularly visible in design-related challenges, where lack of internal product design skills drops from 24% (no strategies) to 2% (three strategies). Similarly, manual data processing declines from 26% to 7%, and limited analytics skills from 20% to 5%.

However, adding a fourth strategy does not produce proportionate further reductions. Challenge levels tend to stabilise, and in some cases rise slightly relative to the three-strategy group. This may suggest diminishing marginal improvements as the strategic set expands, potentially reflecting the greater complexity of authorities engaged in broader institutional transformation agendas.

Across all strategy counts, a subset of challenges remain relatively constant. These include privacy and ethical concerns, vendor lock-in, explainability issues in AI, reputational risks, and misalignment with evolving regulations. Their persistence indicates that some constraints are systemic or technology-specific, requiring specialised governance, regulatory clarity, and market engagement rather than additional strategic frameworks.

Taken together, the findings suggest three overarching patterns. First, strategy adoption is strongly associated with reduced operational and design obstacles, especially when authorities adopt at least two integrated frameworks. Second, beyond three strategies, improvements plateau, reflecting the limits of strategic documentation in overcoming deeper structural or technical barriers. Third, persistent challenges such as ethics, bias, and vendor lock-in require targeted interventions, irrespective of strategic maturity.

While these results do not establish causality, they provide strong indication that coherent strategic planning supports more manageable transformation pathways, and that isolated or absent strategies leave authorities exposed to greater friction and slower progress. As such, strengthening strategy coherence across digital transformation, data governance, suptech, and AI represents a foundational step toward reducing implementation challenges and accelerating supervisory innovation.

TABLE 1.

Distribution of Challenges Faced by Financial Authorities Based on Adopted Strategic Frameworks

Only strategies related to digital transformation, data governance, supervisory technology, and artificial intelligence are considered in this analysis

TABLE 1.A.

Strategy Count x Challenges: Designing + Implementing SupTech

SUPERCATEGORY	CHALLENGE	0	1	2	3	4
Design-related challenges	Aligning organisational culture to support design efforts	17.0%	12.0%	12.0%	6.0%	9.0%
	Attracting or retaining relevant talent	22.0%	14.0%	10.0%	8.0%	10.0%
	Lack of internal product design skills or experience	24.0%	14.0%	13.0%	2.0%	7.0%
	Creating inclusive processes where diverse perspectives are heard	8.0%	6.0%	3.0%	2.0%	2.0%
	Data quality issues	23.0%	14.0%	16.0%	9.0%	11.0%
	Lack of interoperable or machine-readable data	11.0%	10.0%	8.0%	3.0%	4.0%
	Coordination with other agencies to access data	14.0%	6.0%	5.0%	1.0%	6.0%
	Difficulty designing integrated systems	14.0%	11.0%	10.0%	8.0%	5.0%
	Limited ability to share data or knowledge across teams	13.0%	8.0%	6.0%	1.0%	3.0%
	Privacy or ethical concerns related to design choices	4.0%	6.0%	4.0%	5.0%	3.0%
	Long time to production/ delayed iteration cycles	15.0%	15.0%	14.0%	10.0%	8.0%
	Other	3.0%	2.0%	1.0%	1.0%	2.0%

TABLE 1.A. (CONTINUED)

Strategy Count x Challenges: Designing + Implementing SupTech

SUPERCATEGORY	CHALLENGE	0	1	2	3	4
Implementation-related challenges	Lack of buy-in on suptech priorities	13.0%	7.0%	6.0%	1.0%	1.0%
	Collaboration or coordination issues among stakeholders	10.0%	11.0%	8.0%	7.0%	6.0%
	Cost-related issues	24.0%	11.0%	16.0%	7.0%	5.0%
	Resource-intensive deployment	22.0%	12.0%	18.0%	9.0%	11.0%
	Legal or regulatory barriers	8.0%	4.0%	12.0%	5.0%	6.0%
	Procurement constraints	15.0%	13.0%	11.0%	9.0%	9.0%
	Limited flexibility or adaptability of applications	7.0%	10.0%	7.0%	1.0%	3.0%
	Vendor lock-in	7.0%	5.0%	7.0%	4.0%	5.0%
	Vendor misunderstanding of agency needs	8.0%	8.0%	2.0%	2.0%	4.0%
	Quality or functionality issues in delivered solutions	6.0%	6.0%	1.0%	1.0%	3.0%
	"Black box" problem	4.0%	4.0%	5.0%	2.0%	2.0%
	Legacy IT systems or infrastructure constraints	20.0%	8.0%	11.0%	7.0%	7.0%
	Limited internal IT capacity	22.0%	13.0%	10.0%	7.0%	7.0%
	Insufficient staff with data analytics skills	20.0%	14.0%	7.0%	5.0%	6.0%
	Pushback or resistance from private sector stakeholders	1.0%	2.0%	1.0%	1.0%	3.0%
	Difficulty accessing external datasets or coordinating with other agencies	5.0%	3.0%	5.0%	1.0%	2.0%

TABLE 1.B.

Strategies x Challenges Operationalising Effective Data Management

SUPERCATEGORY	CHALLENGE	0	1	2	3	4
Integration and infrastructure challenges	Integrating structured, unstructured, and legacy data sources (e.g., financial reports, alternative data, transaction records)	37.0%	16.0%	16.0%	14.0%	11.0%
	Ensuring data interoperability across multiple systems and jurisdictions	22.0%	12.0%	11.0%	6.0%	8.0%
	Incompatibility between legacy IT infrastructure and modern data tools	22.0%	12.0%	10.0%	8.0%	6.0%
	Lack of common identifiers across datasets (e.g., institution codes, transaction IDs)	11.0%	7.0%	8.0%	4.0%	9.0%
	Dependence on manual processes for data cleaning or transformation	26.0%	15.0%	12.0%	7.0%	7.0%
Data quality and validation challenges	Ensuring timely, complete, and validated data submissions across multiple reporting entities	34.0%	19.0%	18.0%	10.0%	8.0%
	Limited automation in data validation, anomaly detection, and reconciliation	37.0%	19.0%	13.0%	9.0%	7.0%
	Limited visibility into data lineage or transformation history	21.0%	10.0%	9.0%	4.0%	3.0%
	Inconsistent data definitions or taxonomies across internal teams programming in Python, R, Julia, or other languages	16.0%	9.0%	4.0%	1.0%	6.0%

TABLE 1.B. (CONTINUED)

Strategies x Challenges Operationalising Effective Data Management

SUPERCATEGORY	CHALLENGE	0	1	2	3	4
Governance, compliance, and resource challenges	Managing high-volume, diverse, and dynamic data in a rapidly evolving digital environment	32.0%	17.0%	17.0%	10.0%	9.0%
	Balancing data integrity with privacy, security, and regulatory compliance requirements	27.0%	8.0%	14.0%	6.0%	8.0%
	Limited data governance expertise and resources within the agency	27.0%	8.0%	11.0%	6.0%	3.0%
	Unclear ownership or accountability for data quality across departments	22.0%	6.0%	12.0%	3.0%	4.0%
	Resource constraints limiting investment in data infrastructure upgrades	25.0%	10.0%	11.0%	2.0%	6.0%
	Lack of clarity or misalignment between supervisory and reporting entity expectations	16.0%	4.0%	3.0%	0.0%	3.0%

TABLE 1.C.

Strategies x Challenges Deploying AI

CHALLENGE	0	1	2	3	4
Algorithmic bias and discrimination in AI	2.0%	3.0%	3.0%	1.0%	3.0%
Auditability and disclosure of AI techniques used by financial service providers	4.0%	4.0%	4.0%	3.0%	2.0%
Data protection, privacy, and security concerns	8.0%	10.0%	10.0%	10.0%	7.0%
Employment-related challenges and need to upgrade staff skills	9.0%	5.0%	7.0%	5.0%	7.0%
Explainability – lack of transparency in AI systems ("black box")	9.0%	4.0%	5.0%	4.0%	5.0%
Governance and accountability of AI systems	5.0%	7.0%	4.0%	5.0%	4.0%
High implementation costs and resource requirements	5.0%	5.0%	5.0%	2.0%	2.0%
Integration with existing systems and workflows	6.0%	6.0%	3.0%	7.0%	7.0%
Limited compute resources (e.g., CPU, GPU, RAM, HPC clusters)	4.0%	3.0%	7.0%	2.0%	3.0%
Limited internal technological capacity	3.0%	6.0%	4.0%	2.0%	2.0%
Maintenance and lifecycle management of AI systems	1.0%	6.0%	1.0%	4.0%	4.0%
Poor data quality	3.0%	6.0%	3.0%	2.0%	2.0%
Training, validating, and testing models for robustness and resilience	5.0%	4.0%	7.0%	4.0%	5.0%
Vendor lock-in or reliance on external AI service providers	4.0%	3.0%	2.0%	1.0%	2.0%
Misalignment with evolving national or international regulations	0.0%	2.0%	2.0%	1.0%	0.0%
Reputational risks or public trust concerns	4.0%	5.0%	2.0%	3.0%	3.0%
Ethical concerns or unintended societal impacts	3.0%	3.0%	3.0%	2.0%	2.0%

2.2.6 Strategic frameworks as enablers of suptech adoption

The 2025 survey shows an association between strategic maturity and the scale of suptech adoption. Authorities without strategies are concentrated among those with no operational applications, while those with multiple strategies are disproportionately represented in the higher adoption tiers. Operational suptech, data governance, digital transformation, and AI strategies all correlate with greater use of 2–10 and 11–15 applications. Combinations of two or more strategies show a cumulative effect, appearing almost exclusively among authorities with multi-application portfolios. Although the data do not establish causality, the patterns indicate that more comprehensive strategic planning is consistently linked with broader suptech deployment.

From the analysis of the 2025 survey results, a correlation between the presence of strategic frameworks and the scale of suptech adoption across financial authorities emerges. The relationship is not uniform across domains, but the charts reveal a strong general pattern: **authorities with more developed strategies tend to deploy more suptech applications**, while those without strategies remain concentrated among the lowest adoption tiers.

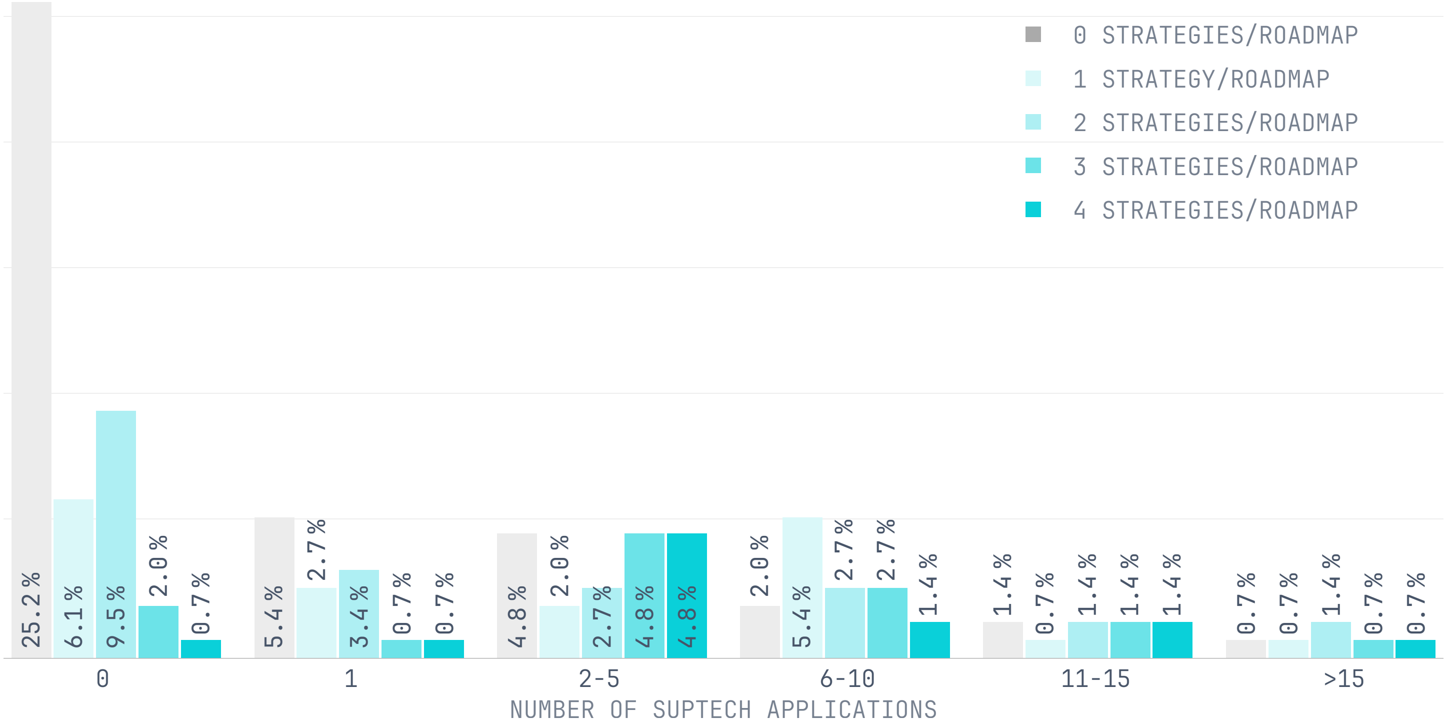
This relationship holds across suptech, data governance, digital transformation, and AI strategies. Figure 35 shows a pronounced gradient across the adoption spectrum:

- **Authorities with no strategies** overwhelmingly cluster in the 0 applications category (25%) and have minimal presence beyond 1–5 applications.

FIGURE 35.

Correlation Between Strategic Maturity and SupTech Deployment

Only strategies related to digital transformation, data governance, supervisory technology, and artificial intelligence are considered in this analysis



- **Authorities with 1 strategy** show modest distribution across 1–5 applications but remain sparse in higher-adoption tiers.
- **Authorities with 2–3 strategies** are progressively more represented in the 2–5 and 6–10 application ranges.
- **Authorities with 4 strategic frameworks** appear predominantly in the 6–10, 11–15, and >15 application categories, despite representing a small share of all respondents.

In effect, the more strategic frameworks an authority has in place, the more likely it is to have deployed multiple suptech applications. The pattern is consistent: higher adoption is associated with richer strategic planning.

Table 2 provides a detailed view of how specific strategic frameworks – suptech, data governance, digital transformation, and artificial intelligence – align with different levels of suptech adoption. Although these results

TABLE 2.

Correlation Between Each Strategic Framework and Suptech Adoption

		NO SUPTECH APPLICATIONS IMPLEMENTED		NUMBER OF SUPTECH APPLICATIONS CURRENTLY OPERATING		
		No plan	Planning	1	2-4	5+
Suptech Strategy	In Development	6.2%	41.7%	12.5%	10.4%	29.2%
	No	19.0%	38.1%	19.0%	9.5%	14.3%
	Yes	5.6%	23.9%	14.1%	15.5%	40.8%
Data Governance Strategy	In Development	7.3%	41.8%	9.1%	14.5%	27.3%
	No	16.7%	36.7%	26.7%	6.7%	13.3%
	Yes	3.6%	20.0%	12.7%	14.5%	49.1%
Digital Transformation Strategy	In Development	5.2%	34.5%	15.5%	15.5%	29.3%
	No	15.8%	50.0%	13.2%	7.9%	13.2%
	Yes	4.5%	13.6%	13.6%	13.6%	54.5%
Artificial Intelligence Strategy	In Development	9.7%	25.8%	11.3%	14.5%	38.7%
	No	9.6%	51.9%	21.2%	7.7%	9.6%
	Yes	0.0%	7.7%	7.7%	19.2%	65.4%

do not establish causality, the associations are strong and consistent: **authorities with formal strategies, particularly operational ones, are significantly more likely to deploy multiple suptech applications**, while those without strategies are far more concentrated in the lowest adoption tiers.

Across all four strategic domains, **absence of a strategy aligns closely with absence of adoption**. Authorities that report having no relevant strategy show the highest shares in the "0 applications" category – 19% for suptech, 17% for data governance, 16% for digital transformation, and 10% for AI. By contrast, among agencies with operational strategies, the proportion reporting zero applications drops sharply to between 0% and 6%. This pattern suggests that strategic planning, at a minimum, is associated with movement away from non-adoption.

Authorities with operational strategies also appear disproportionately in the "5+ applications" tier. This is most pronounced for suptech strategies, where 41% of agencies with an operational roadmap fall into the highest adoption category – by far the strongest association across all strategy types. Operational AI strategies also show a substantial presence in the 5+ tier (25%), despite the overall early-stage maturity of AI planning. Data governance and digital transformation strategies similarly correlate with higher deployment levels, though with greater concentration in the mid-range (2–10 applications). These patterns collectively indicate that strategy operationalisation is associated with scale, with authorities that have moved beyond drafting to implementation reporting broader suptech deployment.

Strategies "in development" occupy a transitional position, clustering around the planning stage and early adoption tiers. This is particularly evident for AI strategies, where more than half of authorities with strategies still in development report having no applications but intending to adopt. Similar transitional patterns appear for suptech, data governance, and digital transformation: authorities in the drafting phase are less likely to be fully inactive than those with no strategy, but far less likely to appear in the higher-adoption tiers than those with operational frameworks. This distribution aligns with the idea that strategy development often precedes – and perhaps enables – systematic scale-up.

The four strategy types also display distinct associations with adoption patterns.

- **Suptech strategies** have the clearest alignment with high deployment, suggesting that targeted supervisory planning supports scaling across multiple functions.
- **Digital transformation strategies** are most strongly linked to the mid-range (2–10 applications), indicating their role in enabling broader but not yet fully mature deployment.
- **Data governance strategies** correlate with balanced, multi-tier adoption patterns, reinforcing their foundational role.
- **AI strategies**, meanwhile, show the sharpest split between early-stage planning and high-end adoption, reflecting the emerging and uneven institutionalisation of AI governance.

Taken together, the results highlight a consistent structural relationship: the presence and operationalisation of strategic frameworks is associated with deeper and broader suptech adoption, while the absence of strategy is associated with non-adoption. Strategy development appears to function as an institutional readiness mechanism – creating conditions for adoption by improving planning, governance, resourcing, and internal alignment.

At the same time, the transitional patterns observed in the "in development" category suggest that many authorities may be formalising strategies because they are beginning to adopt suptech, pointing to iterative and mutually reinforcing development pathways.

While the analysis does not identify causal effects, the associations are sufficiently robust to underscore the importance of coherent strategic planning. Whether strategy precedes adoption or adoption drives strategy formulation, authorities that connect suptech, data governance, digital transformation, and AI through structured frameworks appear better positioned to scale supervisory innovation.

Table 3 examines how combinations of strategic frameworks – across digital transformation (DX), data governance (DG), suptech (ST), and artificial intelligence (AI) – align with different levels of suptech adoption. The results provide a more nuanced view of institutional readiness than individual strategies alone.

A first clear pattern is that combinations anchored in digital transformation and data governance consistently correlate with higher adoption tiers. The DX+DG pairing is the most prevalent among authorities with 5+ applications (43.5%), and it also shows the highest concentration (44.4%) in the 2–4 application range. These results reinforce the role of DX and DG as foundational enablers of supervisory technology: agencies that have invested in institutional modernisation and data readiness are better positioned to scale tool deployment across multiple use cases.

Adding a third strategy – most commonly suptech – is associated with a shift toward broader, but slightly more distributed, adoption patterns. Authorities with DX+DG+ST show strong representation in both the 2–4 (27.8%) and 5+ (32.6%) tiers. While these percentages are lower than the 43.5% seen in the DX+DG combination, the pattern likely reflects the smaller number of authorities with three strategies as well as the transitional nature of multi-framework integration. The results nevertheless indicate that adding suptech strategy to an institutional transformation foundation is linked with sustained multi-application deployment.

Two-strategy combinations involving ST or AI without both DX and DG show weaker associations with higher adoption. For example, DG+ST, DG+AI, and ST+AI combinations display more even distribution across tiers, with fewer authorities in the 5+ category and a notable presence in the "planning only" and single-application ranges. This suggests that while specialised strategies (e.g. ST, AI) support incremental progress, they do not substitute for broader institutional and data-centric frameworks when scaling to higher deployment levels.

The four-strategy combination (DX+DG+ST+AI) shows a modest but meaningful share in multi-application categories (19.6% for 5+ and 16.7% for 2–4). These authorities appear to be building more comprehensive transformation architectures, but the distribution across tiers indicates that implementation is still maturing. Notably, none of the multi-strategy combinations appear in the "0 applications and no plan" category, underscoring that the presence of multiple strategies—regardless of composition—is consistently associated with forward movement in suptech adoption.

Three system-level insights emerge from these patterns:

1. Institution-wide and data-centred strategies are the strongest predictors of scaled deployment. Combinations anchored in DX and DG dominate the top tiers of adoption, emphasising the importance of organisational readiness

TABLE 3.

Combination of Strategies and Suptech Adoption

	0 SUPTECH APPLICATIONS, NO PLAN	0 SUPTECH APPLICATIONS, BUT PLANNING TO	1 SUPTECH APPLICATION	2-4 SUPTECH APPLICATIONS	5+ SUPTECH APPLICATIONS
DX+DG	18.2%	20.0%	21.1%	44.4%	43.5%
DX+ST	18.2%	11.1%	15.8%	27.8%	45.7%
DX+AI	0.0%	2.2%	5.3%	27.8%	30.4%
DG+ST	9.1%	4.4%	21.1%	27.8%	34.8%
DG+AI	0.0%	4.4%	5.3%	22.2%	21.7%
ST+AI	0.0%	2.2%	5.3%	16.7%	32.6%
DX+DG+ST	9.1%	4.4%	10.5%	27.8%	32.6%
DX+DG+AI	0.0%	2.2%	5.3%	22.2%	21.7%
DX+ST+AI	0.0%	2.2%	5.3%	16.7%	28.3%
DG+ST+AI	0.0%	2.2%	5.3%	16.7%	19.6%
DX+DG+ST+AI	0.0%	2.2%	5.3%	16.7%	19.6%

% OF FINANCIAL AUTHORITIES

and data quality as prerequisites for operational suptech.

2. Specialised strategies (ST, AI) add value when layered on top of DX and DG, but have limited impact when adopted in isolation or without institutional foundations. This confirms the complementary, rather than standalone, nature of suptech and AI planning.

3. Authorities with multiple strategies, regardless of configuration, rarely remain inactive. The absence of multi-strategy agencies in the “0 applications, no plan” category reflects a consistent association between strategic coherence and adoption momentum.

Table 3 provides further evidence that integrated, multi-framework planning is associated with wider and deeper suptech deployment, while institutional and data-centric strategies remain the most critical anchors for scale. These results align closely with the earlier analysis of individual strategies and support the conclusion that fragmented planning is often associated with more limited adoption, whereas coherent strategic architectures support systematic, multi-application deployment.

The 2025 results reduce earlier uncertainty around directionality but do not fully resolve causality. While the association is now stronger and more consistent across datasets, the analysis does not establish that strategies cause higher adoption. The data remain consistent with two plausible pathways:

1. **Strategy-first:** Authorities adopt institutional strategies early, creating the governance, data foundations, and prioritisation needed to scale suptech.
2. **Practice-informed:** Authorities begin with pilots or prototypes; early operational learning then serves as the basis for formalising broader strategies.

Both trajectories are visible in the data. The strengthened association in 2025 indicates that strategy alignment has become a more reliable predictor of higher implementation, but causality cannot be inferred without longitudinal or econometric analysis.

Across the shared data, three implications stand out for financial authorities:

- **Strategic coherence matters:** suptech, DG, DX, and AI strategies reinforce each other and create the structural conditions for scaled adoption.
- **Fragmented planning yields fragmented implementation:** authorities with isolated strategies rarely progress beyond early-stage deployment.
- **Integrated frameworks support scale:** multi-strategy authorities are the only group consistently found in the upper deployment tiers.
- **Strategies are enablers, not guarantees:** some authorities with multiple strategies remain early-stage, highlighting the importance of governance, skills, culture, and resourcing.

These findings reinforce the need for strategic alignment as a core institutional enabler.

2.3 Governance frameworks

Governance frameworks for suptech and digital transformation remain uneven, with major gaps in both scope and resourcing, and the absence of dedicated budgets for suptech and AI. However, governance structures are evolving, with leadership increasingly centred on technology units and supported by new specialised roles such as Chief Data Officers. While basic privacy frameworks are common, the adoption of advanced privacy-enhancing technologies (PETs) is still limited. Collaboration is strong within domestic contexts but remains weak at the international level. With funding still dominated by internal agency budgets, sustained investment and stronger institutional capacity are essential to modernise governance and enable effective supervisory innovation.

The successful implementation of suptech and digital transformation initiatives hinges on robust governance structures that bridge strategic ambition and operational delivery. Strong governance frameworks establish clear authority, define decision-making processes, create accountability mechanisms, and enable departmental coordination. Beyond organisational clarity, they cultivate institutional trust, protect data integrity, and ensure responsible deployment of emerging technologies including AI.

Senior leadership commitment remains critical for overcoming organisational resistance and mobilising resources. Authorities are establishing executive-level positions and cross-functional teams for technological transformation, reinforcing data protection protocols, and developing structured inter-agency collaboration. Yet funding constraints and uneven institutional maturity mean many frameworks remain incomplete, particularly in EMDEs, This underscores the need for sustained investment, targeted capacity-building, and international knowledge-sharing to support more coherent, resilient governance.

2.3.1 Leadership

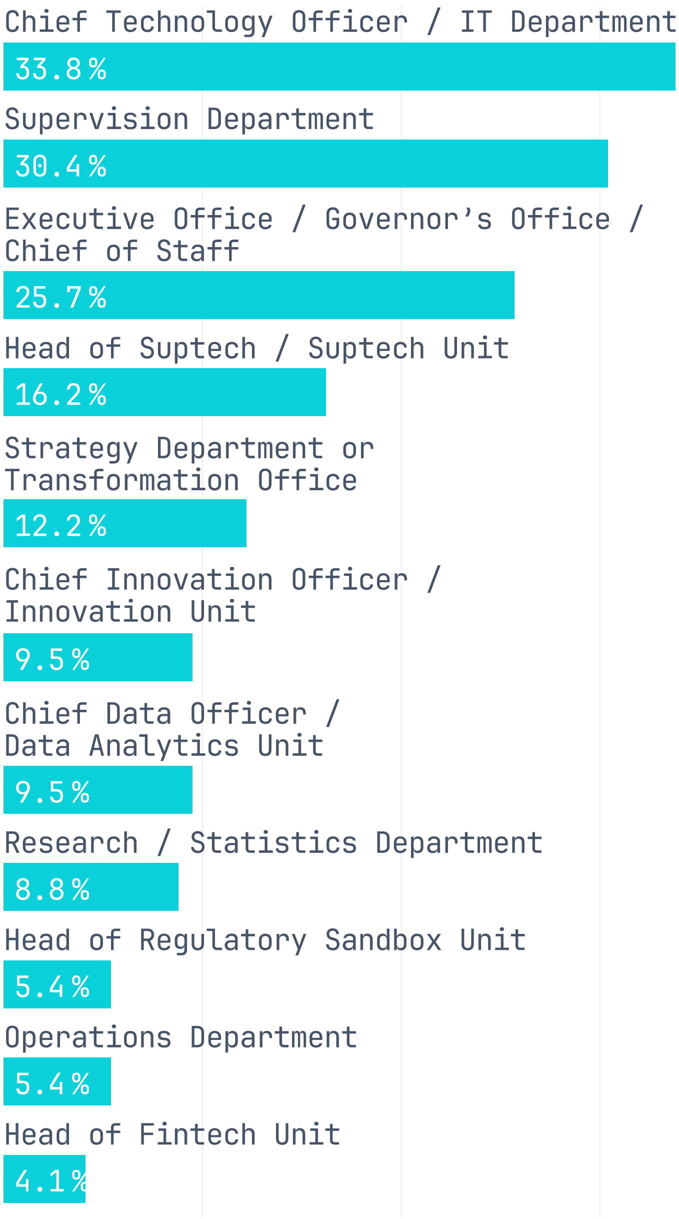
Leadership models for suptech remain diverse, but 2025 data shows a clear shift toward more technology-led and formalised governance. Increasing reliance on CTOs, IT departments, and senior executive oversight, combined with the growing creation of specialised roles such as Heads of SupTech and Chief Data Officers, is consistent with a maturing approach in which accountability, data stewardship, and innovation are becoming central pillars of supervisory governance.

The leadership structure for suptech initiatives across financial authorities in 2025 is diverse and often decentralised, reflecting different institutional priorities and transformation models. Compared to 2024 figures and previous years, which showed a plurality of leadership residing in supervision departments, 2025 data indicates a clearer shift toward technology-led governance and greater institutional formalisation. The initiative is primarily led by technology and core supervisory functions, with the Chief Technology Officer (CTO) / IT Department taking the lead in over a third of agencies (34%). This is consistent with the growing importance of technology architecture, data, and infrastructure decisions in shaping supervisory innovation. The Supervision Department remains the second most common lead (30%), reflecting the continued grounding of suptech in supervisory mandates (Figure 36). A significant proportion of initiatives are also spearheaded by senior leadership, with the Executive Office / Governor's Office / Chief of Staff leading in 26% of agencies, demonstrating higher-level institutional prioritisation and strategic ownership.

Dedicated units are also emerging, with the Head of SupTech / SupTech Unit leading in 16% of responding agencies, indicating a more formalised approach where authorities create specialised governance structures to

FIGURE 36.

Who Leads Your SupTech Initiative

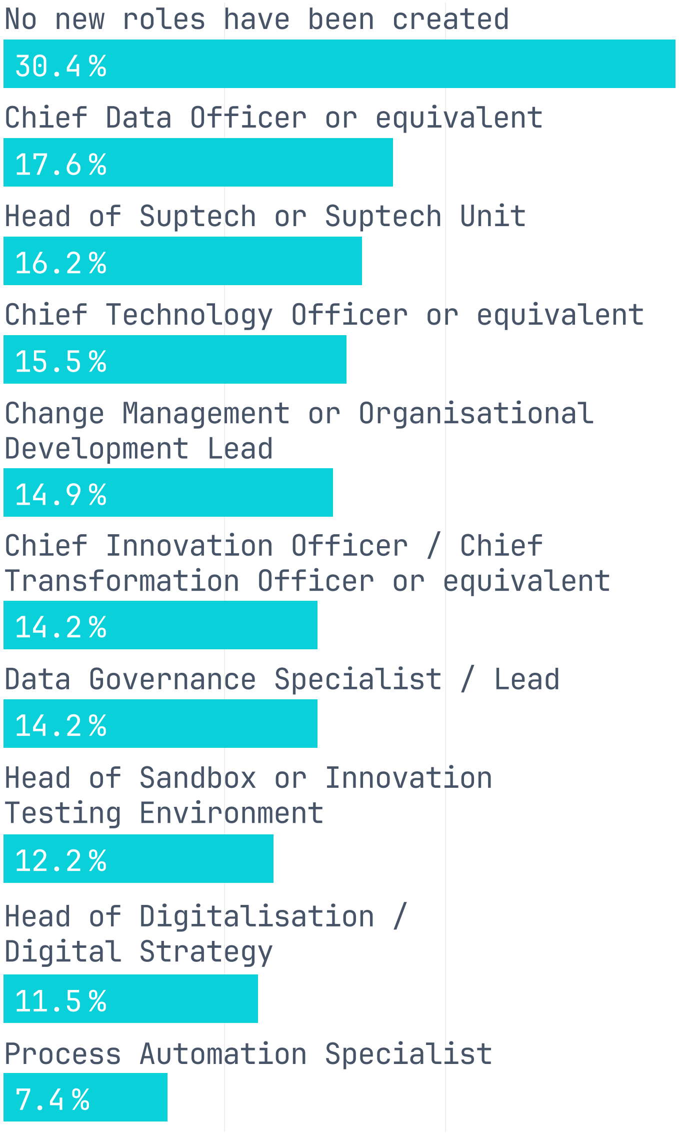


coordinate and scale technological adoption (Figure 37). The Strategy Department or Transformation Office leads in 12% of agencies, and the Chief Data Officer / Data Analytics Unit in 10%. These patterns highlight the importance of data stewardship and enterprise-wide alignment for effective suptech deployment.

The diversified leadership model is reinforced by a growing number of specialised roles created to support suptech and digital transformation. While close to a third of agencies (30%) reported that they had not created any new roles in 2025, indicating ongoing reliance on existing capacity, the most frequently created new roles were tied (16% each) between Head of SupTech / SupTech Unit and Chief Data Officer (CDO) or equivalent. Additional roles strengthen change management and data quality: Change Management or Organisational Development Leads were created by 15% of authorities, and Data Governance Specialists / Leads by 14%. Together, these developments reflect a more structured approach to embedding governance, technical specialisation, and institutional transformation expertise within leadership teams.

FIGURE 37.

Creation of New Positions to Lead Digital Transformation and SupTech Within the Agency



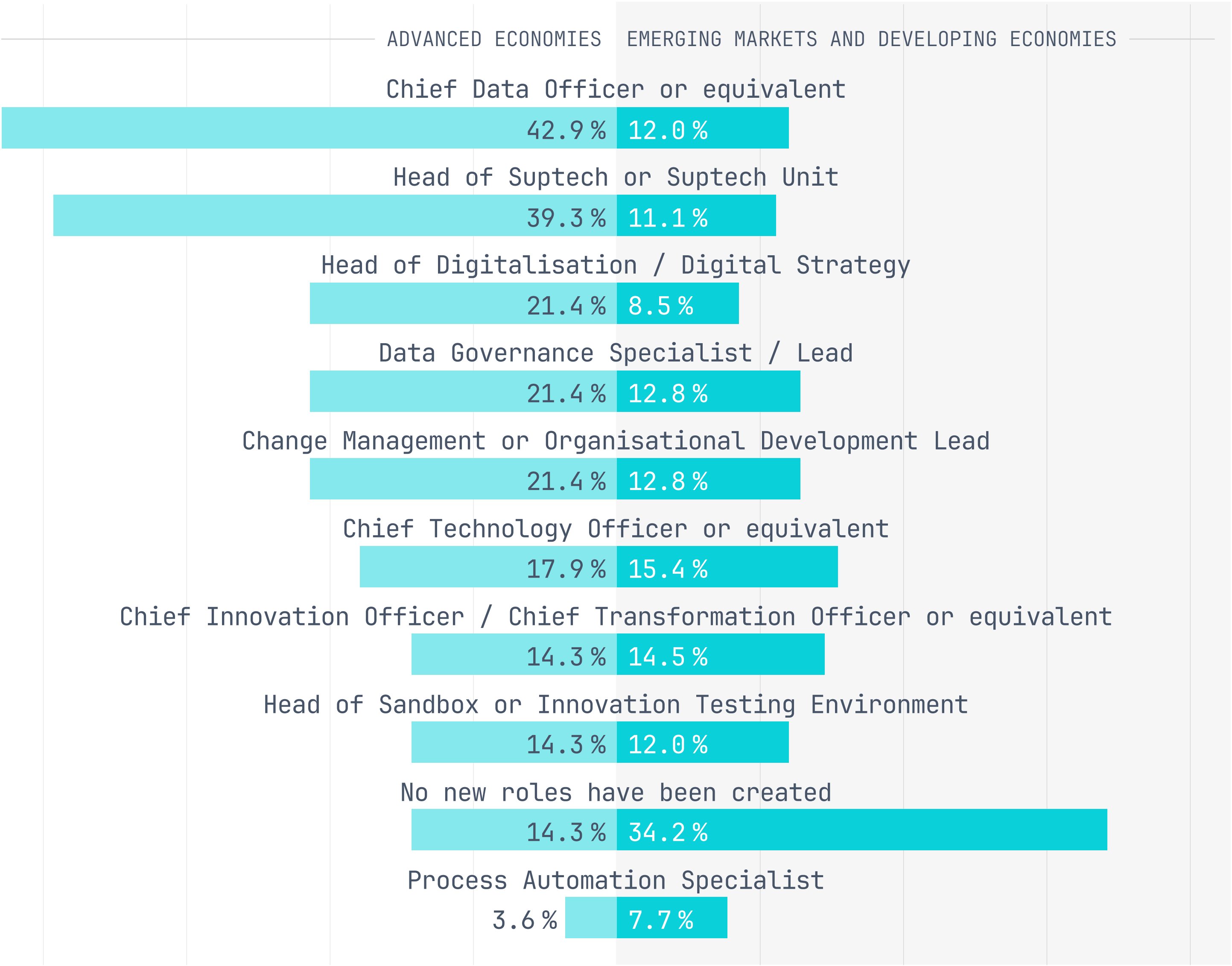
The creation of new leadership and specialist positions to drive digital initiatives is significantly more common in AEs than in EMDEs (Figure 38). AEs primarily focus on dedicated data and suptech leadership, with the most frequent new roles being 'Chief Data Officer (CDO) or equivalent' (43%) and 'Head of SupTech or SupTech Unit' (39%), demonstrating a strategic commitment to governance and supervisory technology. In contrast, a substantial 34% of EMDE agencies report that no new roles have been created, and where new positions exist, the focus is more fragmented, with the CDO (12%) and Head of SupTech (11%) being created less frequently than in AEs, highlighting a pronounced gap in establishing dedicated leadership for key strategic dimensions of the agencies' digital transformation in many EMDEs.

YOY trends indicate a lack of progress in the adoption of advanced data and digital technologies by management teams and boards (Figure 39). Reliance on interactive dashboards has fallen sharply, and the use of advanced analytics remains extremely low. This slowdown, despite increased operational-level investment in suptech, underscores a persistent difficulty in embedding analytical outputs into executive workflows.

A key structural factor is that many suptech applications operate at the departmental

FIGURE 38.

Creation of New Positions to Lead Digital Transformation and SupTech Within the Agency By Economic Classification



level and have not yet been integrated into a consolidated intelligence layer capable of synthesising insights for executives. Without this integration, management continues to receive fragmented information that is difficult to translate into strategic decisions, reinforcing reliance on familiar, low-tech channels such as briefings, spreadsheets, and static reports.

Overall, the data suggests a strategic bottleneck: even as operational adoption accelerates, limited executive-level digital uptake appears to constrain institutional impact. Addressing this diffusion gap will require targeted capacity building for boards and senior leaders, combined with organisational efforts to integrate suptech outputs into coherent, decision-ready supervisory intelligence systems.

2.3.2 Privacy and security

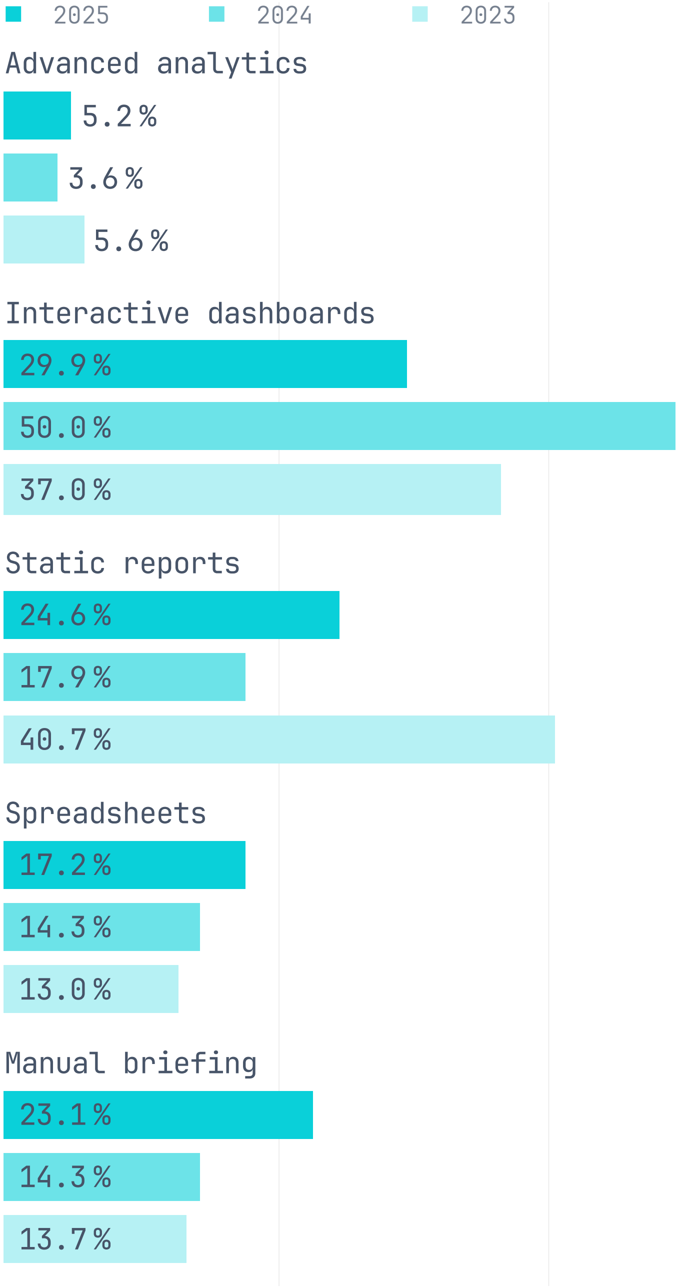
Data protection is fundamental to both suptech and data governance, becoming critical as authorities continue to rely on advanced analytics and AI. While more than half (54%) of financial authorities report having either integrated or comprehensive policies, many may remain exposed to ethical, legal, and operational risks due to fragmented governance structures. Adoption of sophisticated privacy-enhancing technologies (PETs) also remains limited, and regional and income disparities underscore the need for targeted support to strengthen frameworks. Robust data governance, built on clear roles and effective compliance procedures, is essential for trust, transparency, and the responsible implementation of next-generation supervisory technologies.

Privacy and data protection form the foundation of effective data and suptech governance. They ensure that data is managed in line with established standards, preserves public trust, and complies with legal obligations such as GDPR and auditability rules. These governance frameworks set out data protection roles and responsibilities, policy standards (e.g., cybersecurity and data retention), and risk-management protocols for issues like data breaches or model misuse. As regulatory frameworks such as Digital Operational Resilience Act (DORA) grow more complex, financial authorities face increasing pressure to adopt comprehensive and coherent data governance structures.

The commitment to data protection is evident, with 54% of financial authorities implementing privacy and data protection frameworks, confirming that more than half of all responding authorities have some form of governance in place whether comprehensive or integrated (Figure 40). About a third of these authorities employ comprehensive policies, covering all data lifecycle stages, while an additional 21% adopt an integrated approach, harmonising their broad data policies with ethical guidelines, risk management, and staff training. There is, however, still room for more comprehensive and integrated approaches, as 22% of the authorities have ad hoc policies, 14% possess only basic frameworks and approximately 3% lack any formal policy, highlighting the need for increased sharing of best practices and tools to bolster standards globally.

FIGURE 39.

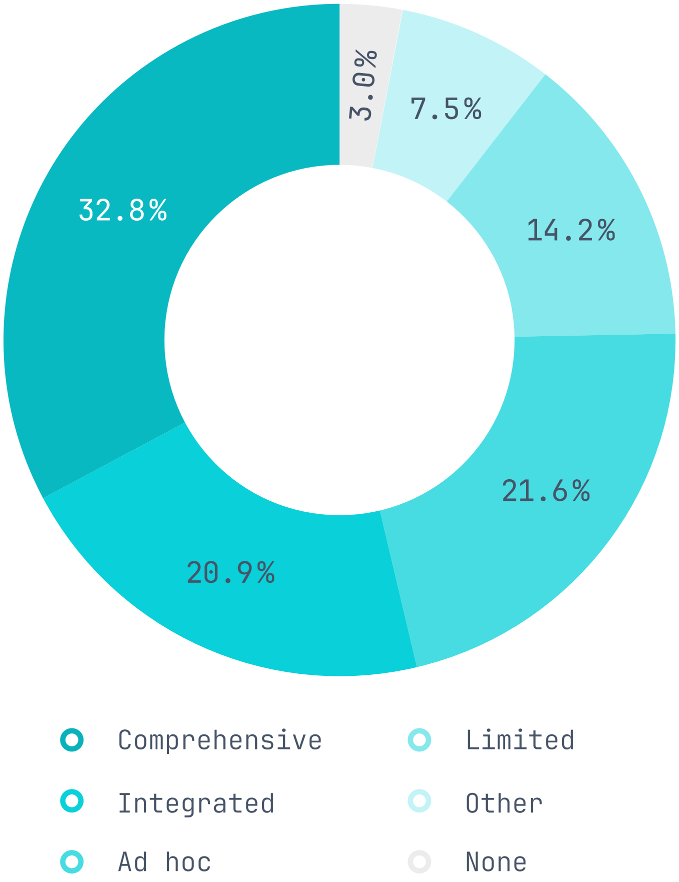
Leveraging of Data and New Technologies by the Management Team or Board 2023–2025



There is a clear maturity gap in privacy and data protection policies between economic

FIGURE 40.

Maturity of Privacy and Data Protection Policies



groups. A significant majority of AEs report having mature, formal frameworks in place, with 42% reporting comprehensive policies and 38% reporting integrated policies, suggesting established, institution-wide standards (Figure 41). In contrast, EMDEs are far more fragmented: while 30% report comprehensive policies and 18% integrated policies, a substantial portion still relies on immature or inadequate measures, with 24% reporting ad hoc policies, 17% reporting limited policies, and 4% having none at all, highlighting that foundational data governance remains a challenge for a large segment of emerging economies. .

Across regions, the maturity of privacy and data protection policies varies significantly, revealing a highly fragmented global landscape (Figure 42). The ECA region leads in formalisation, with the highest proportion reporting comprehensive policies (42%), while North America shows a distinct 50% split between integrated policies and ad hoc policies. In contrast, South Asia demonstrates the lowest maturity, with 80% of agencies relying on inadequate measures, split between limited (40%) and ad hoc (40%) policies. Both SSA and LAC regions show moderate maturity, with roughly a third of agencies reporting comprehensive policies, yet both also report significant reliance on ad hoc or limited frameworks, highlighting that foundational data governance remains a major challenge outside of established regulatory blocs.

The adoption of privacy-enhancing technologies (PETs) and advanced data interoperability practices within financial authorities remains nascent, with a high degree of uncertainty regarding current usage. A substantial number

FIGURE 41.

Privacy and Data Protection Policies in Place
By Economic Classification

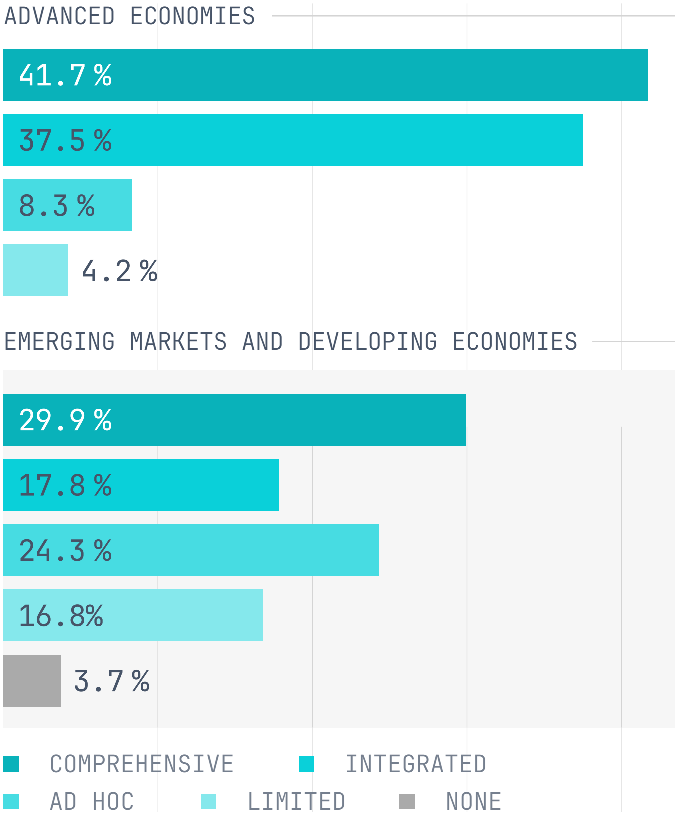
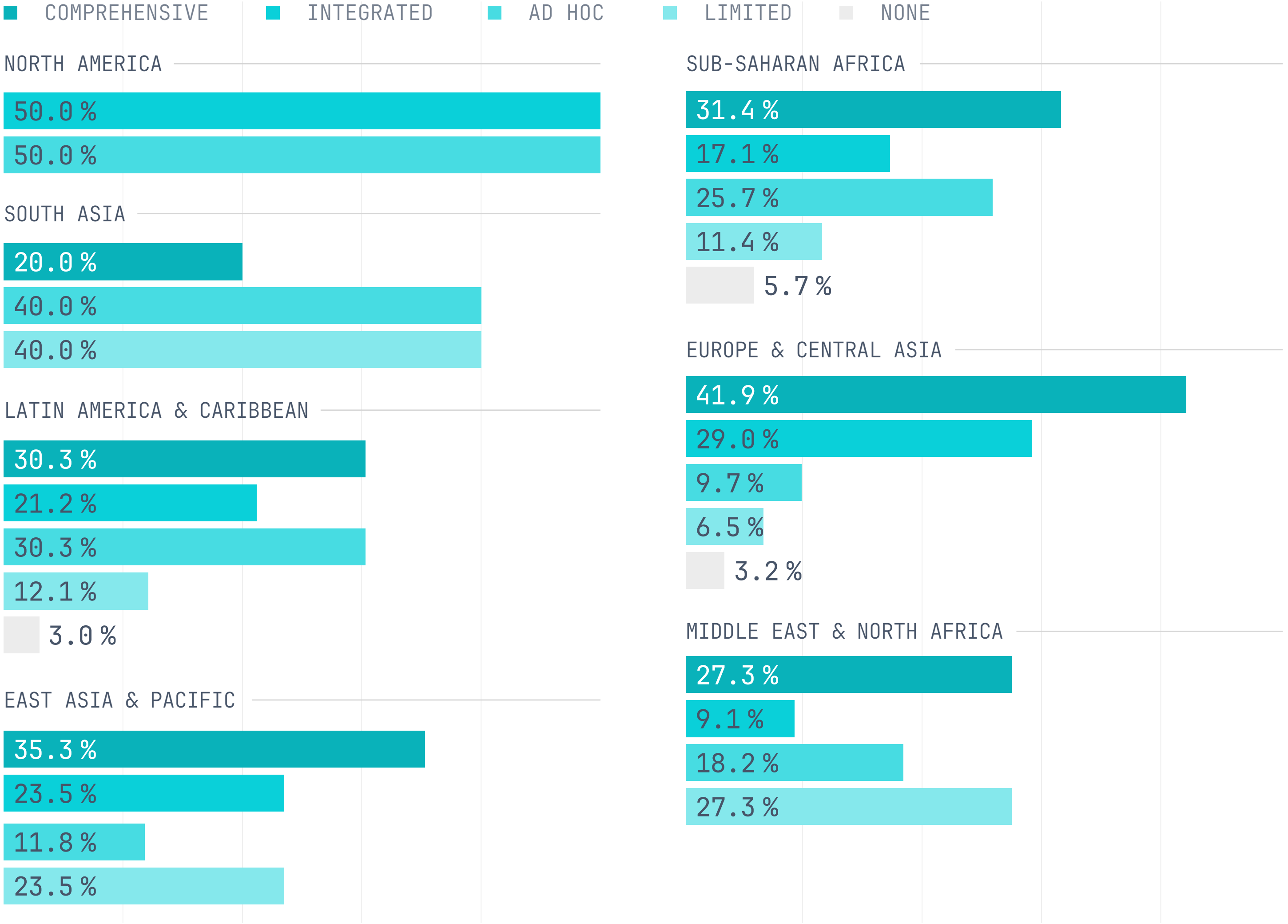


FIGURE 42.

Maturity of Privacy and Data Protection Policies By Region



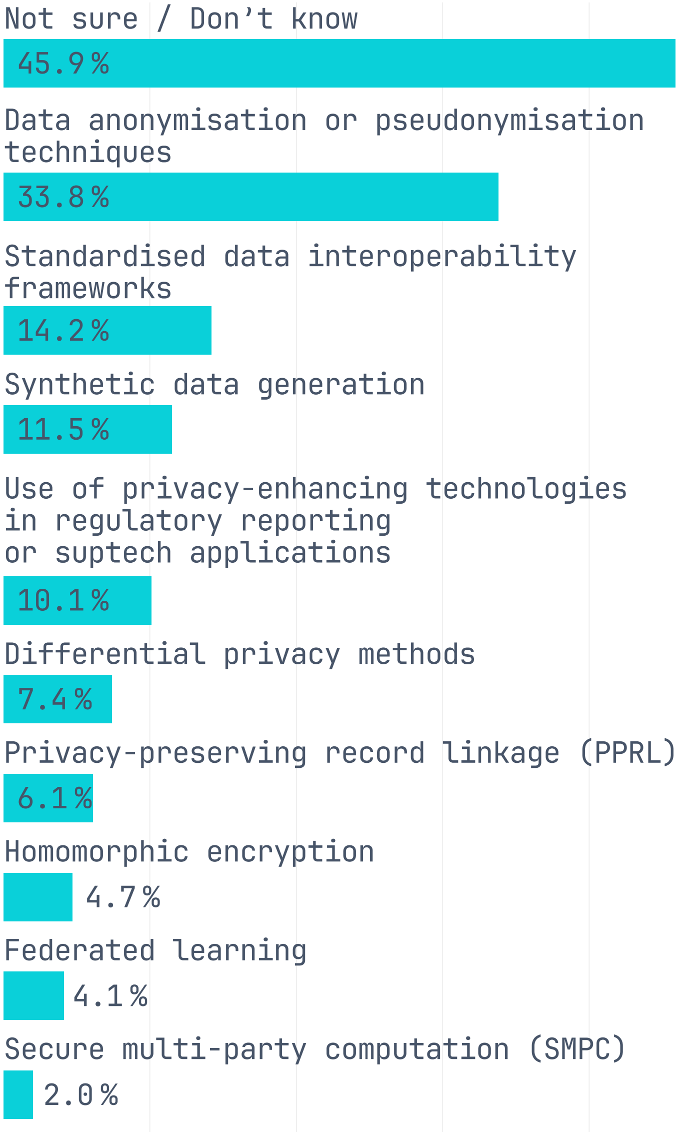
of respondents (46%) indicated they were “Not sure / Don’t know” which PETs their agency uses or plans to implement, highlighting a significant lack of awareness or communication regarding advanced data handling strategies within organisations (Figure 43). Where usage is confirmed, the most common practice involves standard data anonymisation or pseudonymisation techniques (34%), such as tokenisation or hashing, which are mature methods for reducing privacy risks.

Beyond basic anonymisation, usage drops sharply: Standardised data interoperability frameworks (e.g., ISO 20022 or open data APIs) are used or planned by 14%. Synthetic data generation (AI-generated datasets for testing or model training) is used by 12%, reflecting early interest in high-utility, low-risk data alternatives, and the direct use of PETs embedded in regulatory reporting or suptech applications stands at 10%.

More advanced, cryptographic PETs and distributed learning methods show very low adoption: Differential privacy methods are used by 7%, while techniques such as homomorphic encryption (5%), federated learning (4%), and secure multi-party computation (2%) are currently used or planned by only a tiny fraction of agencies. This data suggests that while fundamental anonymisation is becoming

FIGURE 43.

Privacy-Enhancing Technologies (PETS) and Data Interoperability Practices In Use Or Planned



common practice, the institutional adoption of more sophisticated PETs necessary for secure, advanced data analytics and cross-border sharing is still in its very early stages.

2.3.3 Collaborations and data sharing

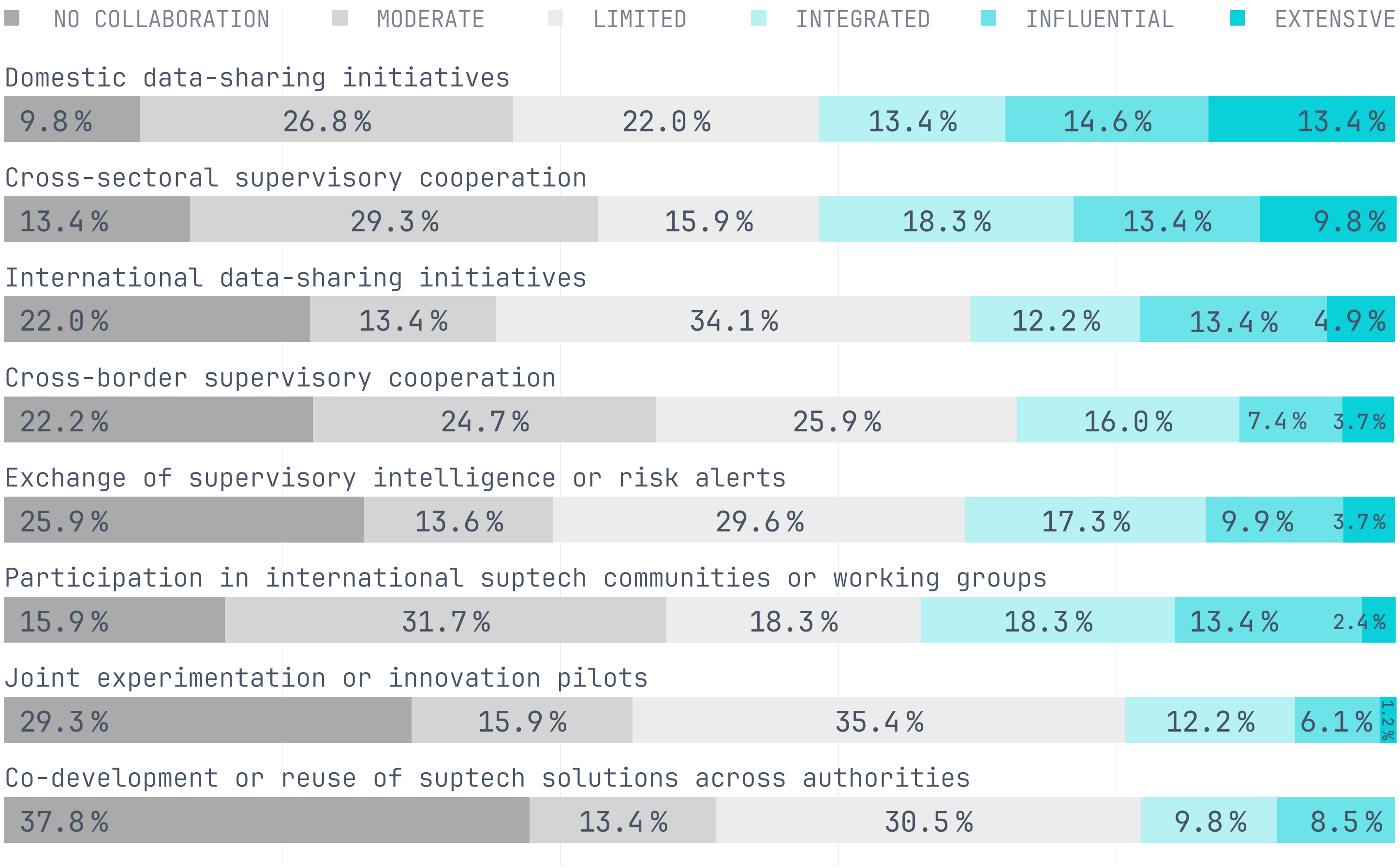
The data for 2025 indicates that suptech has contributed most effectively to collaboration in areas directly related to domestic data sharing and cross-sectoral supervisory cooperation, while collaboration on joint development and international initiatives remains less frequent.

Suptech supports most effectively to collaboration in domestic contexts, yet faces significant challenges in international and co-development areas. Over 40% of financial authorities report contributions that are extensive, influential, or integrated in domestic data-sharing initiatives (41%) and cross-sectoral cooperation (42%) (Figure 44). This suggests that suptech can add immediate value by improving internal operational efficiencies and helping to reduce barriers between local regulators. However, participation in international initiatives, joint development with other agencies, and other forms of external collaboration remain largely limited. Co-development or reuse of suptech solutions is still limited, indicating persistent barriers to pooling resources or standardising solutions internationally. Uptake of joint experimentation or innovation pilots is also low (35% limited; 29% no collaboration), and the exchange of supervisory intelligence or risk alerts remains fragmented, with 30% reporting only limited contribution and 26% no engagement. This suggests that while governance frameworks for domestic data sharing are maturing, the complex legal and architectural hurdles required for international interoperability and joint technological investment remain largely unresolved.

Suptech has contributed positively to the collaboration between financial authorities, particularly in AEs, but the extent of this contribution remains limited or moderate for most activities (Figure 45). AEs report the most success in international data-sharing (14% extensive), yet this area also shows the highest non-collaboration (32%). Suptech has further supported participation in international communities and working groups, with 45% of AEs rating its contribution as extensive, influential, or integrated, and 41% reporting similarly high levels of collaboration in cross-sectoral supervisory cooperation. EMDEs

FIGURE 44.

Collaboration With Other Financial Authorities On Supervision, SupTech, and Data-Sharing Initiatives



show significant integration in domestic data-sharing (47% rank it extensive, integrated or influential) and cross-sectoral supervisory cooperation (40%). However, the most significant barrier remains co-development or reuse of suptech solutions, where both AEs (23%) and EMDEs (40%) report the highest level of non-participation, indicating that sharing fundamental suptech code or tools is the least mature area of cross-authority engagement.

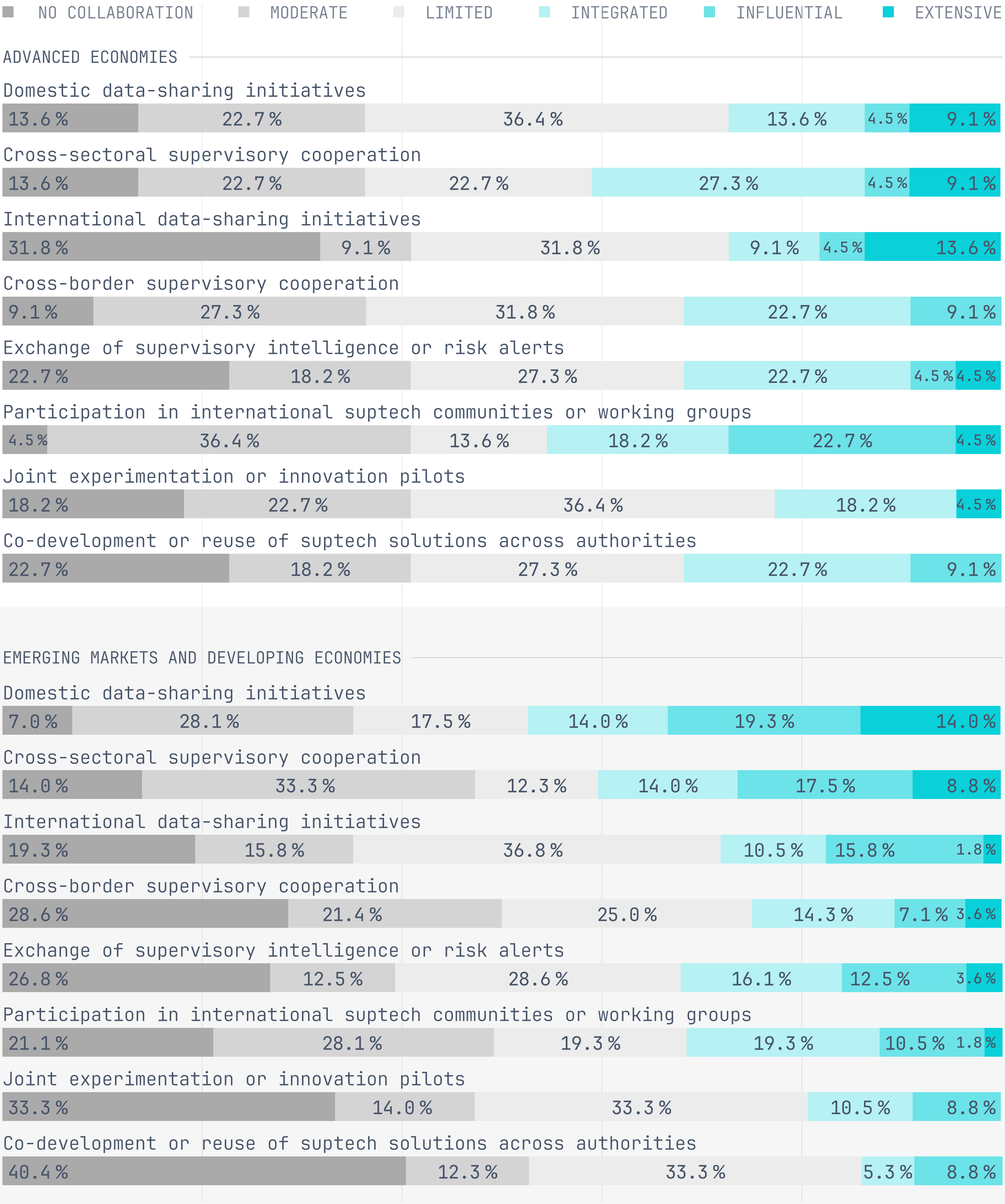
2.3.4 Budgetary resources for suptech and digital transformation

The commitment to suptech and digital transformation funding remains uneven and constrained globally, with many agencies lacking dedicated budgets, particularly for AI/GenAI, raising concerns about a potential widening digital divide. Internal budgets dominate, but few agencies report significant increases of more than 20%, while emerging markets rely heavily on external support, notably multilateral or regional development bank grants, to build capacity.

Public reporting on suptech and digital transformation budgets is sparse, making cross-jurisdictional assessment of capacity difficult, even though resource demands are recognised as a major implementation challenge by 49% of authorities (section 2.4.5). These costs vary significantly based on project scope, chosen technology, whether development is handled in-house or outsourced, and the complexity of integration with existing systems.

FIGURE 45.

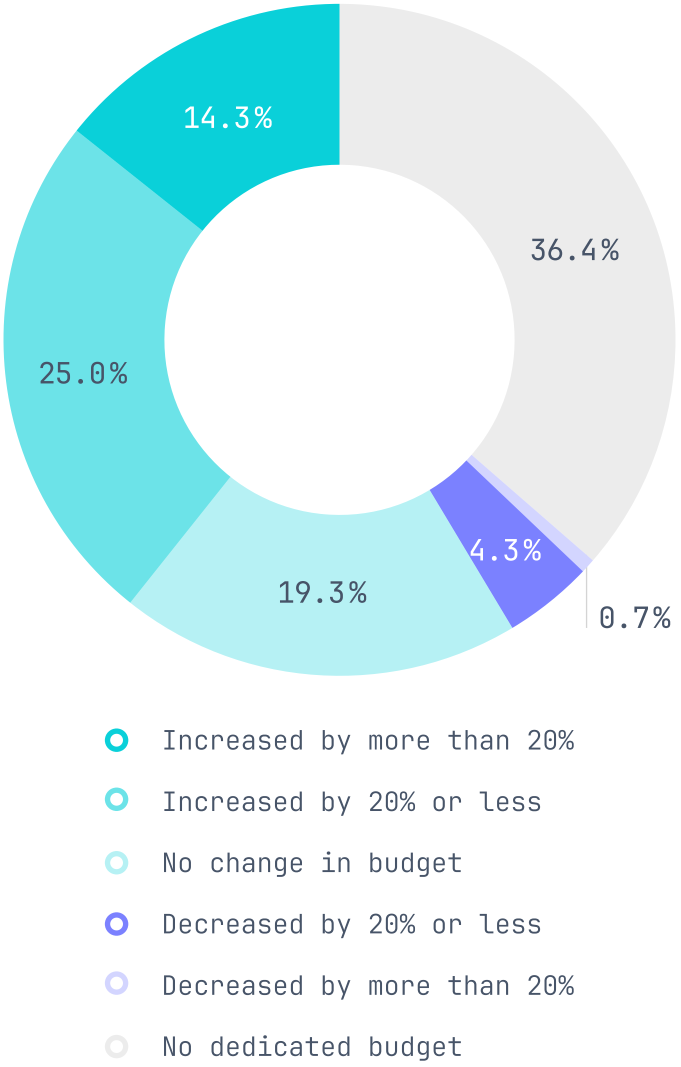
Collaboration With Other Financial Authorities On Supervision, SupTech, and Data-Sharing Initiatives By Economic Classification



Financial authorities continue to demonstrate uneven commitment to suptech and digital transformation funding. Over one-third of respondents lack a dedicated budget for these initiatives (36%), a proportion that has remained relatively high compared to 2024 (31%). Among those with allocated budgets, only 14% increased funding by more than 20%, a modest rise from 13% in 2024, and a further quarter reported increases of 20% or less. Nearly one-fifth (19%) maintained unchanged budget levels, indicating that many agencies operate with constrained or stagnant resources (Figure 46).

FIGURE 46.

How Agencies Are Adjusting Their Budget For SupTech and Digital Transformation Initiatives



These findings point to the ongoing need for enhanced philanthropic and development aid support, alongside sustained advocacy to demonstrate the strategic importance of digital transformation. Resource constraints remain evident across both advanced economies and emerging market and developing economies, indicating that budget limitations are a sector-wide challenge requiring coordinated effort to address.

The prevalent regional trend reported in 2025 was the lack of a dedicated budget for suptech or digital transformation, notably in South Asia (80%), North America (67%), EAP (41%) and SSA (40%). Where adjustments were made, modest increases of up to 20% were most common, particularly in LAC (38%), ECA (27%) and EAP (24%), while larger increases of over 20% were reported in North America (33%), SSA (23%) and MENA (23%). Few agencies reduced budgets, generally by 20% or less (Figure 47). Overall, dedicated funding remains limited, with only a minority of agencies making substantial budget changes in 2025.

Budget constraints are even more pronounced for advanced technologies (Figure 48). Nearly two-thirds of financial authorities lack explicit AI and GenAI budgets (63%). Only a small fraction increased AI funding (less than 25%, with 13% increasing by over 20%), and 10% kept budgets constant. This stark digital divide is a critical gap that threatens to exacerbate disparities between early adopters and other jurisdictions. Addressing sector-wide budget limitations requires coordinated effort, external aid, and a focus on building the strategic frameworks necessary for equitable AI adoption globally.

The financing for suptech applications is predominantly internal, a trend that remains consistent with previous years. The largest share, 67%, comes from the agency's earmarked budget, reflecting a strong institutional commitment, supported by 20% from other government programmes and 15%

FIGURE 47.

How Agencies Are Adjusting Their Budget For SupTech and Digital Transformation Initiatives By Region

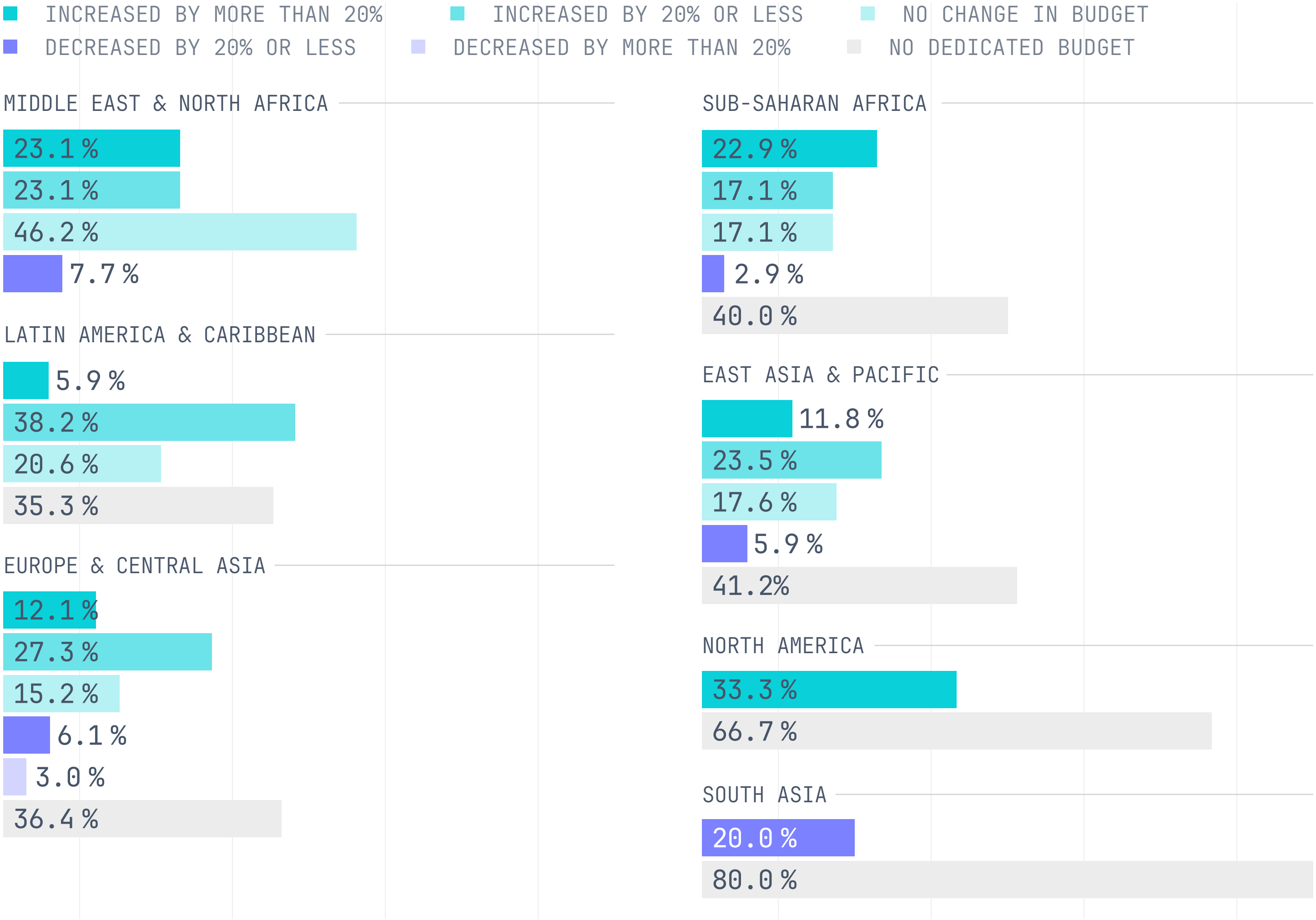
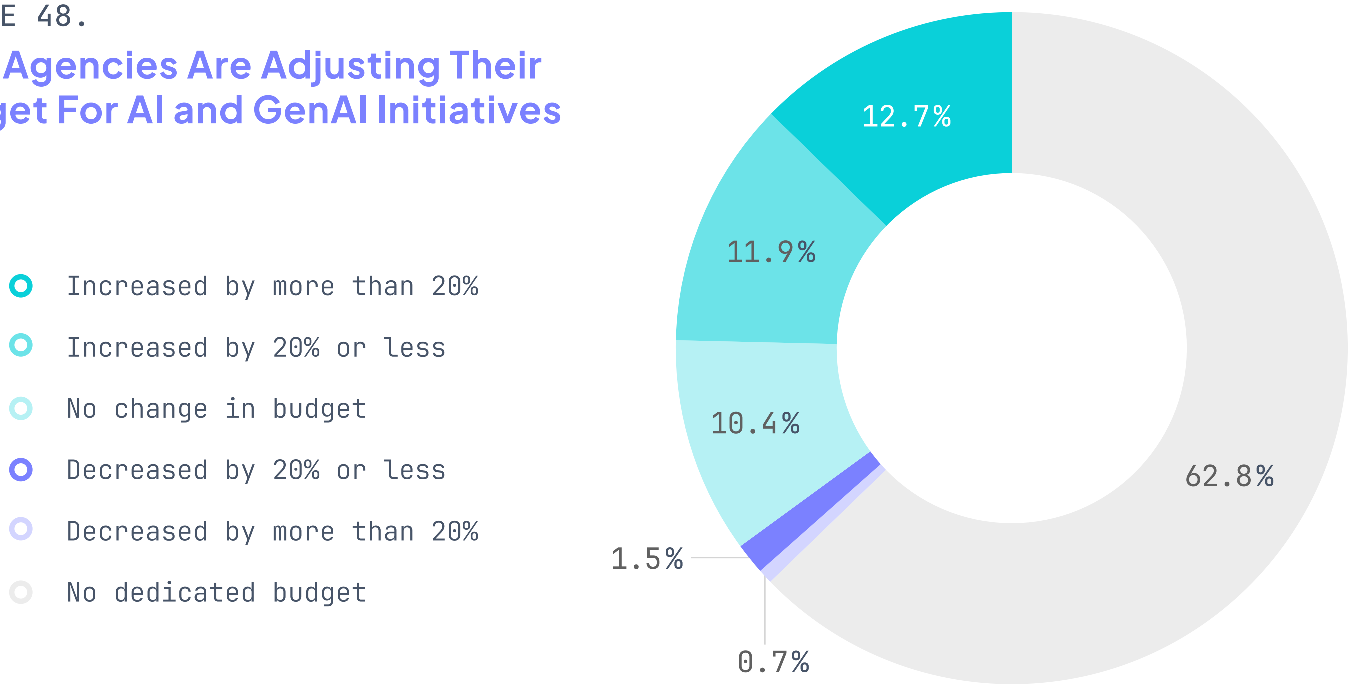


FIGURE 48.

How Agencies Are Adjusting Their Budget For AI and GenAI Initiatives

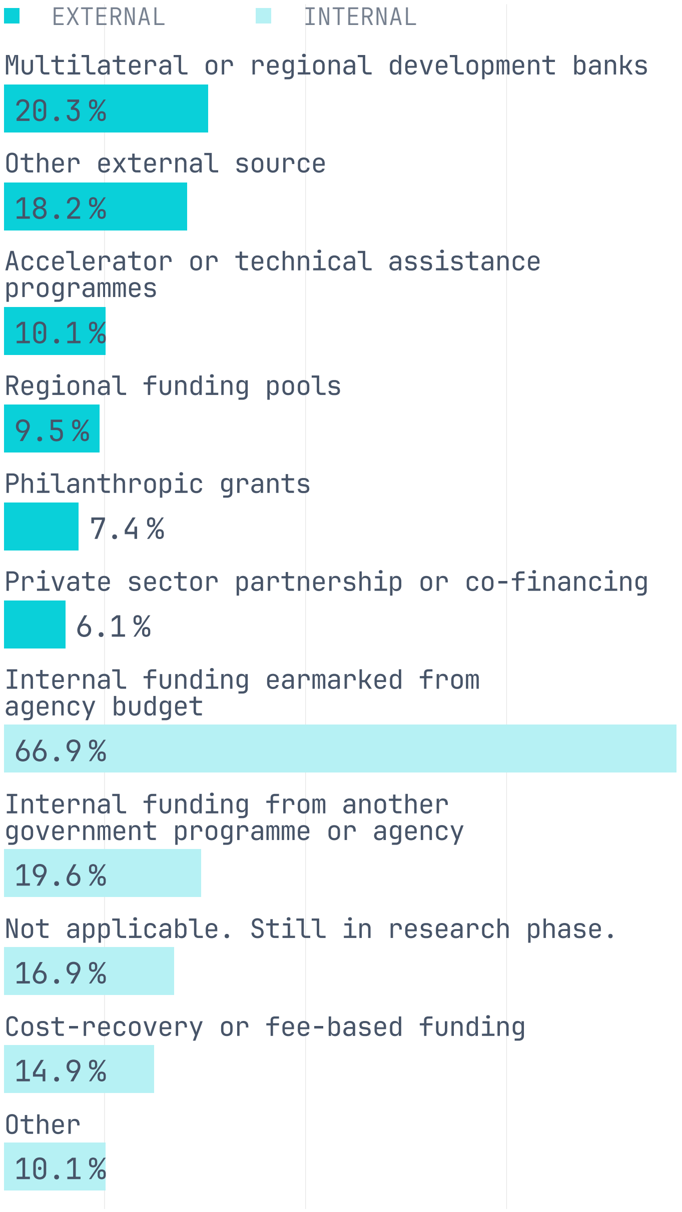


from cost-recovery or fee-based models (Figure 49). Importantly, 17% of initiatives are still in the research phase, currently requiring no deployment funds. This dominant reliance on in-house resources highlights the agency's prioritisation of supervisory technology development.

External funding sources provide essential support, particularly for resource-constrained jurisdictions. Multilateral or regional development banks represent the most significant external source at 20%, followed by other external sources (18%), accelerator or technical assistance programmes (10%), regional funding pools (9.5%), philanthropic grants (7%), and private sector partnerships (6%).

FIGURE 49.

Funding Sources For Developing and Deploying SupTech Applications



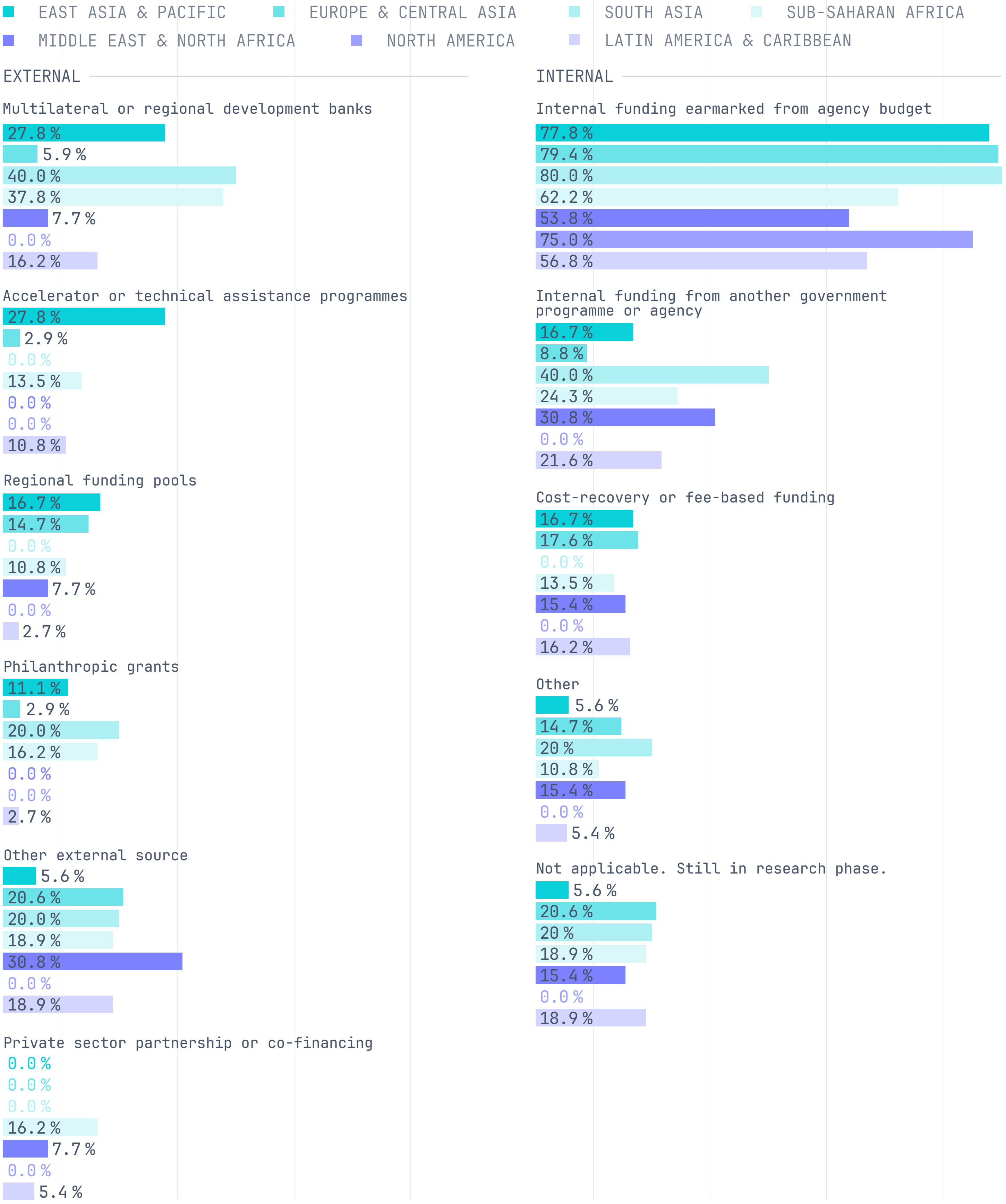
Across regions, internal funding earmarked from agency budgets is the primary source for developing and deploying suptech, dominating the funding landscape in South Asia (80%), ECA (79%), EAP (78%), and North America (75%). North American agencies report no reliance on external sources, whereas emerging markets and other regions supplement their internal budgets with external support: South Asia relies heavily on multilateral or regional development bank grants (40%), EAP draws equally from multilateral banks (28%) and accelerator or technical assistance programmes (28%), and SSA supplements its budget with multilateral banks (38%) and other external sources (19%). MENA, LAC and ECA draw significantly from other external sources (Figure 50). This indicates a pronounced divide: established economies tend to fund technological change primarily through their own budgets, whereas emerging markets more frequently depend on a mix of internal resources and international financial aid for suptech capacity building.

2.3.5 Open data governance

Open data remains weakly embedded in supervisory governance frameworks. Most authorities do not include open-data responsibilities in formal policies, and only a small minority have integrated models that define roles, controls, and publication standards. This limits their ability to manage disclosure risks, ensure data consistency, and support interoperability initiatives. As supervisors adopt machine-readable reporting and participate in broader digital-public-infrastructure efforts, clear open-

FIGURE 50.

Funding Sources For Developing and Deploying SupTech Applications By Region



data governance has become essential to balance transparency with confidentiality and security.

Open data governance remains underdeveloped across most supervisory authorities, reflecting broader gaps in institutional governance frameworks. While many agencies recognise the strategic importance of open data for transparency, market efficiency, and whole-of-government coordination, few have incorporated it into formal governance structures.

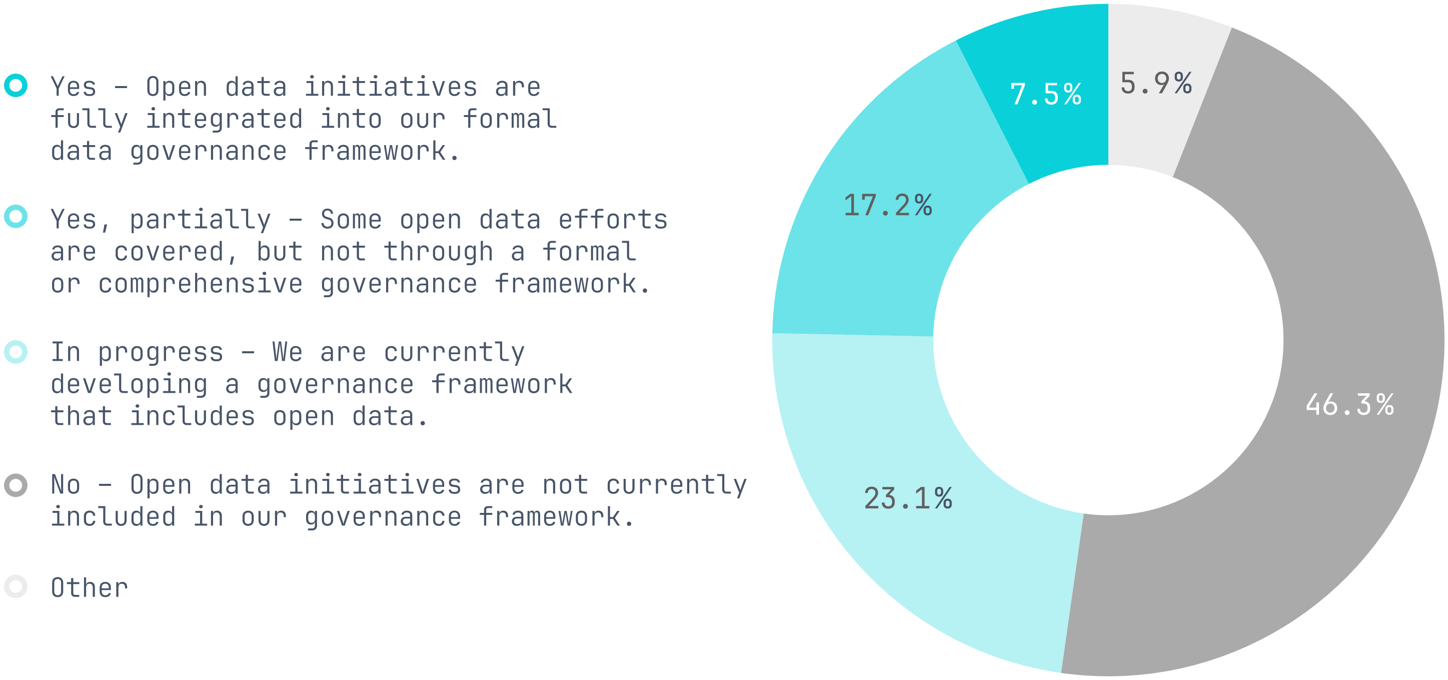
Survey data show that 46% of authorities do not include open data within their governance frameworks, while only 7.5% report full integration (Figure 51). A further 23% are developing structured approaches, and 17% have partial coverage without dedicated oversight mechanisms. These findings indicate that, although policy interest in open data is increasing, operational governance remains fragmented or informal.

This pattern mirrors the wider governance landscape identified in the State of SupTech Report 2024. Most authorities continue to operate with basic or evolving governance structures, and relatively few have established integrated models linking strategy, roles and responsibilities, risk management, and implementation. In emerging and developing economies, gaps are more pronounced due to limited resources, legacy architectures, and the absence of clear mandates for open-data stewardship.

Given the rapid expansion of digital public infrastructure and cross-agency data-sharing initiatives, the absence of structured open-data governance limits authorities' ability to standardise publication processes, manage disclosure risks, and ensure interoperability with government data platforms. As more jurisdictions adopt machine-readable reporting and open-finance frameworks, the need for robust governance covering data classification, access rules, licensing, and quality becomes increasingly critical.

FIGURE 51.

Integration of Open Data Initiatives Into Governance Frameworks



Strengthening open-data governance is therefore a foundational enabler of both suptech and broader supervisory transformation, providing clarity on what can be shared, under which conditions, and with which safeguards, while ensuring alignment with privacy, confidentiality, and security requirements.

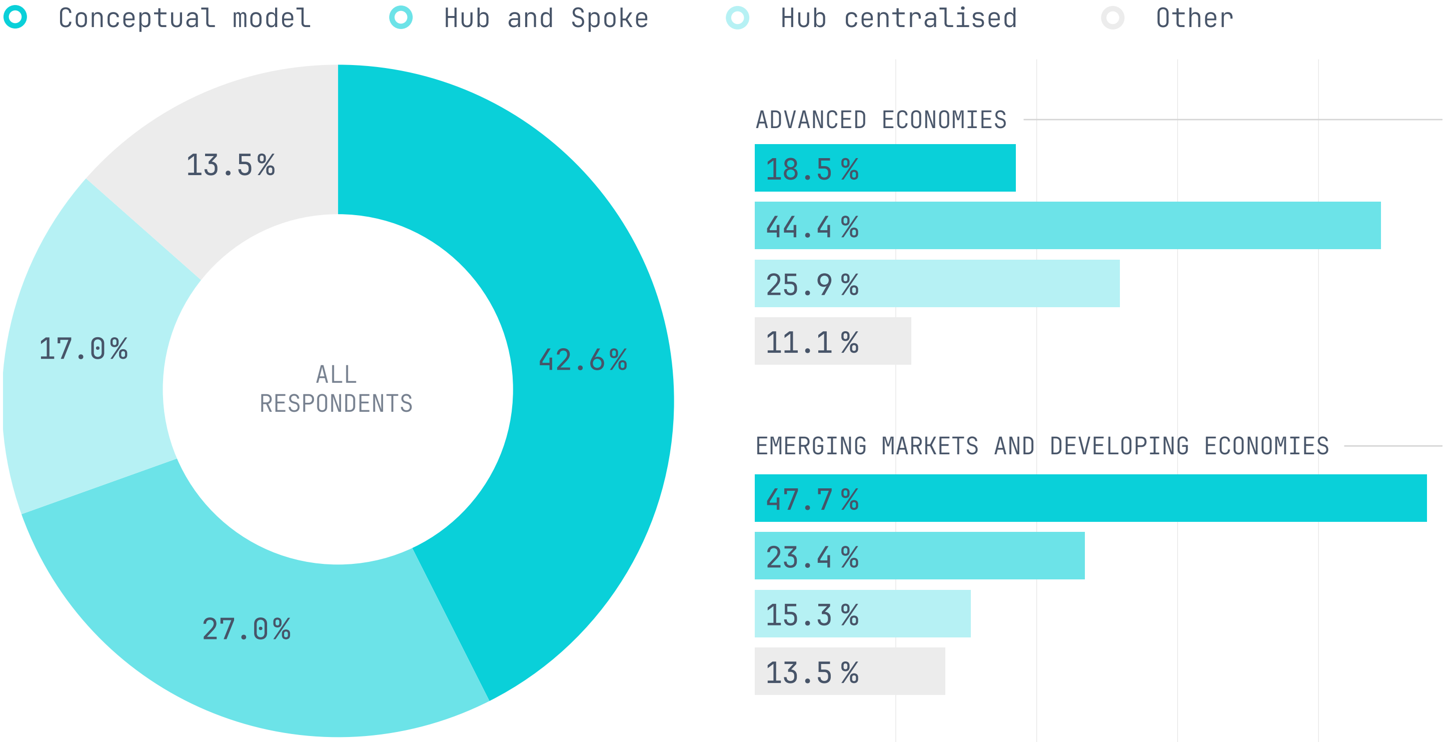
2.4 Operationalising suptech

In 2025, suptech continues to be integrated into supervisory work through increasingly structured and coordinated workflows. While the informal conceptual model remains dominant, there is a steady shift toward structured, hybrid approaches, particularly in AEs, whereas EMDEs still rely largely on informal arrangements. Dedicated suptech units are becoming more common, yet many EMDEs continue to lack formal data science capabilities, underscoring persistent capacity gaps.

The successful operationalisation of suptech hinges on structured coordination between supervisory expertise, IT functions, and data science capabilities to translate strategic intent into day-to-day supervisory practice. It requires aligning organisational structures with people and processes: many agencies are building multidisciplinary teams that combine supervisory, data, and engineering expertise, and investing in capacity-building programmes that keep pace with AI-enabled methods. It also entails establishing repeatable approaches to product design and delivery, addressing persistent design and implementation challenges, and using procurement and ecosystem partnerships to augment internal capacity where needed. The subsections that follow examine how authorities are organising operating models and teams, strengthening skills and training, structuring development work, and engaging external providers to embed suptech in routine supervision.

FIGURE 52.

Organisational Models For Development By Economic Classification



2.4.1 Operational models for suptech delivery

Suptech coordination remains centred on three models — decentralised (conceptual), centralised hub, and hybrid hub-and-spoke — with the conceptual model still dominant in 2025, particularly in EMDEs, while AEs more often use hub-and-spoke. Hybrid arrangements continue to gain traction as authorities establish dedicated suptech and data-science teams, balancing central oversight with embedded expertise. The share of agencies without a dedicated unit has fallen to 38%, and medium-to-large teams have increased from 17% in 2024 to 28% in 2025, reflecting a shift toward more coordinated and scalable organisational structures.

Financial authorities generally adopt one of three models: decentralised (conceptual), centralised hub, and hybrid hub-and-spoke, which dictate collaboration, piloting, scaling, and alignment with priorities (Figure 52).

In 2025, the prevalent approach remains the conceptual model (43%), characterised by direct collaboration between the IT department and the business unit for initiative selection and implementation. This mirrors the 2024 trend closely and reflects continued reliance on flexible, informal structures.

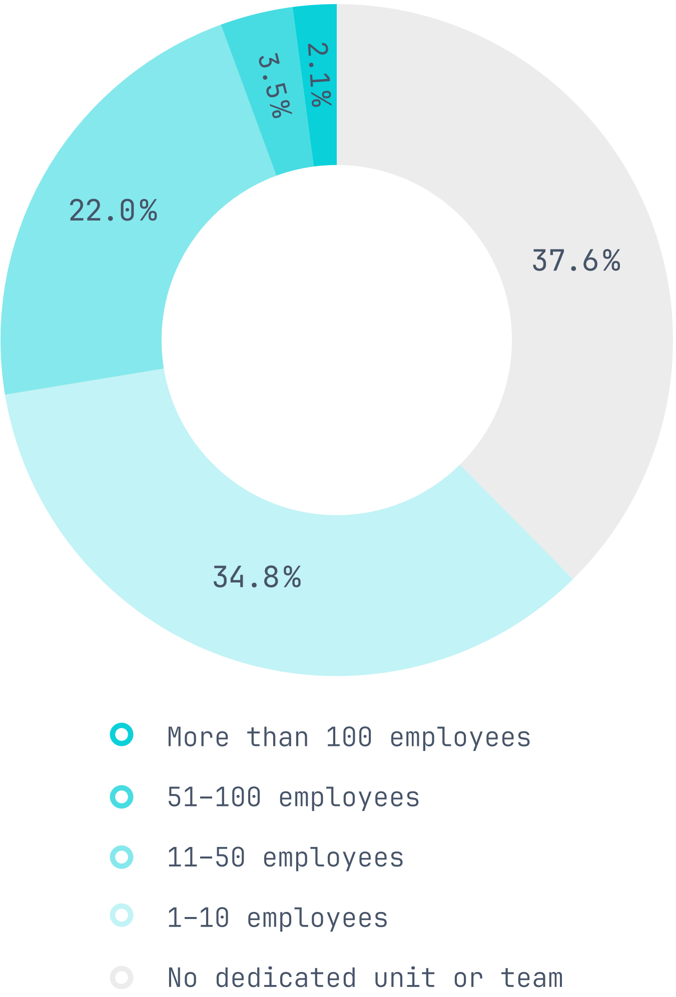
The hub-and-spoke model (27%), adopted for example by the ECB, is the second most common, where the business unit submits initiatives to a central hub (in IT or a dedicated suptech unit), promoting cross-unit project creation. The hub centralised model (17%) involves a dedicated governance structure or department selecting initiatives. Other arrangements (14%) include management-driven selection, joint development with vendors, or standalone development cells. The findings are consistent with the 2024 data.

Nearly half (44%) AE agencies operate a hub-and-spoke model and another 26% use a centralised hub. EMDE authorities, by contrast, lean toward decentralised structures and predominantly rely on conceptual models (48%), indicating that suptech often remains informal or not yet fully defined; only 23% have adopted a hub-and-spoke approach. This pattern is consistent with a greater reliance on flexible or transitional arrangements as EMDEs continue developing internal capacity.

Dedicated suptech capacity is steadily emerging across surveyed financial authorities, with the proportion reporting no dedicated unit falling to 38% in 2025 (Figure 53), down from

FIGURE 53.

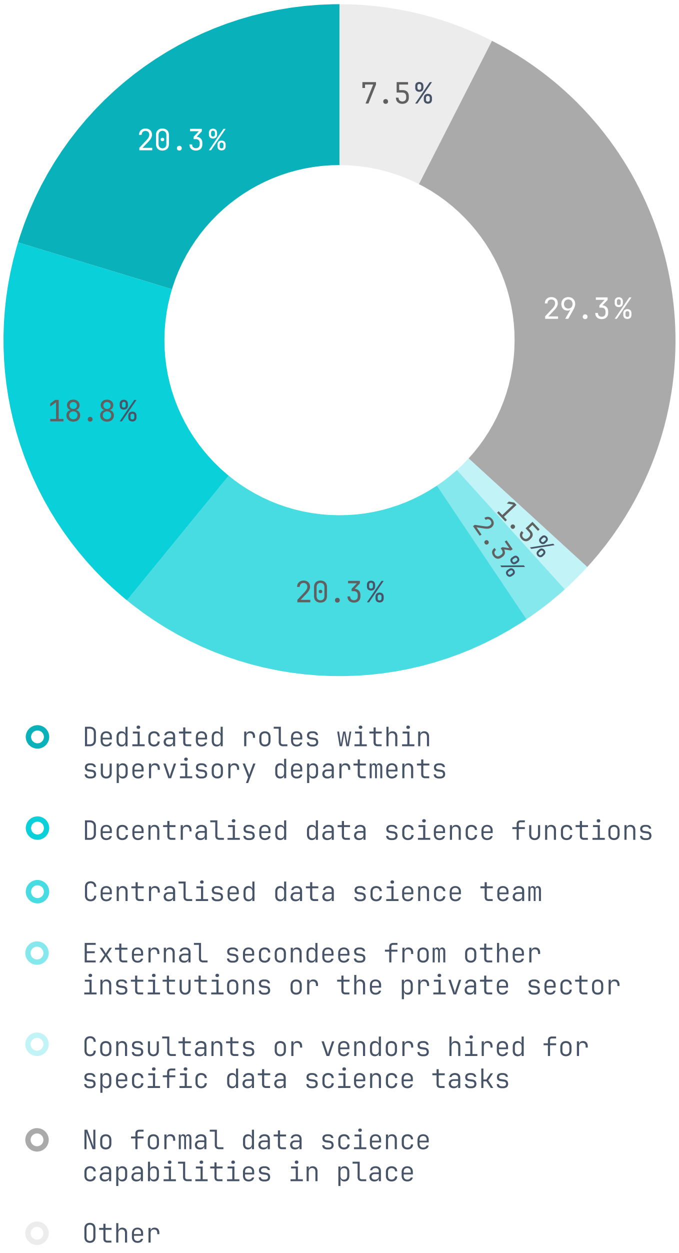
Number of Employees of the SupTech Unit or the Dedicated Unit in the IT or Other Department



46% in 2024. Most existing teams remain small, with 1–10 employees (35%). However, there is a clear trend towards expansion: medium-sized teams (11–50 employees) rose from 15% in 2024 to 22% in 2025, while very large teams (over 50 employees) increased from 2% to 6% over the same period. Overall, the data suggests a gradual move towards establishing and modestly scaling dedicated suptech teams across financial authorities.

FIGURE 54.

Distribution of Data Science Capabilities Across the Agency



Most authorities with data science capabilities either maintain centralised teams (20%) or embed dedicated roles within supervisory departments (20%), with another 19% operating decentralised functions, reflecting a strong focus on building internal expertise (Figure 54). 29% still have no formal data science functions, and reliance on external support remains very low, with consultants and secondees each at 2%. “Other” arrangements such as hybrid models like central departments combined with embedded staff or hub-and-spoke structures, account for 8%.

The organisation of data science capabilities reveals a significant gap in formalisation and maturity between economic groups (Figure 55). AEs tend to adopt structured, formalised models, with a centralised data science team being most common (33%), closely followed by dedicated roles within supervisory departments (29%). By contrast, over a third of EMDEs (35%) report having no formal data science capabilities. Where capabilities exist, they are often fragmented: only 19% have dedicated roles and 18% maintain a centralised team, indicating that many EMDE agencies are still in the early stages of integrating data science into their operations.

2.4.2 Skills and capabilities

Developing and maintaining an appropriate blend of technical, data, and design skills is important for effective suptech operationalisation. While agencies generally have strong foundations in data management, software engineering, and project management, expertise in advanced analytics and user-focused design remains limited. Efforts increasingly target capacity building, cross-team collaboration, and AI and data science development, supported by digital platforms and peer-learning. Gaps persist, particularly in EMDEs, highlighting the need to strengthen internal capabilities to make fuller use of suptech applications.

FIGURE 55.

Distribution of Data Science Capabilities Across the Agency

By Economic Classification

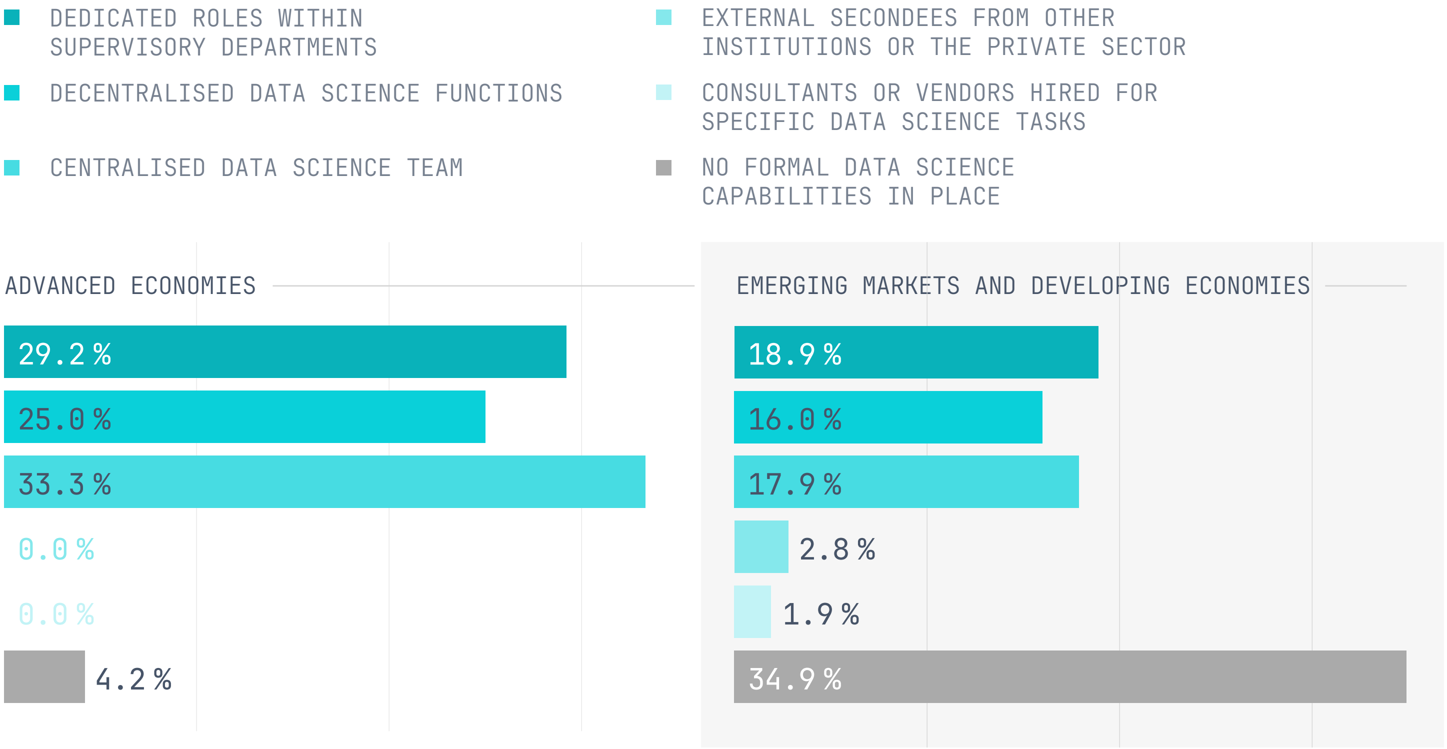
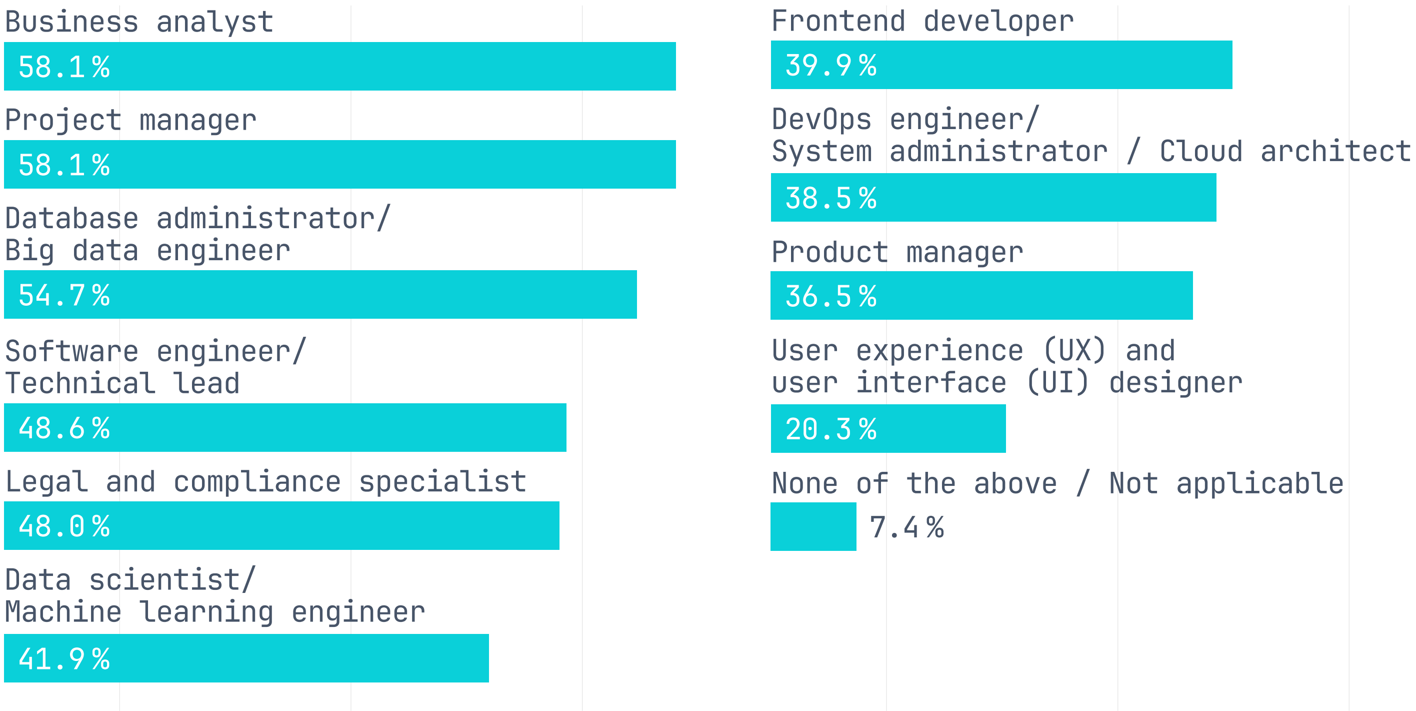


FIGURE 56.

Skills Available Within the Agency

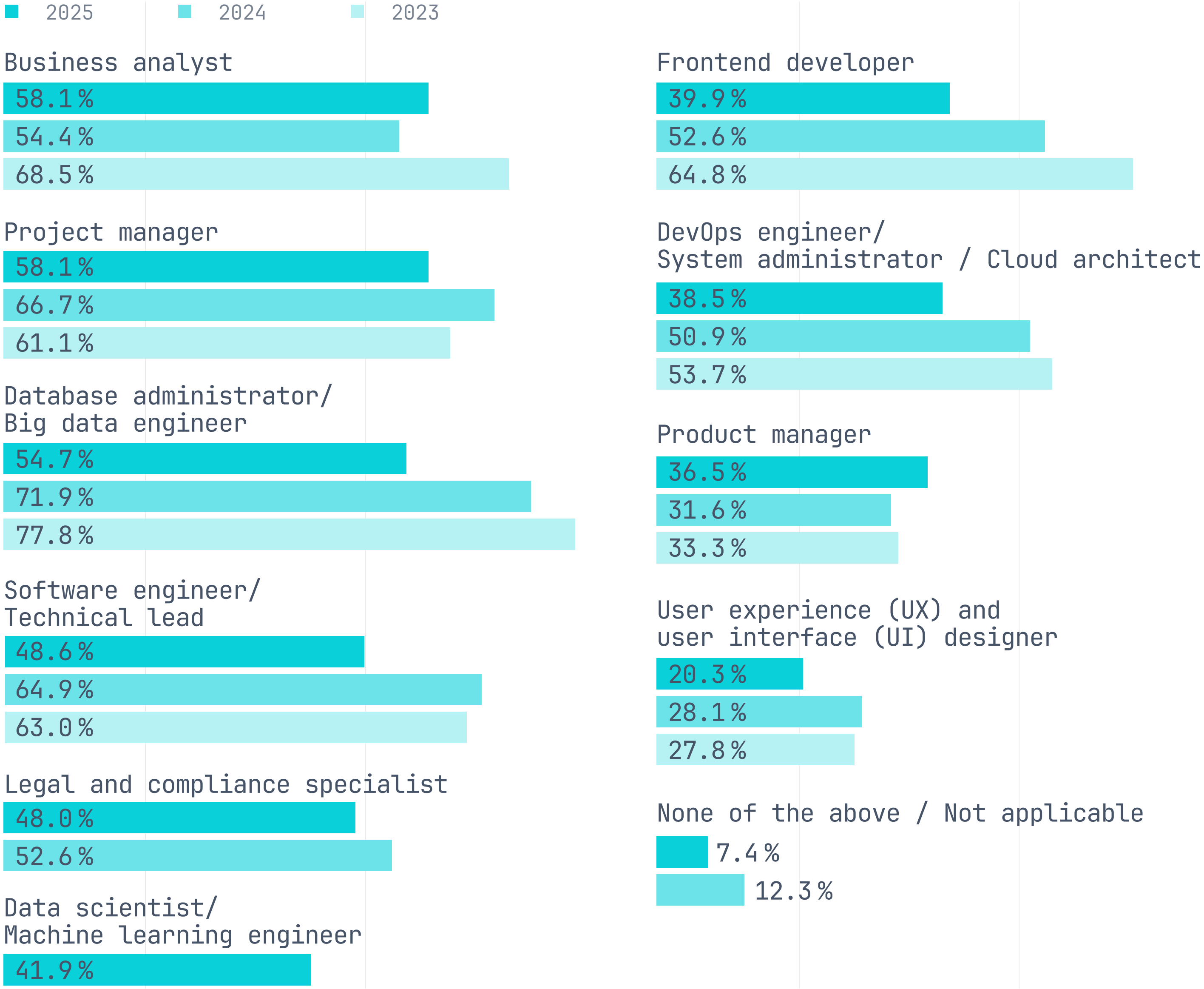


The 2025 State of SupTech survey results show that financial authorities possess a solid foundation of essential skills to support suptech development, deployment and maintenance, led primarily by roles necessary for planning and foundational data management. The most widely available skillsets, present in over half of the agencies, are business analysts (58%) and project managers (58%), closely followed by the database administrators and big data engineers (55%) (Figure 56). This suggests comparatively strong institutional capacity for defining requirements and managing data infrastructure.

Core technical development roles, such as software engineer/technical lead (49%), and essential oversight functions, including legal and compliance specialist (48%), show moderate availability. However, specialist expertise in advanced analytics, specifically data scientist/machine learning engineer (42%), is available in fewer than half of the surveyed institutions. Skills related to deployment, user experience, and product management are the least available, particularly the user experience (UX) and user interface (UI) designer (20%). Only 7% report having none of these skills, indicating that while

FIGURE 57.

Skills Available Within the Agency 2023–2025



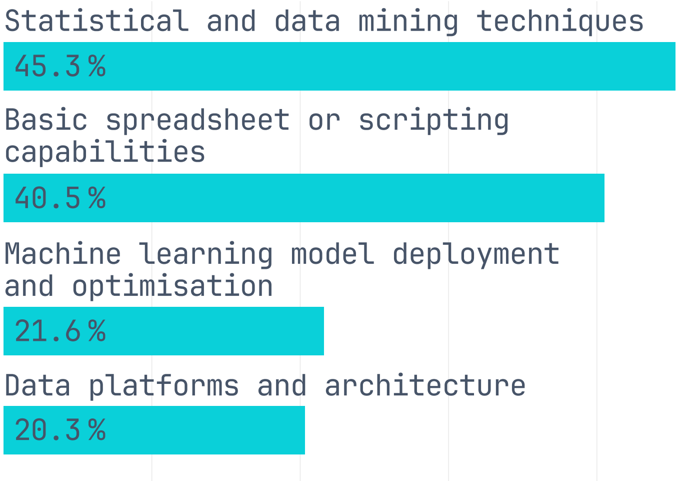
foundational planning and data management are widespread, deep specialisation in advanced analytics and user-centric design remains a notable internal gap.

Between 2023 and 2025, the relative prominence of suptech skills shifted among surveyed authorities (Figure 57). Database administration was initially the most widely cited role, but over time, business analyst and project management functions have become more central, while newer specialisms such as data science and machine learning are gradually gaining relevance. Meanwhile, user-focused design and systems administration remain less prominent, highlighting persistent gaps in certain capabilities needed to support suptech adoption.

Supervisory authorities show moderate proficiency in foundational data science, with 45% skilled in statistical and data mining techniques, capable of manipulating datasets and building models using tools like R, Python, or SQL, and 41% proficient in basic spreadsheet or scripting tasks for data transformation and reporting (Figure 58). However, advanced technical skills remain limited, with only 22% able to deploy machine learning models using cloud infrastructure, streaming pipelines, and ML Ops practices, and 20% skilled in managing data platforms and architecture, including scalable frameworks and API integration, highlighting a key gap in translating analytical ability into operational suptech solutions.

FIGURE 58.

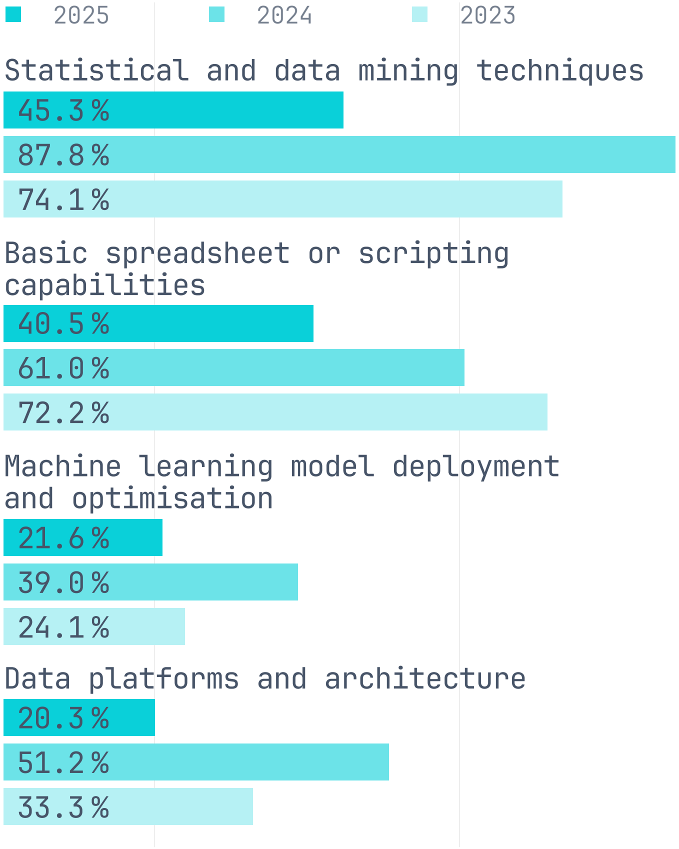
Skill Level of Data Scientists and Analysts



Over the 2023-2025 period, foundational analytical skills (statistical/data mining and basic scripting) have consistently been the most prominent capabilities within supervisory authorities, despite a shift in their relative standing figures (Figure 59). Conversely, advanced technical skills, such as data platform management, remain limited. The ability to perform machine learning model deployment has shown a modest growth in relative terms, moving out of the lowest reported category and signalling gradual progress in operationalising analytical models.

FIGURE 59.

Skill Level of Data Scientists and Analysts 2023-2025



2.4.3 Capacity building programmes and external support

Financial authorities are increasingly investing in training to advance their suptech and digital transformation goals, concentrating on technical and risk areas, particularly cybersecurity, AI, and data science, while expertise in user-focused and innovation skills remains limited. While authorities in AEs are refining mature capabilities and engaging with cutting-edge topics, those in EMDEs are building essential technical and operational foundations, with strong demand for further training. Data science programmes reflect this maturity gap, focusing primarily on foundational coding, while advanced skills like model deployment, governance, and bias detection are still rare, underscoring gaps in capabilities needed to operationalise ethical and scalable suptech solutions.

Supervisory authorities are actively engaging in capacity building programmes related to suptech, with training predominantly focused on technical and risk-related areas. Cybersecurity and ICT risk is the most common topic (61%), followed by AI and machine learning (52%) and data science and analytics (49%). Other frequently addressed areas include AML (47%), data governance, and fintech (43% each), while emerging topics such as cloud adoption, digital assets, ESG, and digital identity are covered less extensively. Training on suptech-specific technologies and toolkits is moderately common (39%), whereas user-centred and innovation-focused skills, including human-centred design (22%) and product lifecycle innovation (18%), remain limited. Nearly 30% of authorities have not yet undertaken such programmes but express strong interest, indicating potential for broader sector-wide engagement (Figure 60).

Capacity building efforts reveal distinct priorities between economic groups, though both focus heavily on core technological skills (Figure 61). AEs focused heavily on advanced technical skills, particularly AI (64%), data science (61%), cloud adoption (61%), and cybersecurity (54%), while also investing in methods such as suptech toolkits (43%), innovation leadership (32%), and design sprints (32%). EMDEs prioritise immediate risk and compliance needs, focusing first on cybersecurity and ICT risk (62%) and AML/CFT/PF (50%), with AI/ML and data Science following closely behind (48% each), alongside data governance and fintech (each 44%), supported by tools-focused efforts such as suptech toolkits (39%), innovation leadership (28%) and human-centred design (23%). 30% of EMDEs express interest in undertaking capacity programmes but have not yet done so, compared to a smaller 18% of AEs. This pattern suggests a greater unmet demand for skills enhancement in emerging markets.

Expanding on data science training, supervisory authorities' programmes are currently focused on foundational programming and introductory primers rather than advanced deployment or ethical considerations. The most common programmes cover programming in Python, R, or

FIGURE 60.

Demand For Training or Capacity Development Programmes Related to SupTech or Digital Transformation

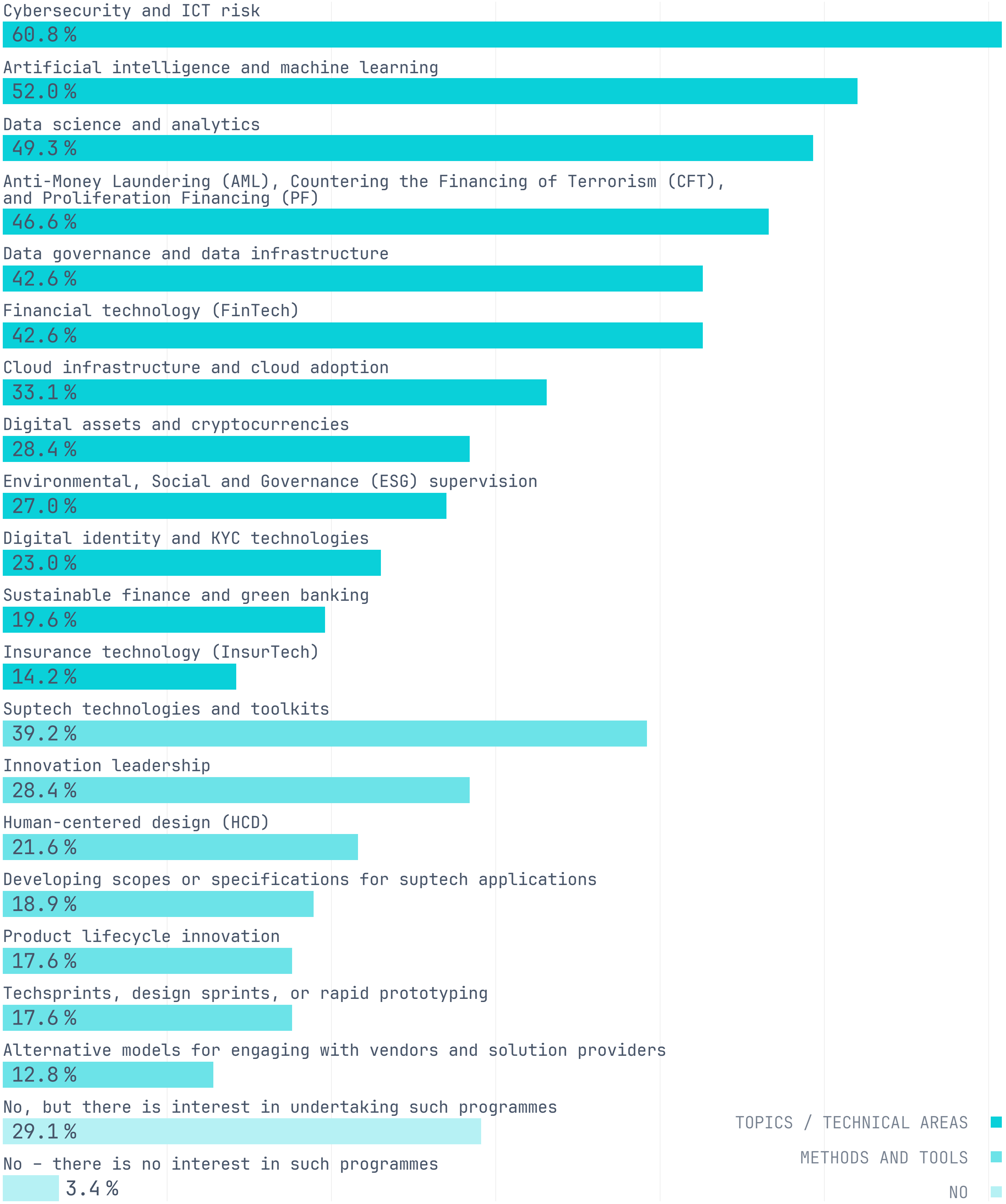


FIGURE 61.

Demand For Training or Capacity Development Programmes Related to SupTech or Digital Transformation By Economic Classification

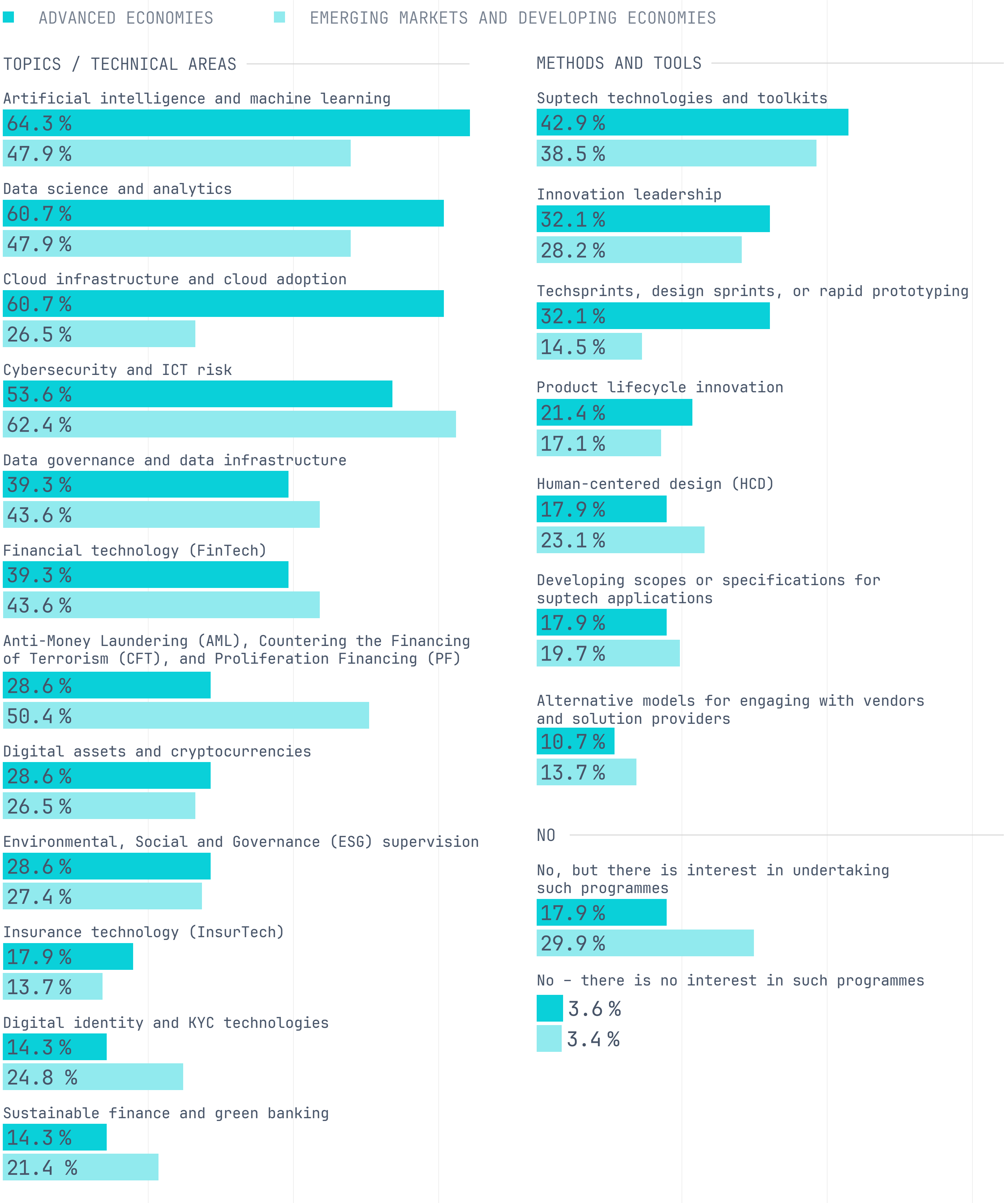
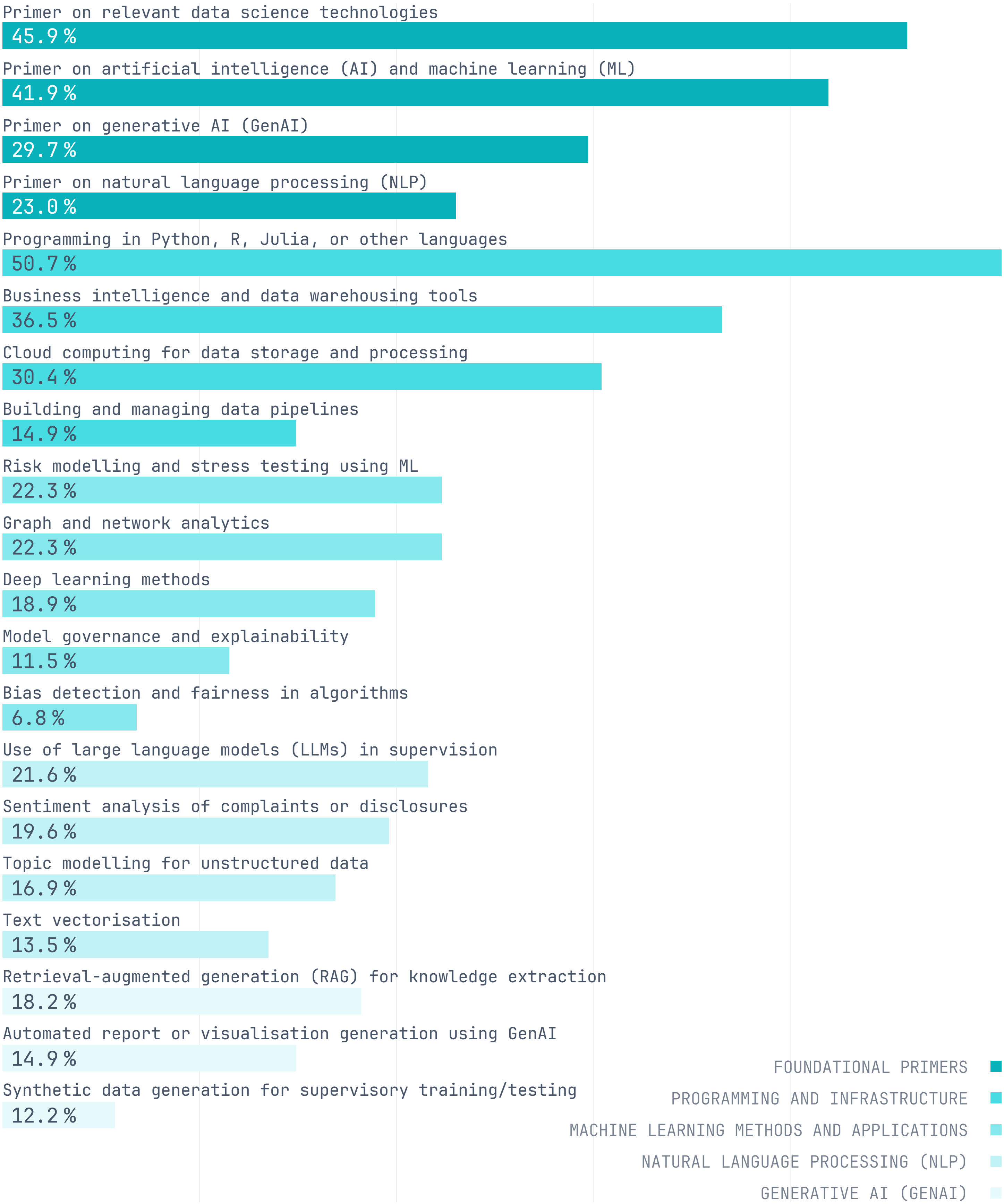


FIGURE 62.

Demand For Skills and Capacity Development Programmes on Data Science for SupTech Applications



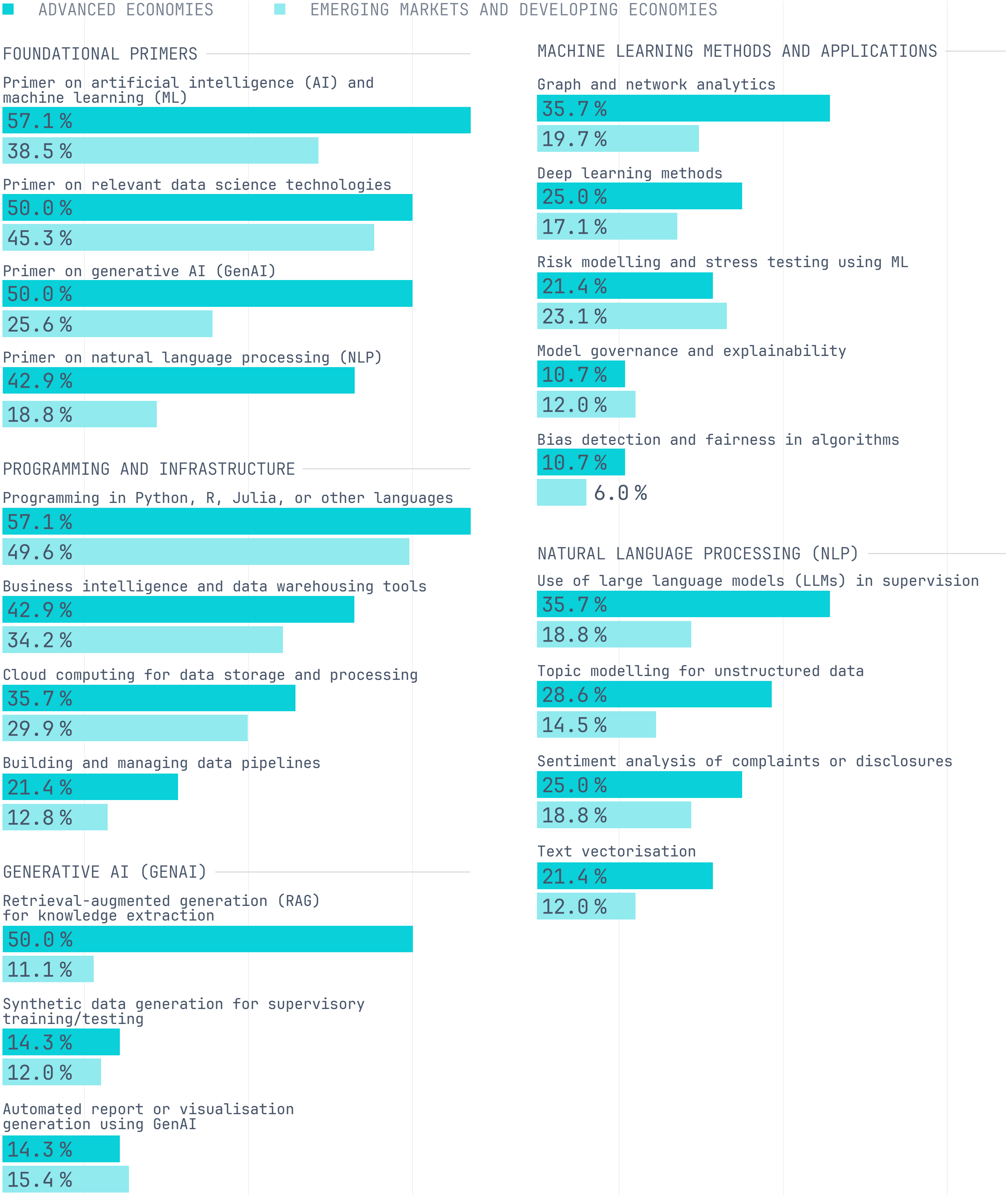
similar languages (51%), followed by primers on relevant data science technologies (46%) and AI and machine learning (42%) (Figure 62). However, participation declines significantly for highly technical and specialised applications: building and managing data pipelines is covered by only 15% of teams. Similarly, advanced topics like model governance and explainability (12%), and bias detection and fairness in algorithms (7%) are rare, indicating that the sector is still primarily building basic coding skills and awareness of new technologies, while neglecting the critical areas of model production, governance, and ethical deployment necessary for mature suptech applications.

The divide between economic groups is clear. AEs prioritise higher-end capabilities, including AI/ML training (57%), GenAI primers (50%), and practical GenAI techniques such as RAG (50%), alongside core programming (57%). EMDEs, by contrast, focus on fundamentals, with programming (50%) and data-science primers (45%) dominating their training portfolios. Yet both groups show limited emphasis on governance-critical skills such as model explainability or fairness, remaining below 13%, highlighting a global gap in preparing supervisory staff for ethical, responsible, and scalable use of advanced suptech models (Figure 63).

Platforms such as GovSpace Transform — where the AI Gymnasium where the AI Gymnasium MVP has been used by more than 300 individuals to create hundreds of capstone projects and prototypes — illustrate how digital environments can support collaborative AI/ML training, experimentation, and solution prototyping. The observations above highlight that capacity development is essential for both suptech and data science. The early traction seen in digital platforms such as GovSpace complements these findings, and further suggests that such tools may have strong potential to meet this growing demand.

FIGURE 63.

Skills and Capacity Development Programmes on Data Science for SupTech Applications By Economic Classification



2.4.4 Approaches to product development

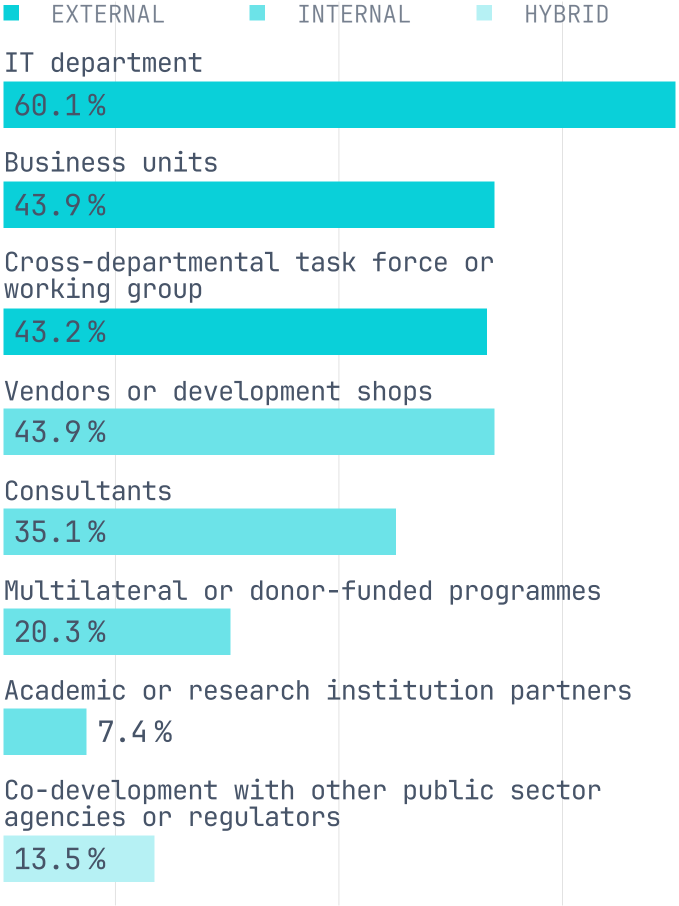
Suptech product development is primarily driven by internal teams, with IT departments, business units, and cross-departmental groups playing central roles. External support remains important, especially from vendors and consultants. Advanced economies rely more heavily on internal capabilities and specialised consulting support, whereas EMDEs balance internal development with vendor engagement and depend more frequently on multilateral or donor-funded programmes.

The skills and training profiles discussed in the previous sections directly influence how authorities organise product development and determine the balance between internal execution and external support. Where data science, engineering, and user-centred design capabilities are stronger, authorities tend to rely more heavily on internal teams; where gaps persist, they compensate through vendors, consultants, and donor-supported technical assistance.

Globally, internal teams remain the primary drivers of suptech development. IT departments lead in 60% of agencies, closely followed by business units (44%) and cross-departmental working groups (43%). This strong internal role is consistent with a preference to align solutions with supervisory needs and to build lasting institutional ownership. At the same time, external actors play an essential complementary role: vendors or development shops are engaged by 44% of authorities and consultants by 35%, providing specialised expertise or additional development capacity where internal skills are limited (Figure 64).

FIGURE 64.

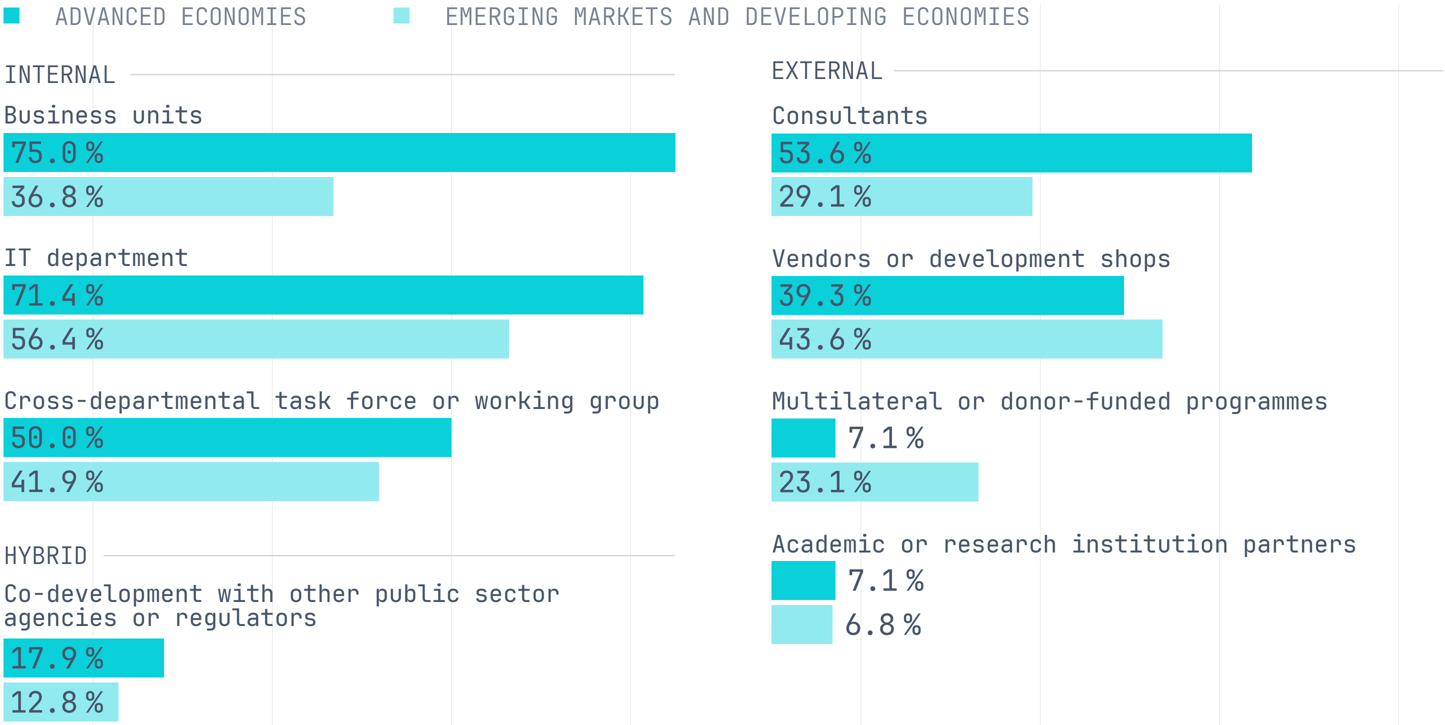
Product Development Approaches For SupTech



The nature of this involvement varies significantly by economic group. AEs rely heavily on internal resources, particularly business units (75%) and IT departments (71%), and draw on consultants (54%) for specialised, high-level expertise. EMDEs take a more balanced approach, splitting responsibility between internal IT functions (56%) and external vendors (44%), and demonstrate far greater dependence on institutional aid: nearly a quarter (23%) involve multilateral or donor-funded programmes, compared with just 7% of AEs, highlighting the important role of international support in strengthening capacity (Figure 65).

FIGURE 65.

Product Development Approaches For SupTech By Economic Classification By Economic Classification



2.4.5 Applications design and implementation

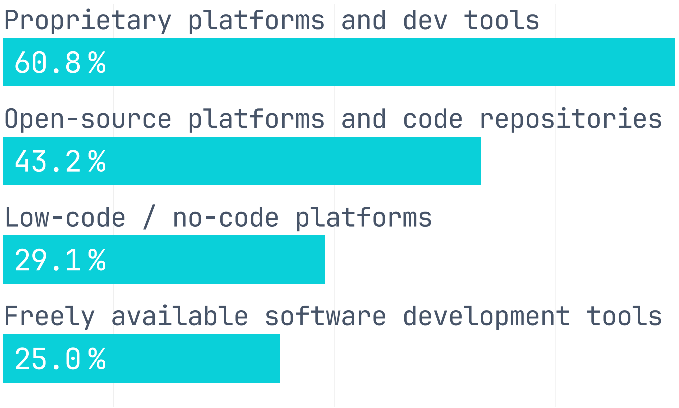
Authorities continue to face significant hurdles in both the design and implementation of suptech applications in 2025. While the drive toward digital supervision remains strong, progress is constrained by persistent internal challenges, most notably data quality issues, limited resources, and shortages of specialised talent, suggesting that many of these barriers may be systemic rather than regulatory. Both AE and EMDE agencies face intertwined design and operational obstacles, but AEs contend more with sophisticated coordination and regulatory issues, whereas EMDEs struggle with capacity and resource limitations.

The continuing drive toward digital supervision has been accompanied by the development of a broad spectrum of tools to design and develop suptech solutions. Proprietary platforms and development tools are the clear preference, utilised by nearly two-thirds of the surveyed authorities (61%). This widespread use is closely followed by reliance on open-source platforms and code repositories, which a significant proportion (43%) employ. Demonstrating a push for efficiency and accessibility, low-code/no-code platforms and freely available software development tools are also leveraged by over a quarter of authorities (29% and 25%, respectively). Beyond the standard categories, the "Other" tools specified reflect diverse, project-specific choices; from development platforms like Python, Django, Vue.js, GitLab, Docker, Figma, and Jira to specialised data and automation tools such as KNIME and n8n. The adoption of AI systems like Anthropic Claude is consistent with a trend toward more data-driven approaches to suptech development.

Despite this robust engagement with diverse technologies, the design and implementation of suptech applications continues to be a

FIGURE 66.

Tools Used For Designing and Developing SupTech Solutions



challenge for many financial authorities. Progress is consistently constrained by persistent internal challenges that are largely systemic rather than regulatory. These key internal constraints include poor data quality, limited resources, and a shortage of specialised talent.

Design-related challenges are led by data quality issues (49%) and difficulties in attracting or retaining relevant staff (43%). These obstacles are compounded by lengthy production cycles (42%) and a lack of product design expertise (41%), as well misalignment between organisational cultures and innovative design approaches (38%).

On the implementation front, agencies cite resource-intensive deployment (49%), cost-related pressures (43%), limited internal IT capacity (40%), and procurement limitations (39%) as major impediments. Systemic obstacles such as legacy IT systems (36%) remain a significant barrier to scalability and efficiency. Overall, survey responses indicate that internal capacity and infrastructure limitations are more frequently cited than external or regulatory barriers.

These design and implementation challenges differ in intensity across economies (Figure 68). In AEs, design hurdles centre on internal efficiency and human capital: long production cycles (50%), data quality issues (46%), and talent retention (43%) are key concerns. Implementation is primarily hindered by bureaucratic and infrastructural constraints: resource-intensive deployment (57%), procurement constraints (57%), legacy IT systems (50%), and legal or regulatory barriers (43%) are the most prominent obstacles, with cost pressures (32%) and vendor lock-in (29%) also affecting many agencies.

EMDEs report broadly similar design challenges, with data quality (50%), talent shortages (43%), and limited internal expertise (43%) being the most common. However, their implementation struggles are heavily resource and capacity-driven: the primary hurdles are resource intensity (46%), cost constraints (45%), limited internal IT capacity (41%), and insufficient analytics skills (40%). While AEs contend more with sophisticated coordination and regulatory issues, EMDEs primarily struggle with securing the fundamental capacity and resources needed for adoption.

2.4.6 Procurement and collaboration models to engage with suptech solution providers and the broader ecosystem

Financial authorities largely rely on traditional, structured procurement to engage external providers for suptech, with most using requests for proposal (60%) or formal tenders (45%) and over half employing cross-departmental evaluation committees to ensure strong internal oversight. While approaches like regulatory sandboxes and tech sprints are being explored, they remain secondary, indicating a preference for risk-managed, competitive sourcing over agile or co-creation models.

Financial authorities primarily engage with external providers using traditional, formal procurement methods, while moderately

FIGURE 67.

Challenges In Designing and Implementing SupTech Applications

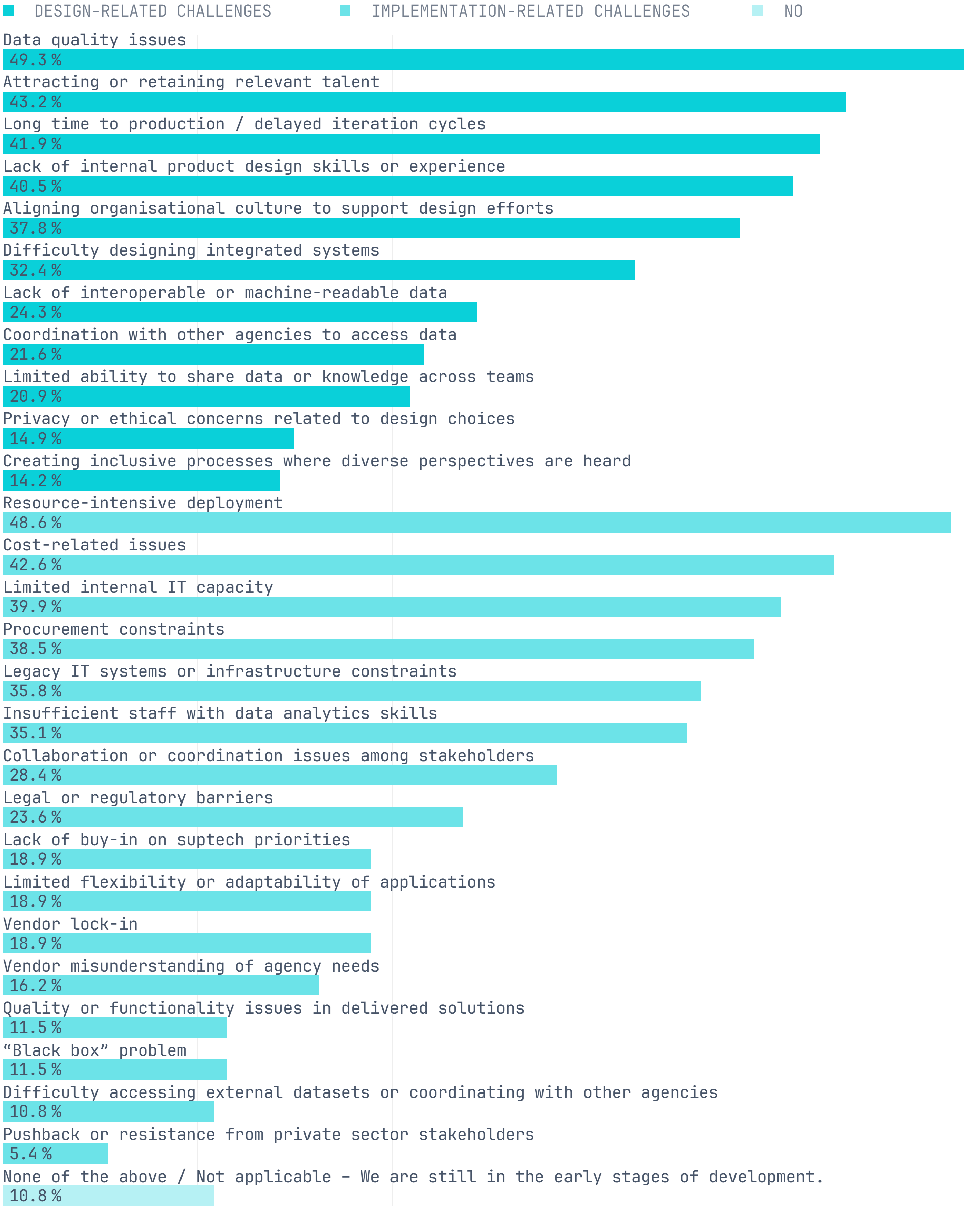


FIGURE 68.

Challenges In Designing and Implementing SupTech Applications

By Economic Classification

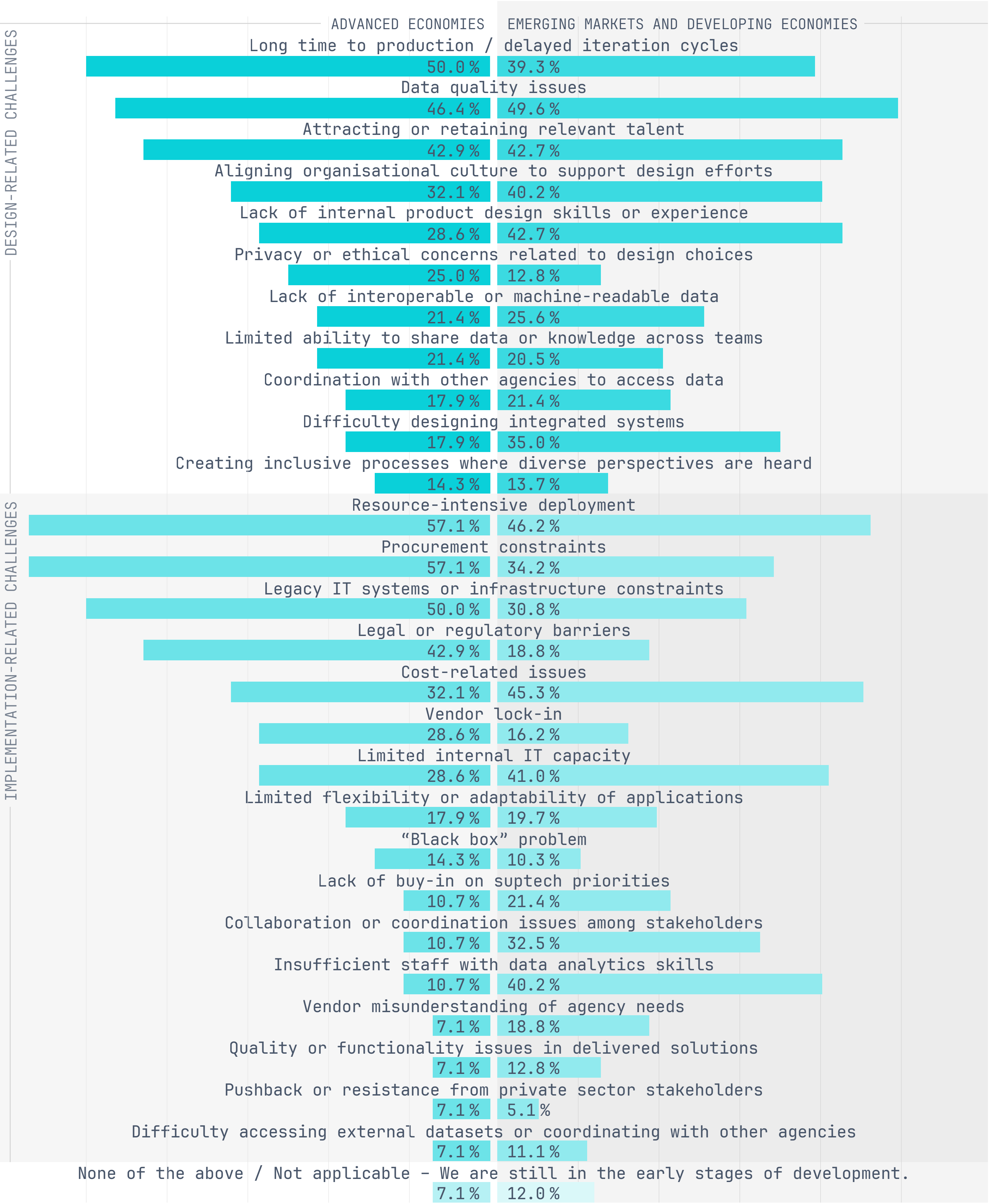
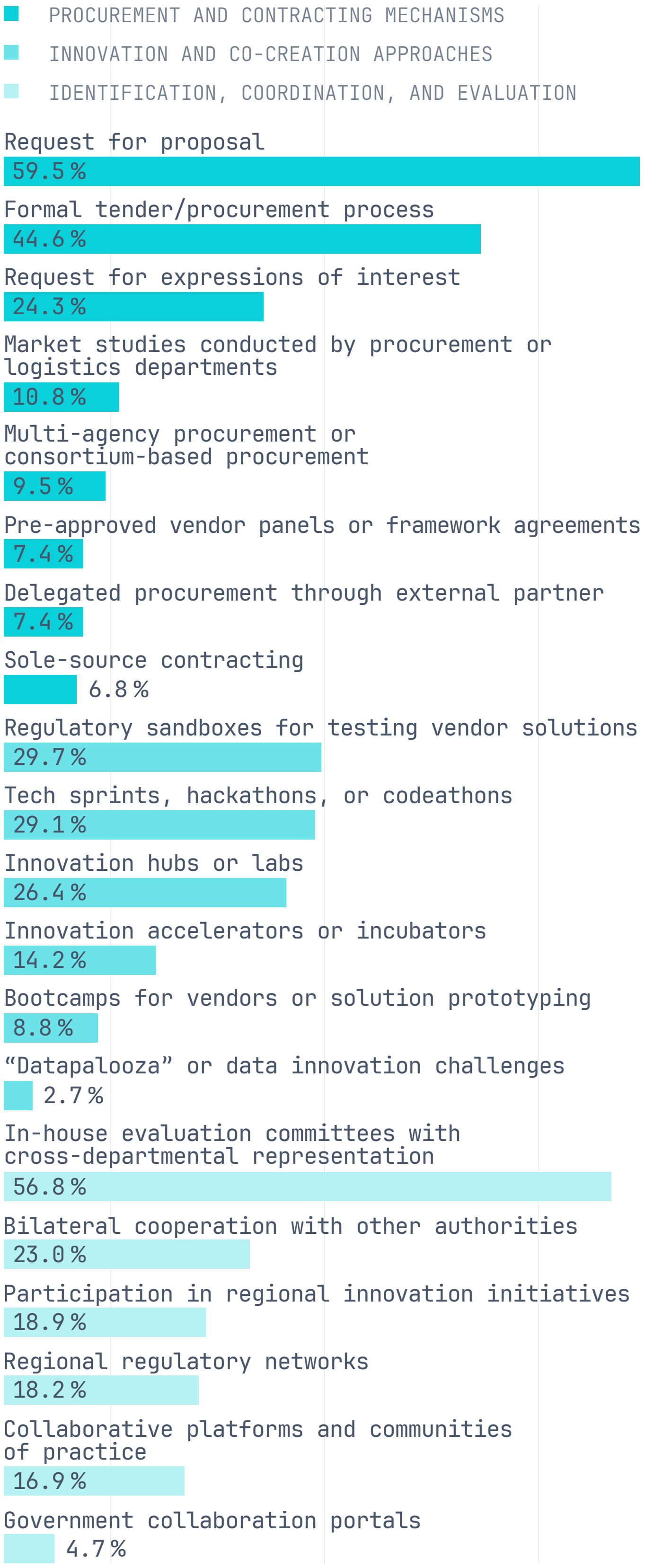


FIGURE 69.

Procurement And Collaboration Models Used By Financial Authorities To Engage SupTech Solution Providers



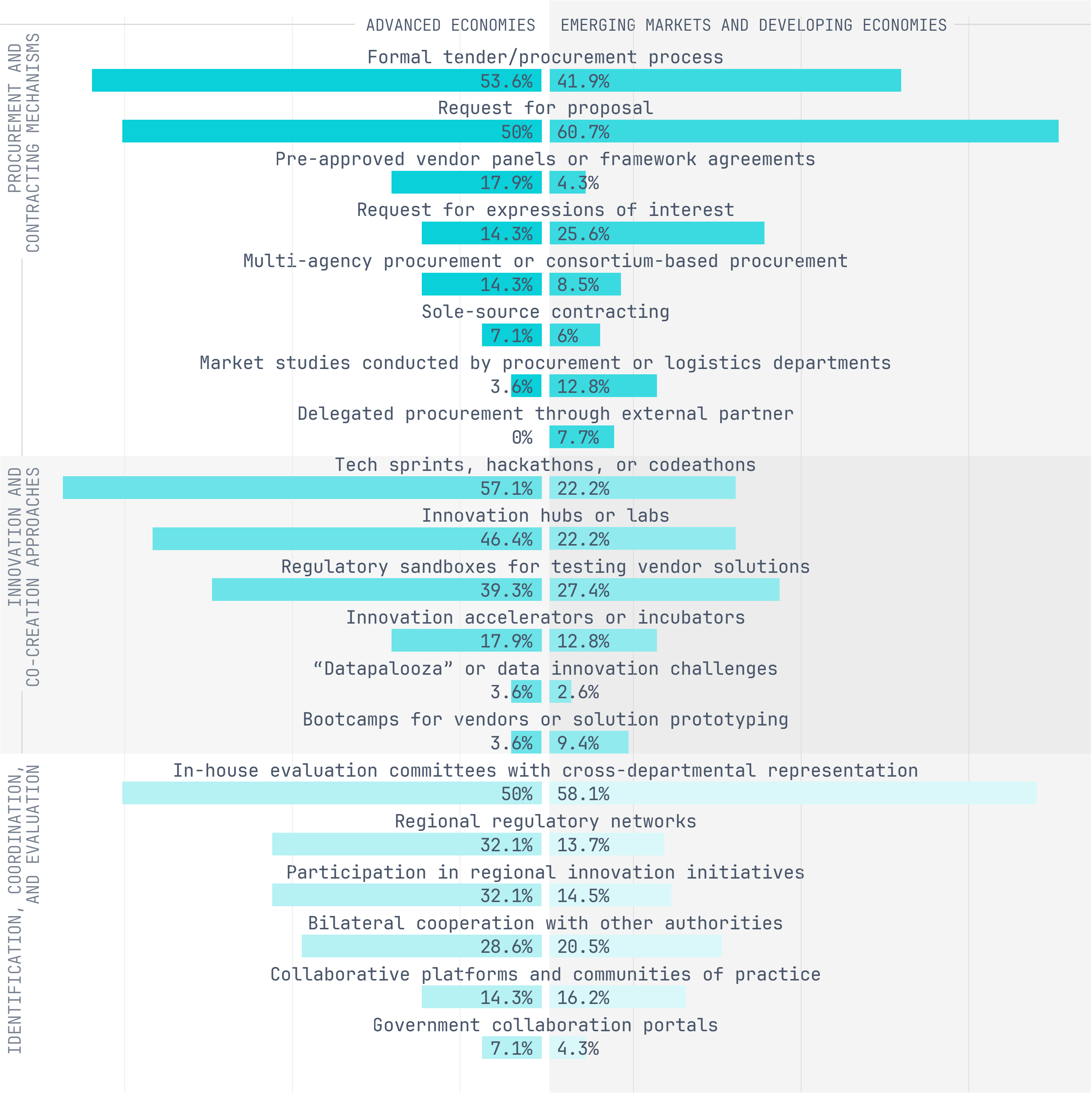
integrating innovation-focused approaches and maintaining strong cross-departmental oversight. The procurement process is overwhelmingly dominated by formal, traditional procedures: nearly six in ten authorities use a request for proposal (RFP) (59.5%), and nearly half rely on a formal tender/procurement process (45%) (Figure 69). Mechanisms designed for flexibility, such as pre-approved vendor panels or sole-source contracts, are rarely used (7% each).

A substantial number of agencies use in-house evaluation committees (57%) with cross-departmental representation, demonstrating strong internal governance over the selection process. While innovation is supported through approaches like regulatory sandboxes (30%) and tech sprints/hackathons (29%), these co-creation methods are still secondary to formal procurement routes. Collaboration with peers is less frequent, with only a minority engaging in bilateral cooperation (23%) or regional initiatives. This pattern is consistent with a strategic preference for formal, competitive vendor selection backed by strong internal scrutiny, rather than highly agile or collaborative co-development models.

Suptech engagement models reveal a notable divergence in procurement and innovation practices between economic groups. AEs combine formal procurement, such as tenders (54%) and RFPs (50%), with strong innovation and co-creation, favouring tech sprints (57%) and innovation hubs/labs (46%), and actively leveraging regional regulatory networks (32%). In contrast, EMDEs rely more on traditional contracting via RFPs (61%) and show lower adoption of innovation methods, including regulatory sandboxes (27%) and tech sprints (22%), with limited use of regional networks (14%), suggesting less integrated and proactive engagement. Both groups, however, maintain robust internal oversight through in-house evaluation committees to guide procurement decisions.

FIGURE 70.

Procurement And Collaboration Models Used By Financial Authorities To Engage SupTech Solution Providers By Economic Classification



3.

Insights and Trends Across Supervisory Areas

Supervisory authorities are integrating data and technology into an expanding range of oversight functions, but adoption remains uneven and closely tied to mandate, data availability, and institutional capacity. Across domains, the 2025 survey reveals a consistent pattern: suptech is progressing fastest where workflows already depend on structured, high-frequency data — such as compliance verification, consumer-feedback processing, and incident reporting — and remains nascent where supervision requires complex behavioural analytics, cross-entity coordination, or visibility into activities outside the traditional regulatory perimeter.

The analysis in this section shows that most authorities continue to prioritise foundational capabilities such as automated data ingestion, validation, and core monitoring. By contrast, more advanced applications — including behavioural risk analysis, algorithmic governance, on-chain forensics, market-abuse detection, open-finance oversight, and systemic-risk modelling — display early but uneven maturity. These patterns underscore persistent constraints in data architectures, governance frameworks, analytical tooling, and specialist skills. They also highlight growing divergence between domains where rich, standardised data are available and those where data are fragmented, proprietary, or technically immature.

Several cross-cutting themes emerge. First, lifecycle maturity remains concentrated in proofs of concept and working prototypes, with fully deployed suptech still the exception in most domains. Second, supervisory effectiveness increasingly depends on the interoperability and quality of underlying data systems — including ISO 20022 adoption in payments, securities, and operational-risk reporting — which directly shape authorities' ability to apply automation and AI responsibly. Third, shifts in financial activity toward digital channels, instant payments, cloud-based infrastructures, AI-enabled decisioning, and digital assets continue to widen the supervisory perimeter, creating demand for new tooling that many authorities have not yet operationalised.

Survey responses from 2025 show different levels of engagement with suptech across supervisory domains. When considering the full spectrum of activity — including deployed applications, working prototypes, POCs, and initiatives that are desired but not yet planned — the most active areas are AML/CFT/CPF supervision (53% of authorities reporting deployed or actively developing solutions), licensing and authorisations (52%) and consumer protection and market conduct supervision (51%) (Figure 71). Prudential supervision also remains significant (48%), though its relative weight has shifted from previous years, as authorities report increasing innovation activity in emerging risk domains.

When focusing on active development and deployment – that is, removing only the "desired but not planned" category while retaining proofs of concept, prototypes, and deployed solutions – the distribution changes (Figure 72). Here, traditional supervisory domains show the deepest pipelines of work. Prudential supervision has the highest combined share of PoCs, prototypes, and deployed tools (58%), followed by capital markets and securities oversight (56%), and licensing and authorisations (45%). AML/CFT/CPF and insurance supervision each account for 44%.

This comparison illustrates that while innovation energy is increasingly directed toward emerging risk areas, the densest pipelines and most

FIGURE 71.

Product Lifecycle Stage Of Suptech Solutions
By Supervisory Domain

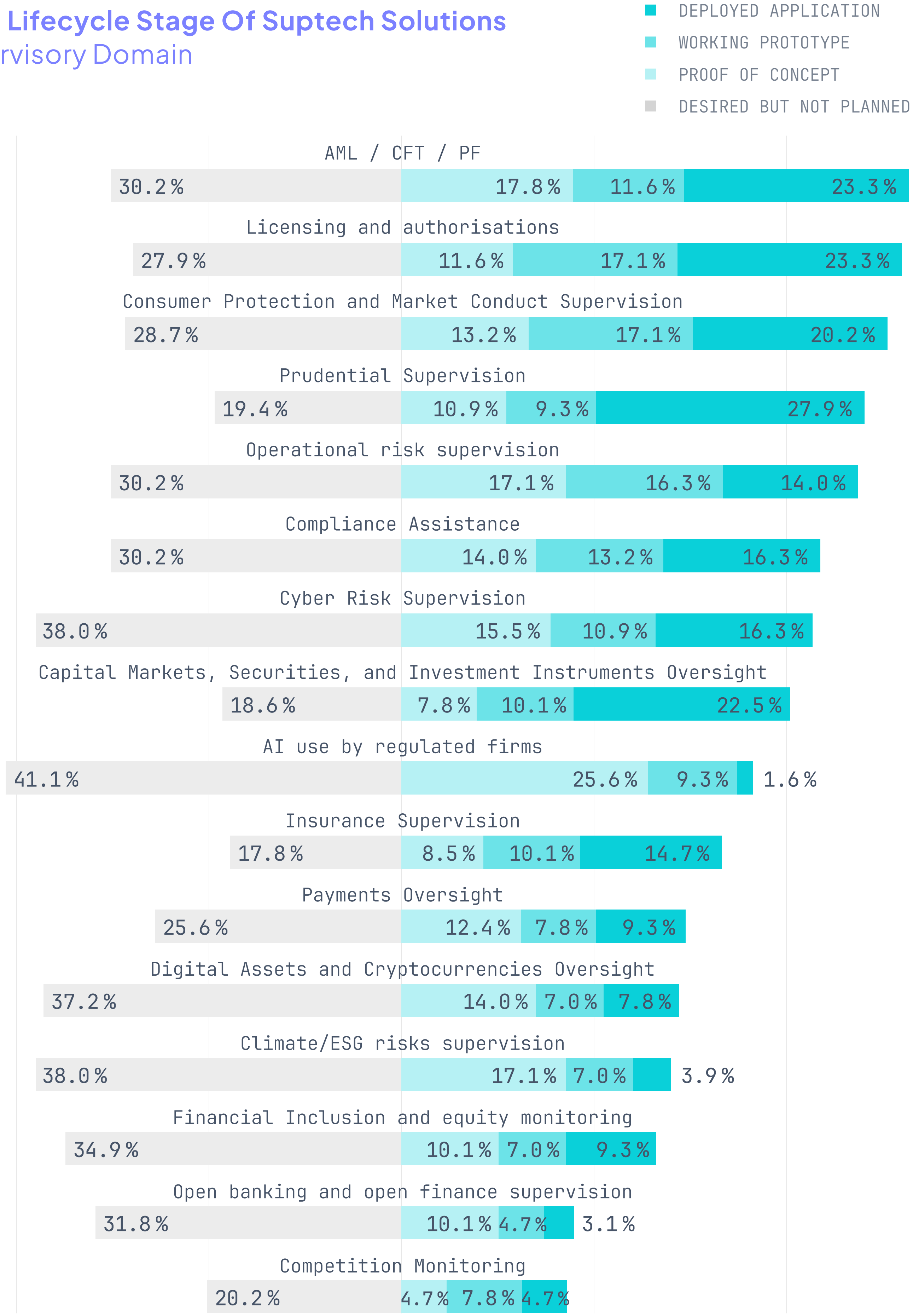
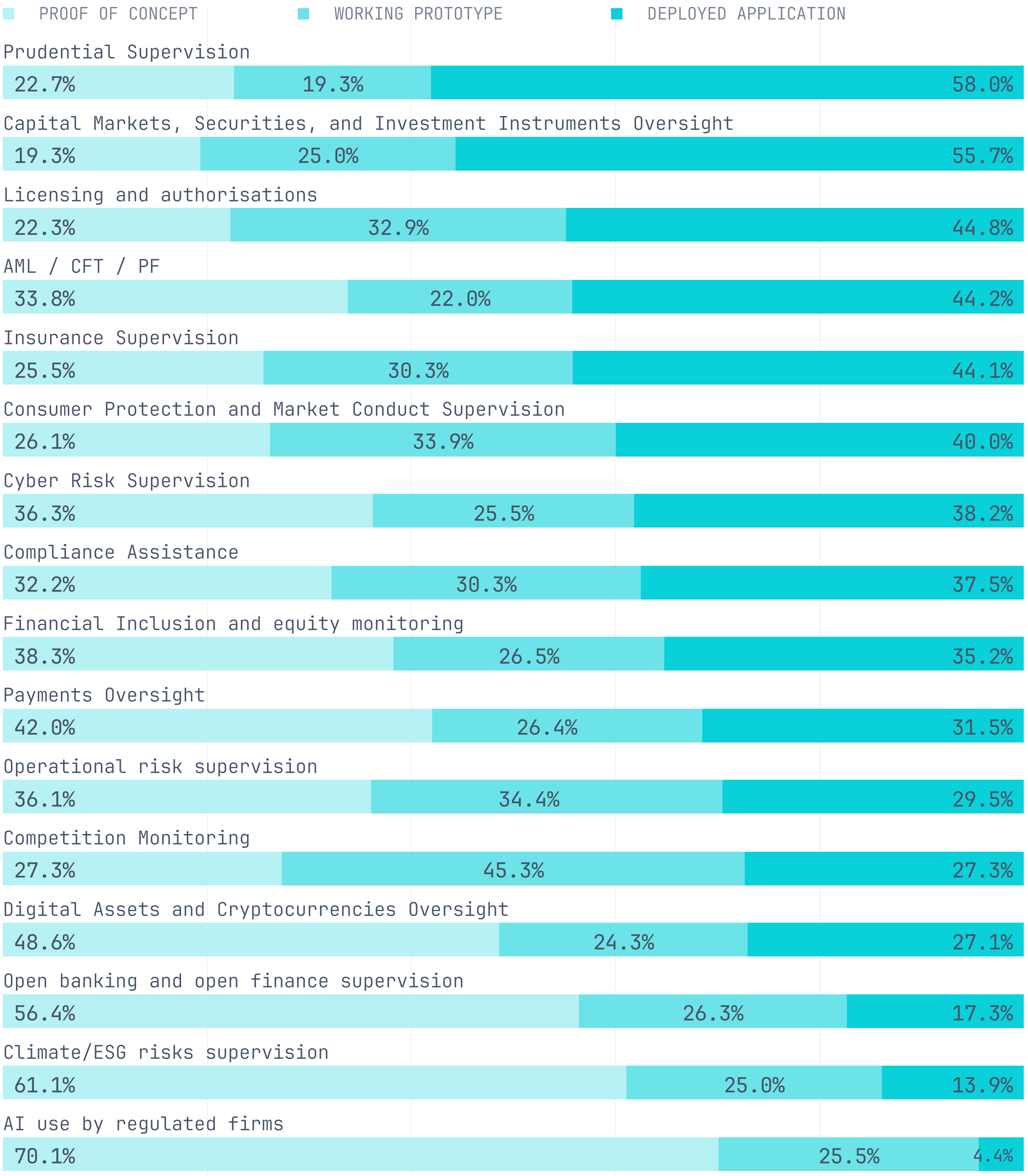


FIGURE 72.

Product Development Pipeline (POCs, Prototypes, And Deployments)

By Supervisory Domain



PERCENTAGES ARE CALCULATED RELATIVE TO THE TOTAL NUMBER OF REPORTED SOLUTIONS WITHIN EACH SUPERVISORY AREA, INDICATING THE INTERNAL DISTRIBUTION OF APPLICATIONS' MATURITY.

established implementation work continue to sit in long-standing supervisory functions. This distribution is consistent with broader trends identified in the report, including growing dependence on structured data architectures, harmonised messaging standards such as ISO 20022, and early foundations of AI-readiness, all of which favour domains with more established reporting frameworks.

The strongest pipeline of POC activity is concentrated in oversight of AI use by regulated firms (70%), climate and environmental risks (61%), open banking and open finance (56%), and digital assets (49%). These areas also show the highest levels of unmet demand ("desired but not planned"), especially in AI use by regulated firms (41%), climate risk (38%), cyber risk (38%), and digital assets (37%). This alignment between interest and experimentation confirms that authorities are beginning to redirect innovation capacity towards emerging systemic risks, even when operationalisation remains constrained by capability, tooling, or data gaps.

The next wave of suptech maturity is also visible in the distribution of working prototypes. Competition monitoring stands out (45%), followed by consumer protection and operational risk supervision (34% each). The prominence of prototypes in competition monitoring is notable given the relatively limited overall uptake in this domain. This may reflect mandate differences – only around one-third of authorities have explicit competition oversight responsibilities – or evolving regulatory frameworks around digital platform conduct. Differences in data availability, interoperability, and supervisory mandate scope continue to shape these maturity patterns, particularly where emerging risk domains require datasets, taxonomies, or entity-coverage rules that are not yet standardised.

A comparison with previous years confirms both consolidation in core areas and rapid diversification into new ones (Figure 73). Licensing and authorisations show the strongest momentum, rising sharply from 19% in 2022 to 52% in 2025. Compliance assistance nearly tripled (14% to 44%). Prudential supervision, while still dominant in terms of deployment, has seen its overall activity decline slightly to 48%. Among frontier risks, climate/ESG supervision increased substantially (16% to 28%), digital asset oversight grew steadily (23% to 29%), and oversight of AI use by regulated firms emerged as a significant new priority at 37%.

These trends suggest a dual trajectory in suptech modernisation:

- Mature domains are solidifying their digital infrastructure and governance as authorities deploy production-grade solutions in established risk areas.
- Emerging domains are experiencing accelerated experimentation as authorities prepare for the supervisory implications of AI, climate, cyber, and decentralised technologies.

Differences across economic classifications reflect divergent supervisory priorities and institutional capacities (Figure 74). Advanced economies focus on complex and systemic risks, with strong pipelines in prudential supervision, AML/CFT/CPF, consumer protection, and climate/ESG risks. Climate risk supervision, in particular, shows the highest POC share in AEs (26%), reflecting alignment with broader sustainability agendas and emerging regulatory mandates.

By contrast, EMDEs prioritise foundational market functions and supervisory efficiency, leading active implementation in licensing and authorisations, compliance assistance, and financial inclusion monitoring. Both groups show limited activity in competition monitoring and open finance supervision, though for different reasons: mandate gaps in EMDEs and early-stage governance frameworks in AEs.

FIGURE 73.

Product Lifecycle Stage Of Suptech Solutions

By Supervisory Domain 2022–2025

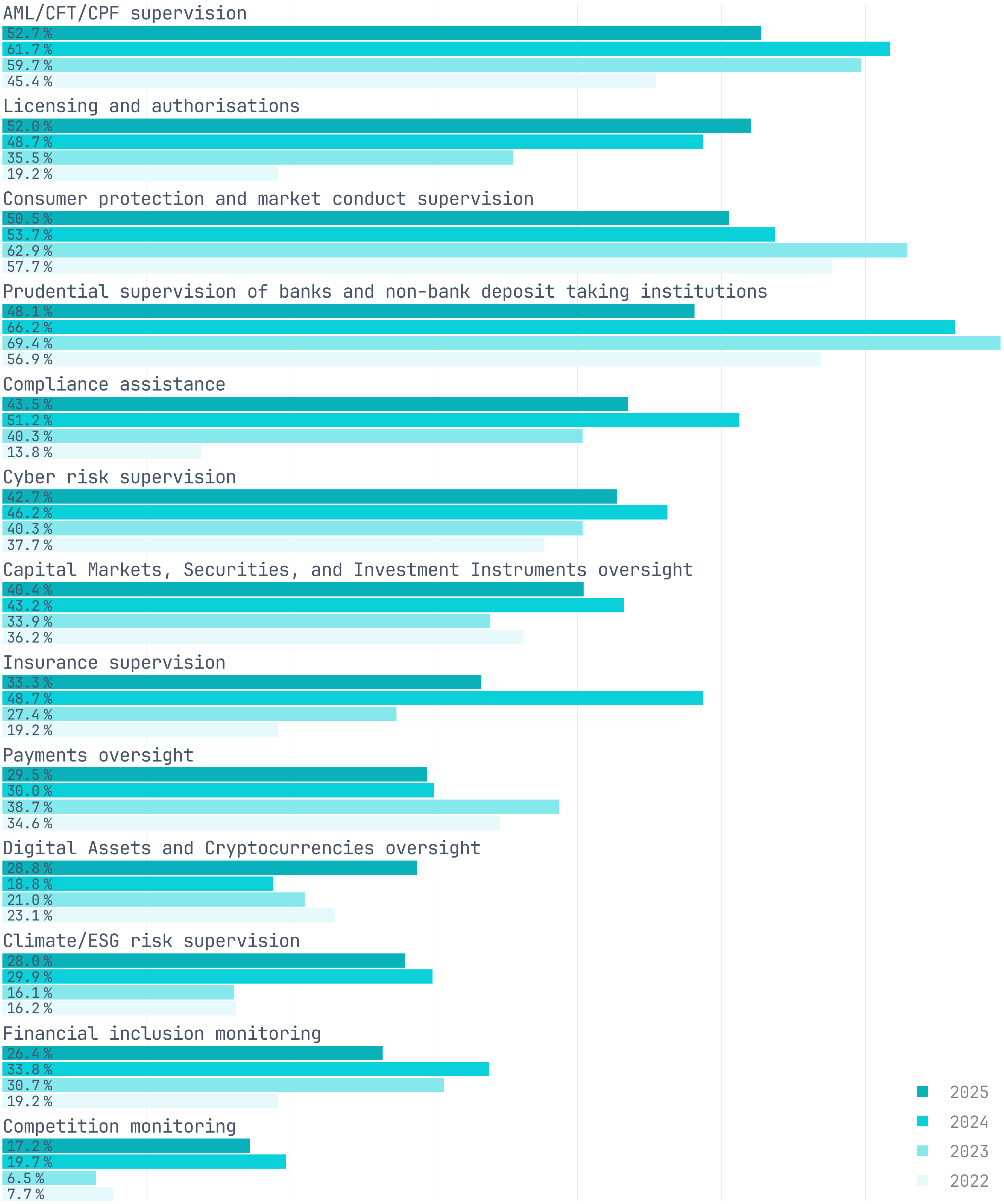
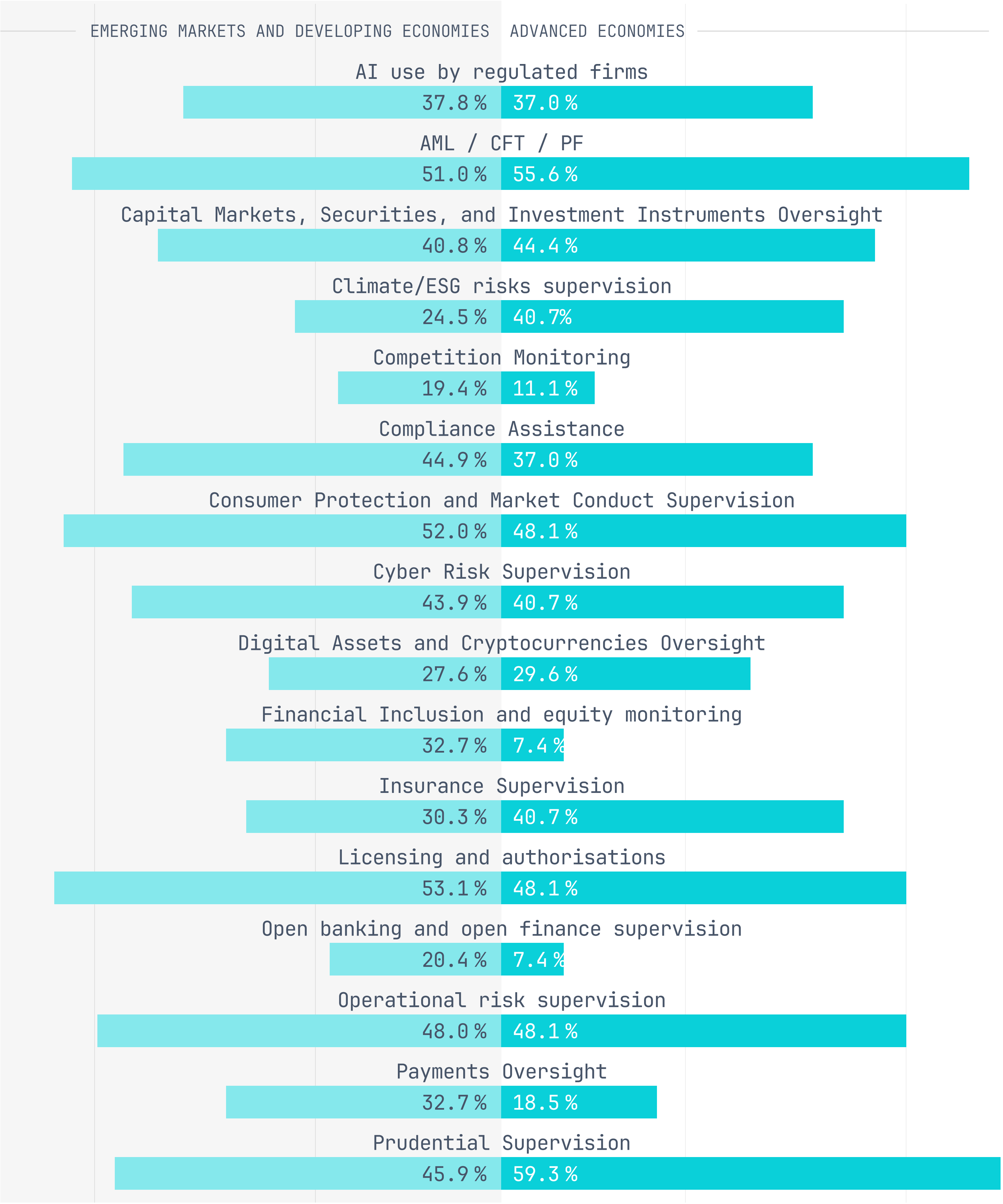


FIGURE 74.

Product Lifecycle Stage Of Suptech Solutions

By Supervisory Domain And Economic Classification



3.1 AML/CFT/CPF supervision

AML/CFT/CPF supervision increasingly depends on high-volume, heterogeneous data — including risk scoring, sanctions matching, behavioural-pattern analysis, and cross-border intelligence exchange — and suptech adoption reflects this operational intensity. In 2025, it remained the most advanced suptech domain, with 53% of authorities deploying or developing applications. Uptake is strongest in rule-based validation and institutional profiling, while more complex capabilities such as network analytics and AI-enabled anomaly detection are still emerging. Policy momentum from FATF's evolving risk-based framework and rising virtual-asset risks reinforces the need for scalable analytical tools, though gaps in data quality, coordination, and cross-border information-sharing continue to limit supervisory effectiveness.

> "To combat Illicit Financial Flows in this digital age effectively, we must evolve our strategies beyond traditional methods. First, we need to shift from a reactive compliance-by-design approach to an intelligence-by-design framework, where advanced analytics and AI-driven insights proactively identify risks before they escalate."
>
> – Muhammad Jiya, Chief Operating Officer (COO), Emerging Technologies and Innovation, Nigerian Financial Intelligence Unit

AML/CFT/CPF supervision increasingly relies on data-intensive workflows — including risk scoring, sanctions matching, transaction-pattern analysis, and cross-border intelligence exchange — and suptech adoption in this domain reflects the need to process high-volume, heterogeneous datasets at scale.Global efforts to strengthen AML/CFT frameworks continued to intensify in 2025, with an emphasis on financial inclusion, digital assets oversight, and enhanced intelligence sharing under the FATF's evolving risk-based agenda. The FATF advanced revisions to Recommendation 1 and issued updated guidance on financial inclusion, promoting simplified due diligence and anti–de-risking measures to expand access to financial services. Complementing these policy shifts, it released a comprehensive National Risk Assessment Toolkit and a Handbook on International Cooperation, providing jurisdictions with practical methodologies to assess risks and improve cross-border collaboration in detecting and prosecuting financial crime.

Supervisory scrutiny over virtual assets also deepened. The FATF's sixth targeted update on virtual assets (VA) and VA service providers revealed uneven compliance, with only one jurisdiction fully compliant with Recommendation 15 related to managing risks related to new technologies, despite most countries having conducted sectoral risk assessments. Gaps in licensing, enforcement, and implementation of the Travel Rule persist, leaving key information-sharing blind spots as criminals increasingly exploit DeFi platforms, stablecoins, and offshore intermediaries. The rising misuse of virtual assets for scams and cyber-enabled laundering further highlights the need for jurisdictions to operationalise these standards and strengthen supervisory technology.

Echoing these concerns, EBA warned of persistent AML/CFT risks in the crypto-asset sector due to governance and KYC weaknesses. They highlighted that crypto-asset firms have exploited regulatory gaps through unauthorised operations and forum shopping, underscoring how the EU's Markets in Crypto-Assets Regulation (MiCA) and updated AML/CFT framework seek to mitigate these risks through harmonised authorisation, enhanced transparency, and stronger governance. With its supervisory powers taking effect on 1 July 2025, Europe's new Anti-Money Laundering Authority (AMLA) also expects crypto-asset service providers to uphold robust standards and controls against ML/TF, given the sector's high cross-border and anonymity-related risks. Panellists at the Central Banking Spring Meetings 2025 further discussed AML/CFT risks arising from virtual assets.

> **"There is no longer a distinction between AML and fraud efforts... Data silos must fall to combat converging financial crime types"**
>
> – Roundtable discussion conclusions held on the sidelines of Regulation Asia's Fraud & Financial Crime conference

Collaboration among authorities remains limited, leading to duplication, data silos and weak information exchange that undermine global efforts to combat financial crime. Only a small proportion of criminal assets are recovered, with more than 80% of jurisdictions rated low or moderate for asset recovery effectiveness in a FATF assessment. However, success stories such as Hong Kong's cross-border operation, which used the Frontier+ collaboration platform and resulted in 1,800 arrests and the seizure of around USD 20 million, demonstrate the impact of cooperation. Emerging harmonised AML/CFT frameworks and technologies such as the next generation of FIU.net are expected to deliver more interoperable and scalable solutions, strengthening collaboration and improving asset recovery.

Financial intelligence units and supervisors are integrating technology to address gaps. In the United States, the Treasury sought views on the use of APIs, AI, and blockchain to detect illicit finance, while DARPA continued to champion for anticipatory and adaptive anti-money laundering via its A3ML program. The EBA's 2024 survey of its 31 competent authorities found that the adoption of AML/CFT suptech has accelerated across the EU over the past three years, with 60 projects underway and nearly half (47%) already implemented, notably supporting risk scoring, ad hoc reporting, and the assessment of AML/CFT policies and procedures. ECB's Supervision Innovators Conference 2025 highlighted how suptech can improve detection beyond conventional suspicious transaction report processes.

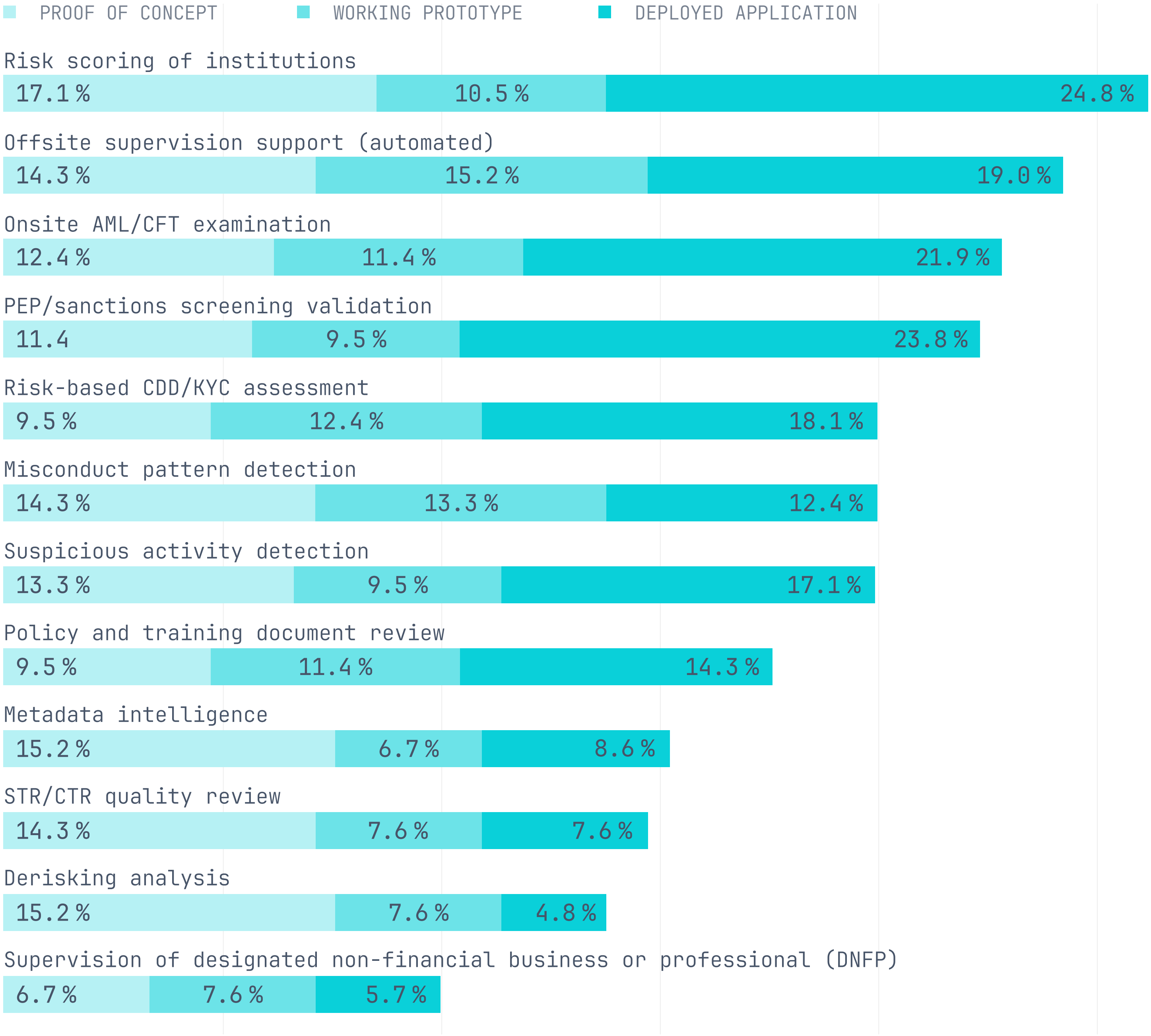
In the Asia-Pacific region, Australian Transaction Reports and Analysis Centre (AUSTRAC) is championing an intelligence-led approach. It leverages the Fintel Alliance Collaborative Analytics Hub to aggregate large datasets securely from major banks, using advanced models to identify concealed financial crime patterns for rapid law enforcement referral. AUSTRAC is committed to expanding its responsible use of AI and has published an AI Transparency Statement to ensure governance and human-in-the-loop oversight, aligning with Australian Government digital guidelines.

Private-sector and regional standards reinforce this technology-driven shift. The Wolfsberg Group published new statements on risk-based monitoring and proportionality in suspicious activity detection, supporting the move from rules-based systems to explainable machine-learning models. The New York Department of Financial Services urged banks to embed blockchain analytics into compliance systems, for wallet screening, crypto monitoring and source-of-funds verification. Central Bank of Ireland's inaugural Innovation Sandbox Programme aimed at combatting financial crime by fostering innovative technology that reduces fraud, strengthens KYC/AML/CFT frameworks, and improves transaction security.

In 2025, financial authorities are increasingly adopting data analytics and automation to strengthen their supervision in this domain. Survey data confirm that AML/CFT/CPF is a leading domain for suptech deployment, with 53% of authorities engaged. Of these, 23% report fully deployed applications, 12% are testing prototypes, and 18% are developing POCs (Figure 71). The most widely deployed tools are those that enhance efficiency and risk assessment: risk scoring of institutions (25%) is used for efficient profiling, while automated offsite supervision (19%) and tools for onsite AML/CFT examinations (22%) streamline both remote monitoring and in-depth physical inspections (Figure 75).

FIGURE 75.

Prioritization of SupTech Use Cases Under AML/CFT/CPF Supervision



A key focus remains on compliance with international standards through PEP/sanctions screening validation (24%) and risk-based CDD/KYC assessments (18%). Authorities are also investing in sophisticated analysis, such as misconduct pattern detection (12%), which aids in identifying suspicious activities within vast transaction datasets. While tools like metadata intelligence (9%), STR/CTR quality review (8%), derisking analysis (5%) and supervision of designated non-financial businesses and professions are in early deployment stages, they show strong potential for detecting hidden risks and enabling more granular supervision. Authorities are actively exploring experimental solutions in these domains to push the boundaries of automation and AI-driven analysis against increasingly complex financial crime risks.

The rapid evolution of AI-driven detection tools is evident in projects such as AMLNet, a knowledge-based multi-agent framework for detecting realistic money laundering activity, illustrate the growing sophistication of AI-driven detection tools being explored by supervisors and researchers alike. The Alan Turing Institute, in collaboration with the FCA, Plenitude Consulting, and Napier AI, is also developing privacy-preserving synthetic datasets using cutting edge technology including generative adversarial networks to support AML system testing and innovation. The French supervisor ACPR uses the AI-based LUCIA tool during on-site AML/CFT inspections to analyse large volumes of banking transactions, assessing the performance of banks' AML/CFT models and further advancing the use of AI in financial supervision.

At the same time, initiatives like Project Hertha, a joint project between the BIS Innovation Hub London and the Bank of England, demonstrate the growing importance of collaborative, network-level risk assessments. By using synthetic transaction data, the project shows that payment system analytics can uncover money-laundering patterns that individual banks may miss, particularly when risk scores are shared across institutions. The BIS Innovation Hub further galvanised this development by conducting an analytics challenge among innovators to develop tech solutions using AI, privacy tech, or collaborative design to tackle illicit finance, enable secure data sharing, and support compliance with nuanced regulatory measures. These developments signal a future where supervisory authorities are increasingly equipped to manage emerging risks in a more connected, data-driven, and technologically advanced environment.

Overall, 2025 marks a further transition from incremental digitisation to strategic integration of suptech within AML/CFT/CPF supervision. Authorities are moving beyond compliance monitoring towards adaptive, analytics-driven oversight capable of addressing complex and fast-evolving financial crime risks. Although challenges persist around data quality, capacity, and coordination, the growing maturity of prototypes and POC tools signals an imminent phase of operational deployment. Effective implementation will depend on continued international collaboration and supervisory frameworks that balance innovation with accountability, cementing suptech's role as a cornerstone of modern, risk-based financial crime and integrity supervision.

3.2 Artificial Intelligence (AI) use by regulated firms — supervisory oversight

Supervisory oversight of AI use by regulated firms increasingly centres on model-risk management, data governance, and the evaluation of opaque, adaptive systems. Policy activity expanded in 2025, but operational suptech adoption remains limited: only 2% of authorities report deployed tools, with most work in POC or prototype stages. Authorities prioritise explainability assessment, model validation, and monitoring of AI-driven consumer outcomes, yet capacity constraints and fragmented data continue to limit implementation. Overall, this is a high-priority but early-stage domain where supervisory readiness is still developing.

Global AI adoption is accelerating, offering financial institutions efficiency and value across their operations. However, it brings risks to consumers and financial stability, particularly around data management, model design, and deployment. Concentrated AI use can amplify operational risks, market concentration, and systemic vulnerabilities, while potentially increasing herding behaviour and correlations. Where existing regulation falls short, targeted policy measures may be required to ensure resilience and fairness. In 2025, policy and supervisory attention on AI remained high, focusing on promoting responsible innovation, building capacity, and defining clear oversight expectations.

Authorities globally are accelerating responsible innovation through dedicated testing environments. The UK's Financial Conduct Authority (FCA) is actively working on its AI Lab, which includes a new Supercharged Sandbox offering access to accelerated computing and the AI Live Testing programme, welcomed by firms for assessing models under real-world conditions. Similarly, the Hong Kong Insurance Authority (IA) launched an AI Cohort Programme to establish a regional AI Centre of Excellence for talent development and knowledge sharing. The National Bank of Georgia also launched an AI Sandbox pilot project within its Regulatory Laboratory, providing a trusted, controlled environment for firms to test AI-driven financial innovations. In the US, a bipartisan bill was introduced to mandate AI Innovation Labs in federal financial agencies, operating as supervised sandboxes for time-limited test projects. Building on its initial efforts, the Hong Kong Monetary Authority (HKMA) announced the second cohort of its Generative AI Sandbox, in collaboration with Cyberport, shifting industry focus from AI capability experimentation to secure and reliable implementation.

Standard-setting and policy frameworks have also advanced in parallel. The IAIS and EIOPA issued guidance applying existing Insurance Core Principles to AI systems, setting out a risk-based supervisory approach covering governance, security, transparency, and fairness. The International Organization of Securities Commissions (IOSCO) also sought feedback on AI impact in the capital markets. Global policy frameworks also advanced, notably with Indonesia's OJK releasing a comprehensive, risk-based AI Governance framework for banking, which sets minimum reference standards for reliability, explainability, and ethics. The Securities and Exchange Board of India (SEBI) also proposed principles for responsible AI use in securities markets, focusing on model governance, investor protection, robust testing, and fairness. The EU AI Act, fully adopted in mid-2024, began phased implementation throughout 2025, with specific rules on general-purpose AI (GPAI) models and public governance becoming applicable in August 2025.

Authorities also leveraged focused events and collaborative sprints to inform policy and build capacity. Following the FCA's AI Sprint, which convened diverse stakeholders to shape its regulatory approach, practical industry focus shifted to evaluation. Events like the FINOS AI Evaluation Benchmarking workshop and subsequent techsprint in September 2025, also drove co-ordinated efforts on setting standards for assessing AI models. The European University Institute's EU Sustainable Digital Finance Alliance (EU SDFA) programme also further contributed through an advanced workshop aimed at enhancing supervisory capacity in AI oversight. High-level forums such as the UNESCO Priority Africa Artificial Intelligence Action Summit, complemented these technical activities, demonstrating a global commitment to translating broad AI principles into actionable governance.

Despite the intense regulatory focus on AI governance, suptech adoption for overseeing firms' AI use is at an early stage compared to traditional supervision areas (Figure 71). Nevertheless, financial authorities exhibit cautious optimism about its potential. A significant majority of respondents believe suptech will be effective in mitigating new supervisory risks: 37% view it as *very effective*, addressing most challenges, while 28% see it as *moderately effective*, addressing many challenges (Figure 76). Combined, 65% of authorities perceive suptech as a strong solution. 10% believe it will be *somewhat effective*, addressing only a few challenges. Only 2% consider it *ineffective*, while 23% are unsure.

Currently, 37% of authorities report AI oversight tools in the POC (26%) or working prototype (9%) phase, with only 2% currently deployed (Figure 71). The most active development areas for these tools are model validation and explainability (21% in deployment/testing), consumer outcome monitoring (17%), governance and accountability of AI systems (17%), and bias and discrimination detection (16%) reflecting the priority given to assessing model reliability and consumer fairness (Figure 77). Beyond these core areas, most other use cases remain mostly at the proof-of-concept stage, including initiatives on audit trail and traceability validation (13%), monitoring AI use in high-risk or opaque areas (13%), third-party AI model and data provider oversight (10%). These trends confirm that

FIGURE 76.

Perceived Impact of SupTech on Supervisory Challenges Created by AI Adoption

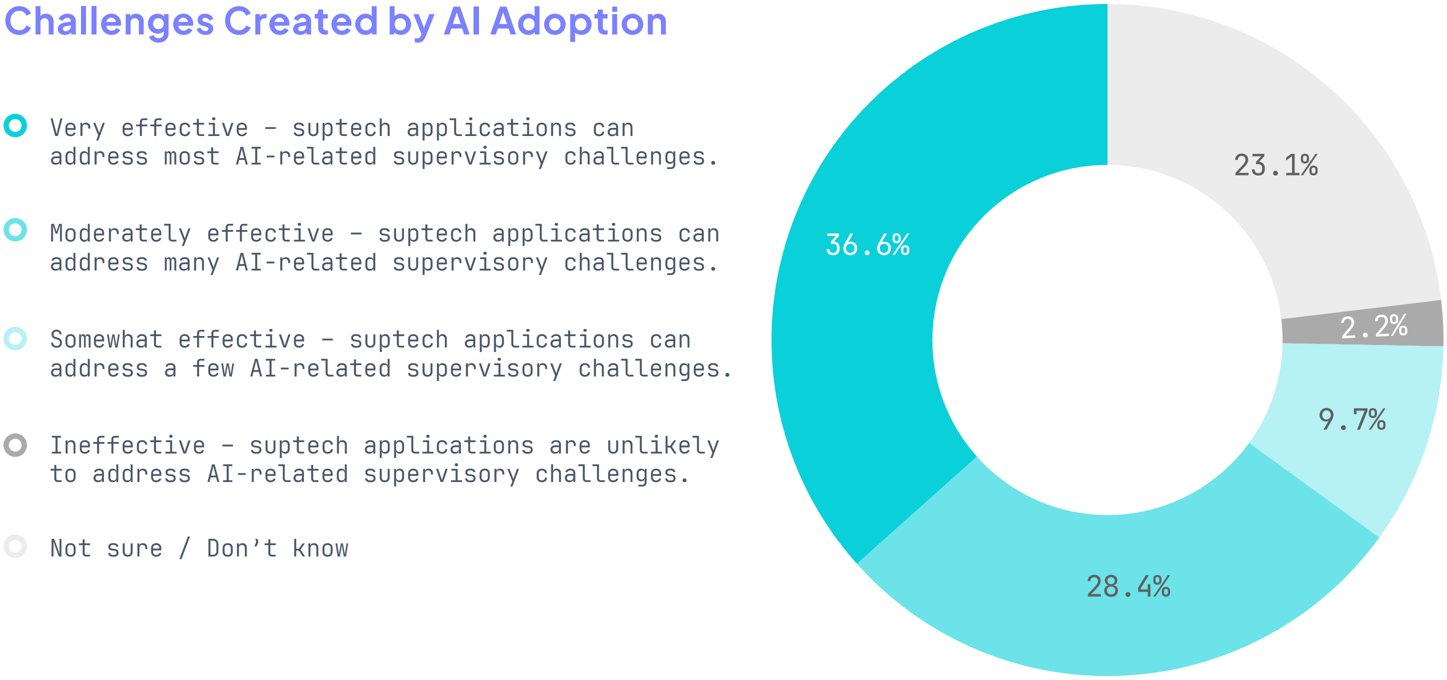
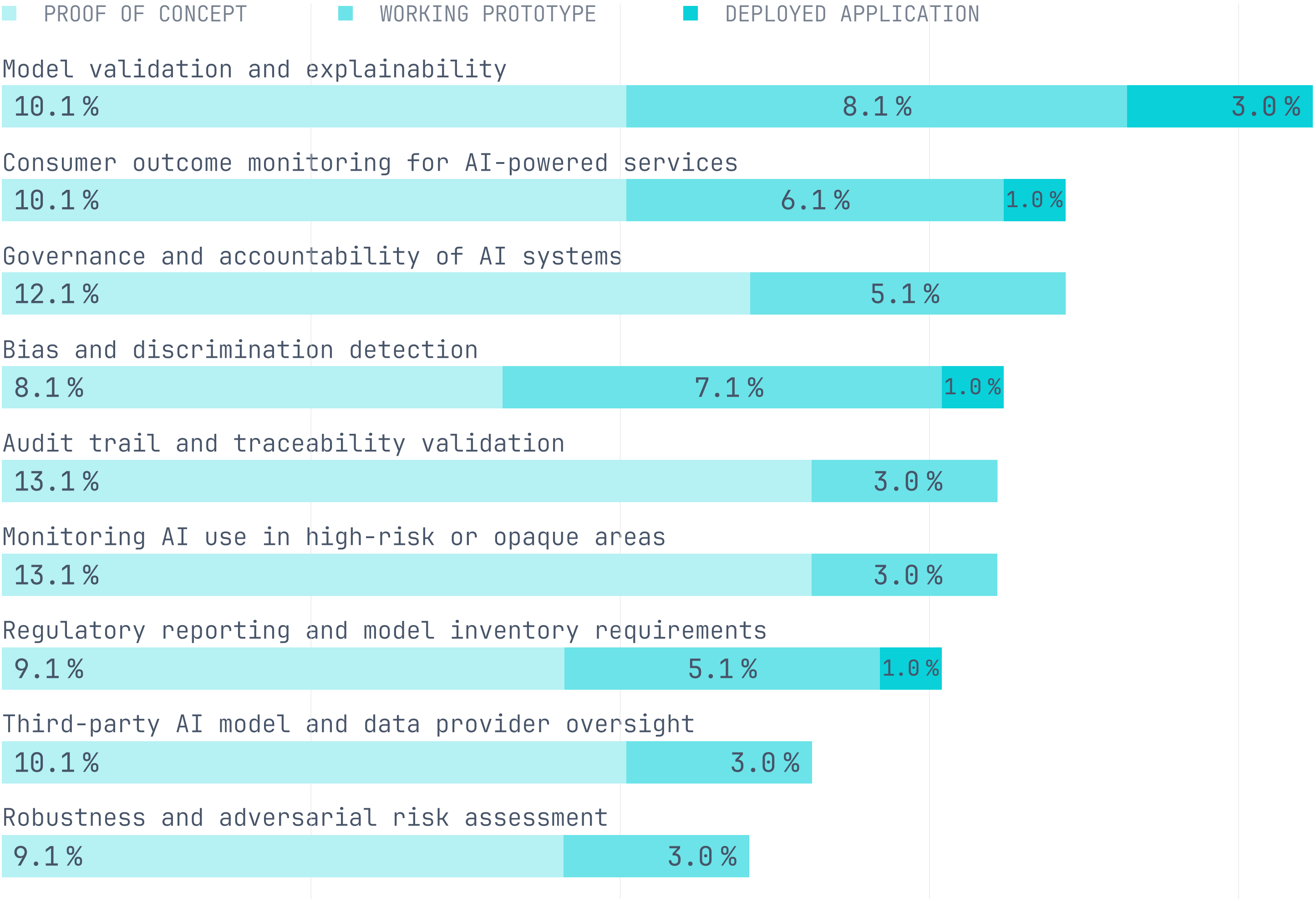


FIGURE 77.

Priority SupTech Use Cases For Oversight of AI Use By Regulated Firms



supervisors are still building the technological capacity necessary to independently scrutinise and validate complex AI models, highlighting the importance of tools such as Explainable AI (XAI) for effective oversight.

Explainability remains a central challenge, as authorities grapple with the difficulty of scrutinising advanced, opaque AI models. Researchers from leading AI labs, including OpenAI, Google DeepMind, Meta, and Anthropic, have highlighted increasing challenges in understanding the reasoning process of advanced AI models, emphasising the need to preserve transparent reasoning processes. The BIS Financial Stability Institute has noted the tension between high model performance and low explainability, particularly where current model risk management frameworks struggle to assess high-impact applications. Recommendations include tailoring explainability standards by use case, preferring inherently interpretable models where possible, and using safeguards such as human oversight and circuit breakers where complex models are adopted. To support supervisors, the BIS Innovation Hub Hong Kong Centre launched Project Noor in partnership with Hong Kong Monetary Authority (HKMA) and FCA, to equip authorities with XAI tools for independent model evaluation.

Data collection on AI adoption presents further challenges, as documented in the FSB 2025 AI report. While most financial authorities are collecting data, via industry surveys, outreach, and publicly available data, monitoring remains in an early stage, constrained by fragmented indicator sources, inconsistent definitions, resource/skills constraints, and difficulties in assessing the criticality of AI services. To improve monitoring, key considerations identified include mapping indicators to specific vulnerabilities, minimising collection burdens, improving data representativeness and timeliness, and fostering collaboration across functional authorities and borders. Authorities plan enhancements to address gaps in monitoring critical areas such as third-party dependencies, market correlations, and cyber risks.

Overall, 2025 marked a significant period of "innovation with oversight," with AI sandboxes and governance frameworks proliferating across jurisdictions. While policy intent is clear and authorities are cautiously optimistic about suptech, low deployment levels indicate that supervisors are still developing the technological and analytical capacity needed to independently scrutinise complex AI models. Building this capacity, including through tools such as XAI, will be critical to achieving effective, technology-enabled oversight and ensuring that the benefits of AI in financial services do not come at the expense of stability, fairness, or consumer protection.

3.3 Capital markets, securities, and investment instruments oversight

Capital-markets oversight increasingly relies on high-frequency trading data, structured disclosure pipelines, and automated market-abuse detection, and suptech adoption reflects this shift toward data- and analytics-intensive supervision. In 2025, 23% of authorities reported deployed applications and 18% were testing POCs or working prototypes. Adoption is most mature in enforcement-aligned areas — market-manipulation detection, insider-trading surveillance, and risk-based review triage — while more complex domains such as HFT analysis, derivatives oversight, and cross-market surveillance remain early stage. Migration toward ISO 20022-aligned reporting taxonomies and cloud-based regulatory-reporting platforms is strengthening data foundations, but supervisory capacity continues to lag the speed and fragmentation of modern markets, underscoring the need for interoperable datasets and more advanced analytical workflows.

Capital-markets oversight now depends on high-frequency, multi-venue trading data, issuer-disclosure pipelines, and complex market-abuse detection architectures, and suptech adoption in this domain reflects the growing need for automated surveillance, anomaly detection, and risk-based prioritisation.

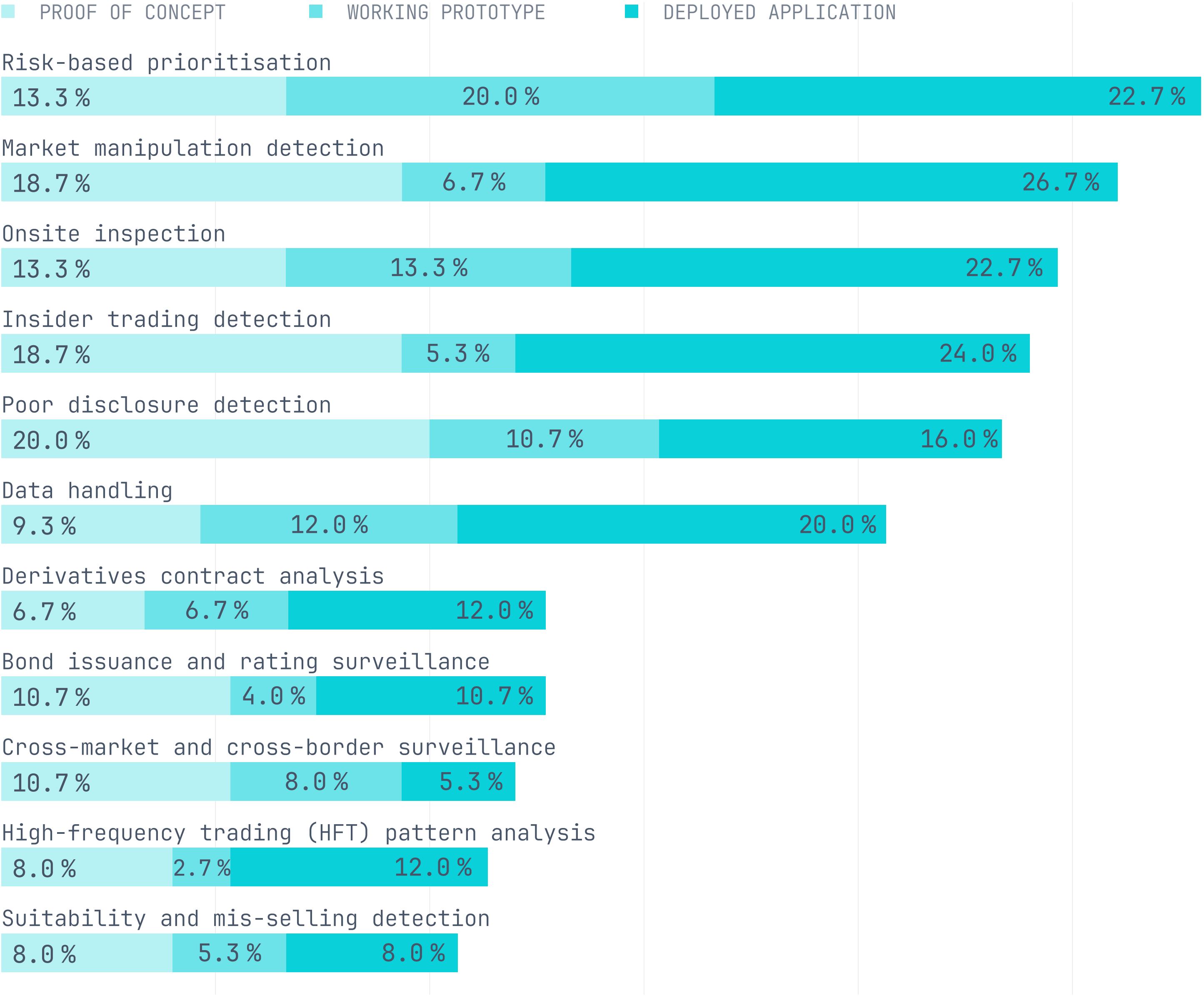
Capital markets supervision continues to emerge as a key area for suptech adoption. Across IOSCO regions, suptech is being integrated into core supervisory functions, driven by the need for efficiency and timely oversight. Advancements in AI, enhanced data access, and cloud-based solutions are enabling this shift. Authorities are deploying data-driven and AI-enhanced tools to prioritise reviews, detect market manipulation, monitor disclosures, manage regulatory data, and support inspections.

In 2025, 23% of authorities reported fully deployed applications, while many others were testing working prototypes (10%) or POC (8%) solutions, indicating strong experimentation and accelerating innovation (Figure 71). The emphasis remains on improving market integrity, transparency, and operational efficiency in an evolving trading environment.

The highest deployment rates for suptech in this domain are concentrated in core risk and enforcement activities: Market manipulation detection (27%), insider trading detection (24%), risk-based prioritisation (23%), and onsite inspections (23%) (Figure 78). These rates reflect the sector's priority on timely identification of misconduct and efficient resource allocation. Examples include Hong Kong's Securities and Futures Commission (SFC) AI-driven market scanning detection model, which evaluates governance indicators, financial disclosures, and market trends, proactively engaging company boards to address concerns before escalation. Similarly, Indonesia's Financial Services Authority (OJK) rolled out the OSIDA PMDK data analytics app to modernise its capital market oversight using big data, initially focusing on investor profiles and market segmentation before expanding to detect manipulation and integrate machine learning for enhanced investor protection in the future.

FIGURE 78.

Prioritisation of SupTech Use Cases Under Capital Markets, Securities, And Investment Instruments Oversight



Data handling, which was the leading use case in 2024 relative to other domains with 35% of fully deployed applications, declined to 20% in 2025 as focus continues to shift towards AI-driven surveillance and risk-based prioritisation. While authorities are moving from data infrastructure upgrades to advanced analytics, data handling remains central to suptech adoption. In 2025, Indonesia's OJK launched the Integrated Financial Services Sector Data and Metadata portal to centralise financial data and enhance transparency, accessibility, and data-driven supervision. In parallel, securities regulators adopting ISO 20022–aligned data dictionaries and harmonised reporting taxonomies are improving the interoperability of transaction, issuer, and post-trade datasets, enabling more automated analytics and reducing validation burdens.

Specialised areas remain heavily concentrated in the early development phase, including derivatives contract analysis (12%), high-frequency trading (HFT) pattern analysis (12%), and bond issuance and rating surveillance (11%). Nonetheless, development is actively progressing, as seen with the Cambodian Securities Regulator (SERC) testing suptech for its derivatives supervision system and India's SEBI launching "Bond Central", a centralised corporate bond database. Advanced surveillance techniques, such as Deutsche Börse's recent adoption of social media intelligence for derivatives monitoring, further support these analytical efforts.

Cross-market surveillance remains the least deployed suptech use case in 2025, with just 5% of authorities reporting fully operational applications, though about 19% are testing prototypes or POCs. Regulators are using AI and advanced analytics to integrate data across trading venues, targeting manipulation, arbitrage, and insider trading. Examples include South Korea's FSS building an unfair transaction system for its first alternative trading platform dubbed NextTrade, and the US Commodity Futures Trading Commission (CFTC) is leveraging Nasdaq's surveillance technology to deliver cross-market monitoring, analytics, and fraud detection across traditional and digital asset classes. These efforts aim to provide a comprehensive view of trading activity and improve detection of complex cross-market risks.

Cross-border collaboration, capacity building and knowledge sharing remain central to advancing suptech in capital markets. In 2025, regulators stepped up training and best-practice exchanges, with the U.S. SEC creating an AI task force to explore collaboratively opportunities and risks, support staff in using AI tools, and promote innovation, and efficiency. IOSCO planned to expand its NEXTGEN capacity building programme to over 40 initiatives and launched the I-SCAN investor alerts portal to protect retail investors. Toronto Centre hosted a risk-based supervision programme for Asia-Pacific securities regulators, the MAS (Singapore) and SSC (Vietnam) enhanced collaboration on capital markets regulation, three Korean authorities introduced joint measures to stamp out stock price manipulation, and the Pakistan Stock Exchange (PSX) and SECP signed a memorandum granting the SECP direct access to PSX's new surveillance system. These initiatives help embed suptech tools within existing frameworks to enable predictive supervision, improve data interoperability and strengthen enforcement.

Beyond collaboration, 2025 also saw active developments across capital markets regulation. Regulators embraced digital assets and innovation, with IOSCO publishing guidance on tokenisation and national authorities adopting new frameworks. The Securities Commission Malaysia sought public feedback on tokenisation and introduced a regulatory sandbox. Thailand issued a tokenised bond, Cambodia unveiled a ten-year plan to develop its securities sector, and the Korea Securities Depository completed a testbed platform to prepare for security token legislation. In India, SEBI issued rules requiring exchanges to monitor and supervise stock broker system audits using technology. These initiatives reflect a broader shift to digital tools for greater market transparency, investor protection and long-term sector growth.

3.4 Climate/ESG risks supervision

In 2025, climate and ESG supervision continued to evolve in line with major international policy developments, yet the digital tools needed to monitor these risks remained limited. Climate/ESG suptech adoption was among the lowest across supervisory domains, with only 4% of authorities reporting deployed applications and most activity concentrated in exploratory stages. Despite high interest – particularly in exposure analysis, disclosure supervision, and ESG portfolio alignment – advanced use cases such as greenwashing detection and climate-risk transmission mapping showed minimal implementation. This gap indicates that supervisory capabilities are still catching up with the rapidly expanding global policy agenda.

In 2025, the policy landscape for climate and ESG risks advanced significantly. International bodies refined disclosure regimes, strengthened transition-planning expectations, and issued updated guidance to support supervisory approaches. Examples include the FSB updated roadmap and climate transition planning – underlining that supervisors require scalable analytical capabilities for transition-risk modelling and forward-looking assessments - , the International Association of Insurance Supervisors (IAIS) guidance on climate-related insurance risks, new Network for Greening the Financial System (NGFS) notes and guides on climate scenario tools and transition planning, and the UNDP's Nature-Insure initiative to build supervisory capacity on biodiversity-related risks. The IFRS Foundation released a road-mapping tool to assist the adoption of sustainability standards for capital markets, and the South Africa's G20 presidency promoted scaled up of sustainable finance initiatives, while CGAP examined the distributional implications of climate-related regulation for low-income households and MSMEs in EMDEs.

Regionally and local actors also increased their activity. The European Supervisory Authorities (ESAs) initiated consultation on draft guidelines for ESG stress testing, and regulators in Canada, Malaysia, Hong Kong and Austria advanced frameworks for sustainability reporting and risk management. In contrast, the United States saw a shift away from coordinated climate efforts, including withdrawal from several international initiatives and the repeal of previously issued interagency principles for climate-related financial risk management.

Alongside policy developments, several innovations emerged to strengthen climate-risk data and supervisory methods. The BIS Innovation Hub and HKMA progressed Project Symbiosis to address climate and nature-risk information gaps through AI-enabled supply-chain analytics, and subsequently launched project Danu, exploring the use of digital twin technologies to model physical risks and their financial-stability implications. Singapore's Gprnt platform introduced automated sustainability reporting tools, while CONSOB and the University of Trento developed an LLM-assisted prototype for detecting potentially misleading claims in green bond disclosures. Malaysia's Bursa Centralised Sustainability Intelligence platform advanced digital reporting for IFRS S1 and S2 compliance, and analytical sandboxes such as Ecomonitor supported policymakers in testing climate interventions through interactive simulation (see the case study below).

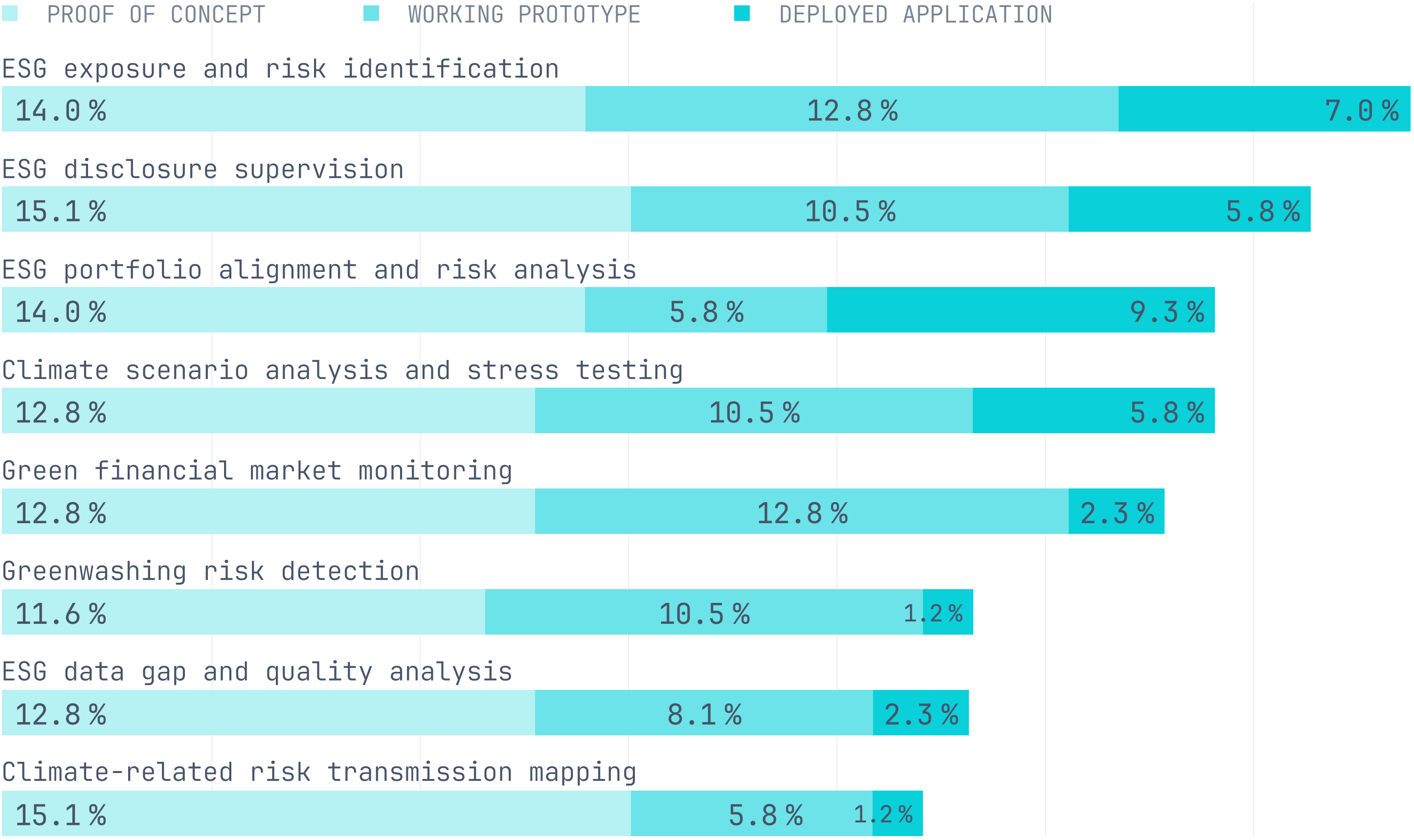
Despite this momentum, suptech adoption in climate/ESG supervision remains at an early stage. Survey data show that only 4% of authorities have deployed applications in this domain – one of the lowest shares across all supervisory functions (Figure 71). A further 38% report interest in developing solutions but remain in planning phases, signalling recognition of the need for digital capabilities but limited operationalisation to date. Most tools are still at proof-of-concept (17%) or prototype stage (7%), underscoring the experimental nature of current work.

Among specific use cases (Figure 79), the most developed areas are ESG exposure and risk identification (34% combined maturity, including 7% deployed), ESG disclosure supervision (31%, 6% deployed), and ESG portfolio alignment and risk analysis (29%, 9% deployed). These patterns reflect supervisory priorities rooted in disclosure frameworks and early-stage transition-risk assessment. By contrast, advanced monitoring use cases – such as greenwashing risk detection, climate-risk transmission mapping, and data-gap analysis – show minimal deployment (1–2% each), highlighting ongoing challenges in accessing consistent data, developing risk-sensitive taxonomies, and integrating climate metrics into existing supervisory workflows.

Persistent structural constraints limit progress. As highlighted in the State of SupTech Report 2024, supervisors face difficulty obtaining reliable climate-related data, operate with non-standardised ESG metrics, and struggle to integrate climate risks into broader prudential or conduct frameworks. Skills gaps also remain significant, particularly in scenario modelling, environmental data analytics, and the interpretation of sustainability disclosures. Together, these constraints help explain why climate and ESG supervision shows high strategic interest but low digital readiness.

FIGURE 79.

Prioritisation of SupTech Use Cases Under Climate/ESG Risks Supervision



Ecomonitor

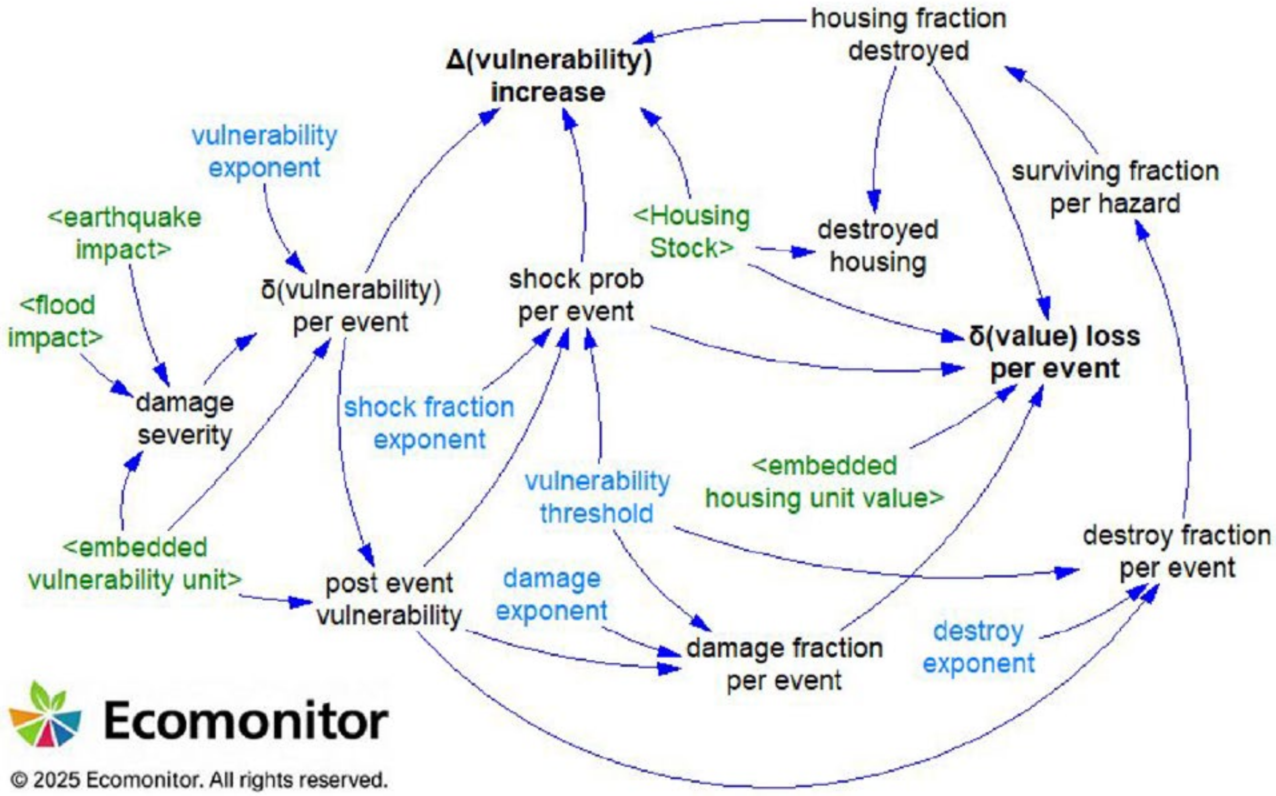
Building Climate Resilience:

A Systems Approach to Close the Protection Gap

By Min-Si Wang (Ecomonitor) and Marios Kargarlis (Ecomonitor)

A widening climate insurance protection gap threatens global stability, as extreme weather phenomena driven by climate change increasingly expose vulnerable populations and institutions to climate hazards and financial risks. Currently, assessments of climate risk relyon linear catastrophe models, which are ill-suited for capturing the nonlinear, feedback-driven dynamics of escalating natural hazards under the increasing pressure of climate change.

HOUSING DAMAGES FROM NATURAL HAZARDS



CONTINUED ON NEXT PAGE

Catastrophe Climate Risks in an Era of Heightened Risk

Traditional catastrophe models follow a simple hazard-vulnerability-loss pathway, ending at loss calculations. However, as floods, typhoons, and wildfires intensify around the world, the protection gap, which is defined as the difference between economic losses and insured losses, widens. This places unsustainable immediate fiscal pressure on institutions charged with covering the vulnerable populations exposed to the protection gap, not to mention the longer-term repercussions on the well-being and economic growth of the affected communities and national economies. For supervisors and regulators, this represents systemic risk that current frameworks struggle to capture and measure effectively.

Closing the protection gap starts with quantifying both its drivers and potential leverage points for mitigation or reversal. Using a systems-based analysis reveals feedback loops that contribute to climate exposures, and the root causes that reinforce a widening protection gap. For instance, climate change intensifies hazard impacts, which in turn damage housing assets in exposed geographies, concentrating risk and increasing vulnerability while raising the cost of insurance. Uninsured losses reduce household capacity for resilience investments, falling affordability reduces insurance coverage, and rising claims push insurance costs ever higher. This creates vicious cycles that accelerate system decline. Without systems analysis that models these interconnected dynamics, and, moreover, accounts for local conditions and contextual nuances, government planners cannot adequately oversee insurers' burgeoning climate risk exposures or assess macro policies that can financially safeguard vulnerable populations by facilitating sustainable and affordable insurance coverage.

A Policy Sandbox Framework

A "sandbox" approach that models systemic impacts offers a pathway for planners tasked with addressing increasingly complex challenges with limited resources. Unlike traditional models, taking a systems approach at natural hazard planning provides decision support tools that enable planners to test policy interventions and understand macro system impacts. For instance, a policy sandbox can integrate the physics of natural hazards with demographics, economics, and infrastructure standards, revealing how these systems interact historically and into the future.

A systems based approach can integrate diverse sources of empirical data to realistically simulate the impact of natural hazards on local infrastructure. This methodology enables models to simulate natural disasters with frequency and magnitude profiles calibrated against

CONTINUED ON NEXT PAGE

historical data, linking the severity of damage with housing vulnerability while accounting for intensifying natural disasters over time. This approach leverages AI/ML capabilities while maintaining flexibility to be adapted across geographies, which is essential for supervisors overseeing a variety of regions.

Whereas the systems approach is adept at representing the dynamics of cause-and-effect relationships, and has been exploited effectively in policy and planning for decades, complex real-world settings encompass aspects that evade such analytical descriptions. This historical limitation can now be effectively addressed by the proliferation of data and powerful ML/AI techniques. In particular, beyond the traditional low-dimensional models aimed at capturing any known and well-understood causal interactions, integrating ML/AI components (e.g., either as preprocessed datasets, or by direct interfacing with external modules such as climate models) into hybrid systems brings empirical data and statistical methods to bear on capturing otherwise intractable features beyond the scope of dynamical systems modeling. The end result is hybrid systems able to produce forecasts of enhanced predictive power for high-stakes decisions.

Policy Levers for Supervisory Intervention

In Ecomonitor’s Bali case study, applying the systems approach summarized above to understand natural hazard impacts, the model explores four strategic policy levers supervisors should consider when reviewing climate risks: retrofit subsidies that reduce future vulnerability, insurance subsidies improving recovery capacity, stricter building code enforcement preventing baseline risks, and post-event relief programs that lessen burdens both for homeowners and insurers. For regulators, understanding how these interventions transform vicious spirals into stabilizing loops is important for designing countercyclical regulatory measures.

Looking Ahead: From Vicious Spirals to Narrowing the Protection Gap

Supervisory decision support tools that capture complex feedback loops are better equipped to assess policy impacts for extreme climate risks. A systems based approach can enable supervisors to identify tipping points, where incremental climate pressures suddenly cascade into systemic financial disruption. With insured losses reaching $145 billion in 2024 ,financial authorities should consider embracing tools that reflect the interconnected nature of policy and climate risks to better manage the widening protection gap.

3.5 Competition monitoring

Competition monitoring remains one of the least developed suptech domains in 2025, reflecting both limited mandates and the early stage of digital tools available to financial authorities. Although interest is growing – particularly in pricing analytics, market concentration monitoring, and data-driven screening – adoption remains low, with very few deployed solutions and most initiatives still in proof-of-concept or prototype form. At the same time, advances in computational methods and AI-enabled detection systems used by competition authorities globally demonstrate the potential for more proactive, data-driven approaches to identifying market distortions, collusion, and emerging conduct risks in digital financial markets. Supervisors are beginning to explore these capabilities, but strategic prioritisation and resourcing remain limited.

Competition monitoring requires structured data on pricing, concentration, switching frictions, and market-power dynamics, yet most authorities lack integrated datasets or analytical tooling capable of detecting distortions across digital financial markets.

Digitalisation is reshaping competitive dynamics across financial services, creating new business models and data-driven platform ecosystems that can generate efficiency but also exacerbate market concentration and switching frictions. Evidence from competition and financial inclusion research indicates that these structural features can materially affect affordability and access, particularly for underserved populations. As markets evolve, supervisory authorities face increasing pressure to understand how pricing patterns, algorithmic systems, and market structures influence competitive behaviour.

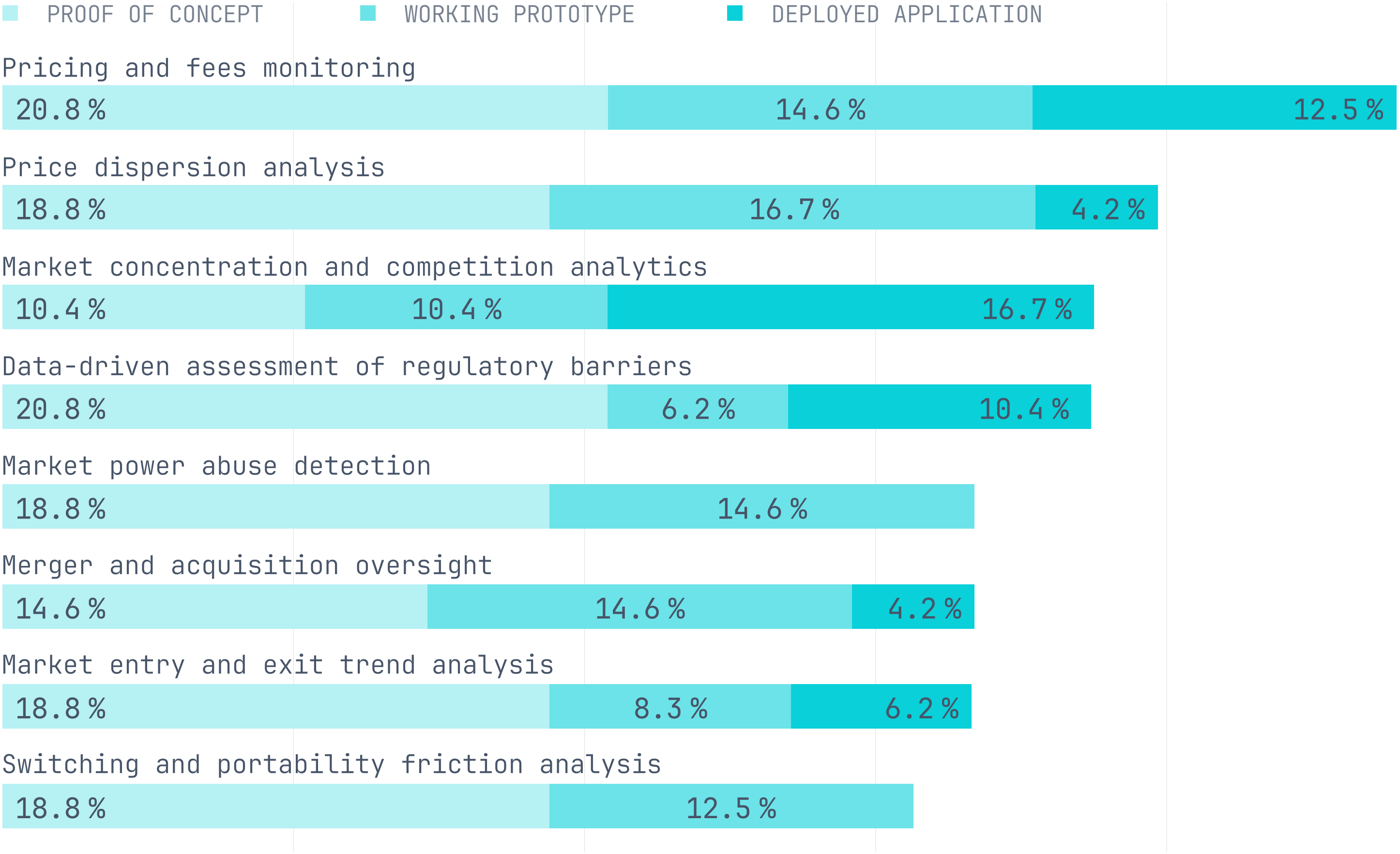
Historically, competition monitoring has relied on a blend of reactive approaches – such as leniency programmes and whistle-blower evidence – and more proactive supervisory instruments including market studies and screening exercises. As discussed in last year's report, competition authorities globally have begun experimenting with computational methods that support earlier detection of potential harms. Examples include initiatives in Brazil, Korea, and the United Kingdom, which incorporate machine learning or network analytics to identify anomalies. European agencies have expanded in-house analytical capabilities for similar purposes, including algorithmic screening and document analysis. Although these developments fall outside traditional financial supervision, they represent a broader shift toward data-driven surveillance that may become relevant as competition issues gain prominence in digital financial markets.

Survey results, however, show that competition monitoring remains a comparatively low priority within suptech portfolios. Only a small share of authorities report fully deployed applications, and most activity is concentrated at early stages of experimentation (Figure 71). A significant proportion of respondents indicated that solutions in this domain are desired but not yet planned, while proof-of-concept and prototype initiatives are present only in select areas. This pattern is consistent with the limited formal mandate many financial authorities have in competition oversight, as well as the data constraints associated with assessing market power, pricing behaviour, or switching frictions at scale.

Where development is occurring, it is concentrated in foundational analytical capabilities (Figure 80). Pricing and fees monitoring shows the highest level of combined activity (48%), reflecting its alignment with existing supervisory datasets. Price dispersion analysis (40%), market concentration and competition analytics (38%), and data-driven

FIGURE 80.

Prioritisation of SupTech Use Cases Under Competition Monitoring



assessments of regulatory barriers (37%) also appear across a meaningful subset of authorities. These areas rely on structured data and established analytical techniques, making them more accessible entry points for experimentation.

More complex forms of competition analysis remain less developed. Supervisors report limited engagement in market power abuse detection (33%), switching and portability friction analysis (31%), and merger and acquisition oversight (33%). No authorities report deployed solutions in these areas, and activity is generally confined to early-stage pilots. These gaps underline the technical complexity of competition analytics in digital markets and reflect the broader institutional reality that many financial authorities do not collect the behavioural or transaction-level data required for robust assessments.

Taken together, the findings suggest that competition monitoring is still at the periphery of suptech development. Activity is low, mandates are often limited, and technical requirements are high. Nevertheless, the broader evolution of computational antitrust demonstrates a growing set of analytical tools that could support financial authorities as competition issues become more intertwined with consumer outcomes, data access, and digital market design. As digital platform finance expands, demand for these capabilities is likely to increase, but materially scaling them will require clearer institutional mandates, improved data access, and collaboration with national competition agencies already developing advanced digital enforcement methods.

3.6 Compliance assistance

Compliance assistance is emerging as a practical entry point for suptech adoption as authorities increasingly depend on structured reporting taxonomies, machine-readable rules, and automated validation architectures. These tools support consistent interpretation of regulatory requirements, reduce procedural workload for supervised entities, and improve the timeliness and accuracy of submissions. Survey results show moderate but steady maturity, with foundational capabilities such as automated reporting and rule-based validation widely deployed, while more advanced functions remain at early stages of development. Progress reflects a broader shift toward standardised, data-driven compliance processes, though supervisory independence, safeguards for automated guidance, and cross-jurisdictional knowledge exchange will remain critical as authorities scale these systems.

Compliance assistance increasingly depends on machine-readable rules, structured reporting taxonomies, and automated validation architectures, making it a natural entry point for suptech adoption.

Compliance assistance applications aim to reduce the regulatory burden on supervised entities and enhance the clarity, consistency, and timeliness of compliance processes. As regulatory frameworks become more complex and supervisory resources remain stretched, these tools support automated reporting, provide real-time regulatory guidance, and streamline compliance checks.

In 2025, 44% of authorities reported deploying or developing compliance assistance solutions, with 16% indicating fully operational systems. Early-stage activity is also evident, with 14% at proof-of-concept stage and 13% piloting prototypes. Demand remains strong: 30% of authorities report seeking such tools but without formal plans for implementation (Figure 71).

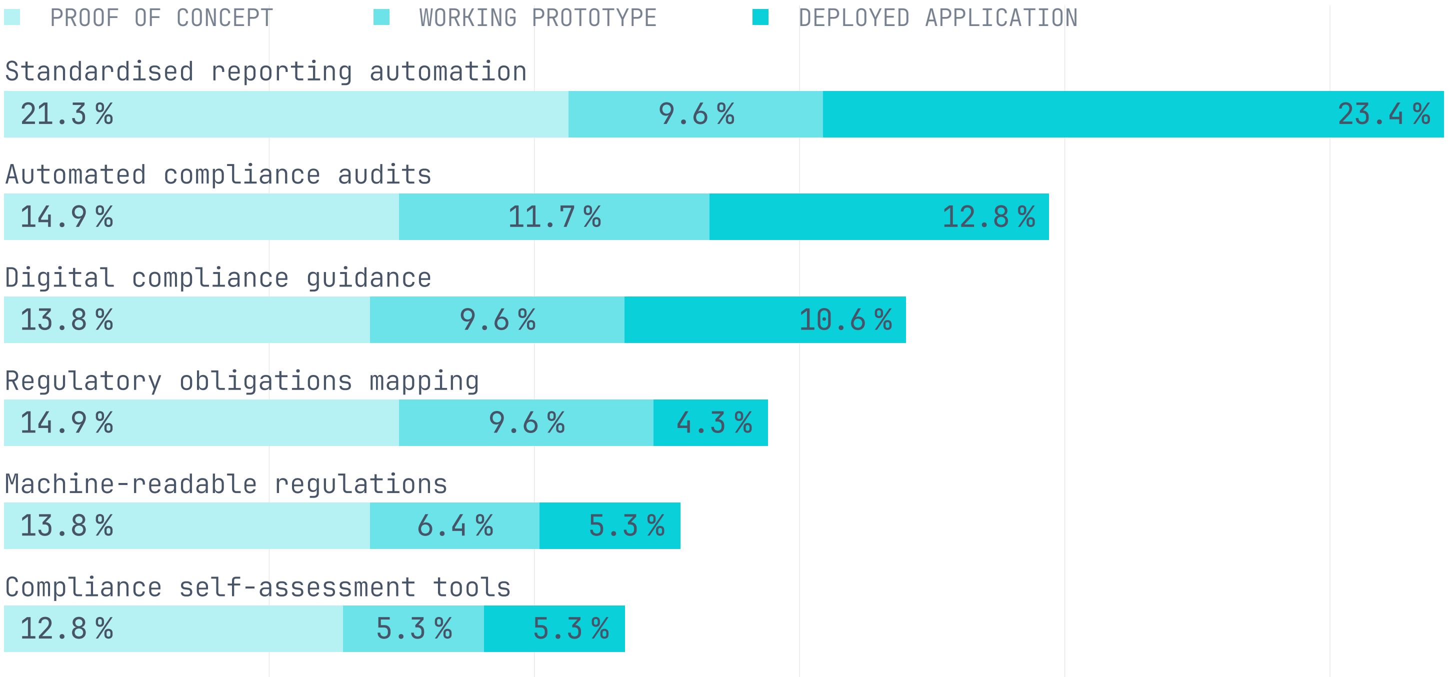
At the use-case level (Figure 81), standardised reporting automation is the most mature application, with a combined 54% of authorities either deploying, prototyping, or testing solutions. Automated compliance audits follow at 39%, reflecting interest in systems that automatically validate submissions against predefined rules. Digital compliance guidance reaches 34%, including AI-enabled portals and chat interfaces that assist firms with regulatory interpretation. More advanced capabilities remain underdeveloped: regulatory obligations mapping (29%), machine-readable regulations (26%), and compliance self-assessment tools (23%) show lower uptake, indicating that continuous, proactive compliance management is still in its early stages.

A number of authorities have begun to pilot innovative solutions. The Philippines SEC introduced SEC AInnovation, an AI-powered multilingual chatbot providing real-time guidance on laws and regulations, reducing manual research and physical visits. Abu Dhabi's FSRA developed Jisr, a translation tool converting Arabic documents to English while preserving legal context, improving clarity and turnaround and also piloted RegBuddy conversational AI Assistant to help firms access regulatory guidance in real time. Jersey's FSC provides Reggie, a regulatory chatbot guiding industry compliance, while Regxelerator's supervisory compliance assessment tool uses workflow automation and generative AI to deliver end-to-end, evidence-based assessments of firms' policies against regulatory standards.

Overall, compliance assistance demonstrates solid progress in areas closely linked to reporting and rule-based validation, but uneven uptake in more advanced, data-driven applications. As regulatory complexity increases, these tools

FIGURE 81.

Prioritisation of SupTech Use Cases UnderCompliance Assistance



can help reduce burdens, particularly for smaller institutions, while improving the consistency and efficiency of supervisory processes. Ensuring appropriate safeguards, maintaining supervisory independence, and supporting knowledge exchange across jurisdictions will be central to scaling these innovations responsibly.

3.7 Consumer protection and market conduct supervision

Consumer protection and market conduct supervision remains a mature and high-priority suptech domain, ranking third globally. Authorities in both advanced and emerging markets show strong adoption, primarily using suptech to improve the efficiency and responsiveness of consumer-facing processes. The most widespread applications support complaints referral, tracking, and resolution, followed by trend analysis and real-time complaints monitoring. While these foundational capabilities are well established, more advanced supervisory use cases – such as algorithmic auditing, dark-pattern detection, and profiling of vulnerable consumers – remain markedly underdeveloped, indicating a continued emphasis on reactive, case-driven oversight rather than proactive identification of emerging risks.

Consumer-protection supervision relies on rapid ingestion and classification of high-volume, multi-channel data — complaints, social-media signals, behavioural indicators — and suptech tools are being deployed primarily to improve timeliness and consistency in these workflows.

Global attention in consumer protection has increasingly concentrated on two fast-moving areas: the rapid rise of finfluencer activity and the persistent escalation of fraud and scams. Scams remain pervasive, with surveys indicating that 57% of adults globally experienced an attempted scam in the past year. This includes digital payment fraud, online investment scams, deepfake-enabled impersonations, and social-engineering schemes. Supervisory responses include new finfluencer guidance aligned with IOSCO, stronger cross-platform cooperation with social media companies, and investments in early detection tools and cross-border information-sharing mechanisms such as IOSCOS's I-SCAN hub.

Authorities are expanding their toolkits to strengthen prevention, detection, and disruption of misconduct, combining technological innovation with reforms to governance, collaboration, and public education. Cross-sector alliances – such as the Canadian Anti-Scam Coalition (CASC), the Anti-Scam Alliance in New Zealand, and the Indonesia Anti-Scam Center, led by the Indonesian Financial Services Authority (OJK) in collaboration with other government agencies. The Securities Commission Malaysia and Malaysian Communications and Multimedia Commission are also stepping up cooperation against online scams, using enforcement, prevention, and AI. Regionally, efforts such as the West Africa Payments Fraud Policy Sprint, hosted by Alliance for Innovative Regulation in collaboration with the West African Monetary Institute, seek to close governance and coordination gaps.

Policy and governance initiatives continue to evolve in tandem. The Anti-Scam Consumer Protection Charter 3.0 in Hong Kong introduces principles targeting improved financial scam reporting and internal platform monitoring, and Singapore implemented restrictions for scam mules. In the United States, the CFPB imposed a USD 175 million penalty on Block for fraud management failures and the CFTC reorganised its Division of Enforcement into two task forces to better safeguard fraud victims.

Technology plays an increasingly central role in fraud detection and supervisory intelligence. South Korea's FSC developed an anti-vishing AI platform, and Malaysia's BNM/PayNet implemented AI-based fraud monitoring. Swift, in collaboration with thirteen international banks, is piloting AI-powered fraud detection using federated learning to improve real-time identification rates. Concurrently, authorities and vendors are expanding capabilities for takedown, investigation, and recovery. ASIC in Australia has expanded its ability to remove fraudulent investment ads from social-media platforms, while suptech providers such as FNA and Proto are supporting end-to-end recovery solutions. FNA has secured a Gates Foundation grant to develop a cloud-based fraud portal, and Abhi is supporting central banks in extracting supervisory value from unstructured data using AI and LLMs (see case study).

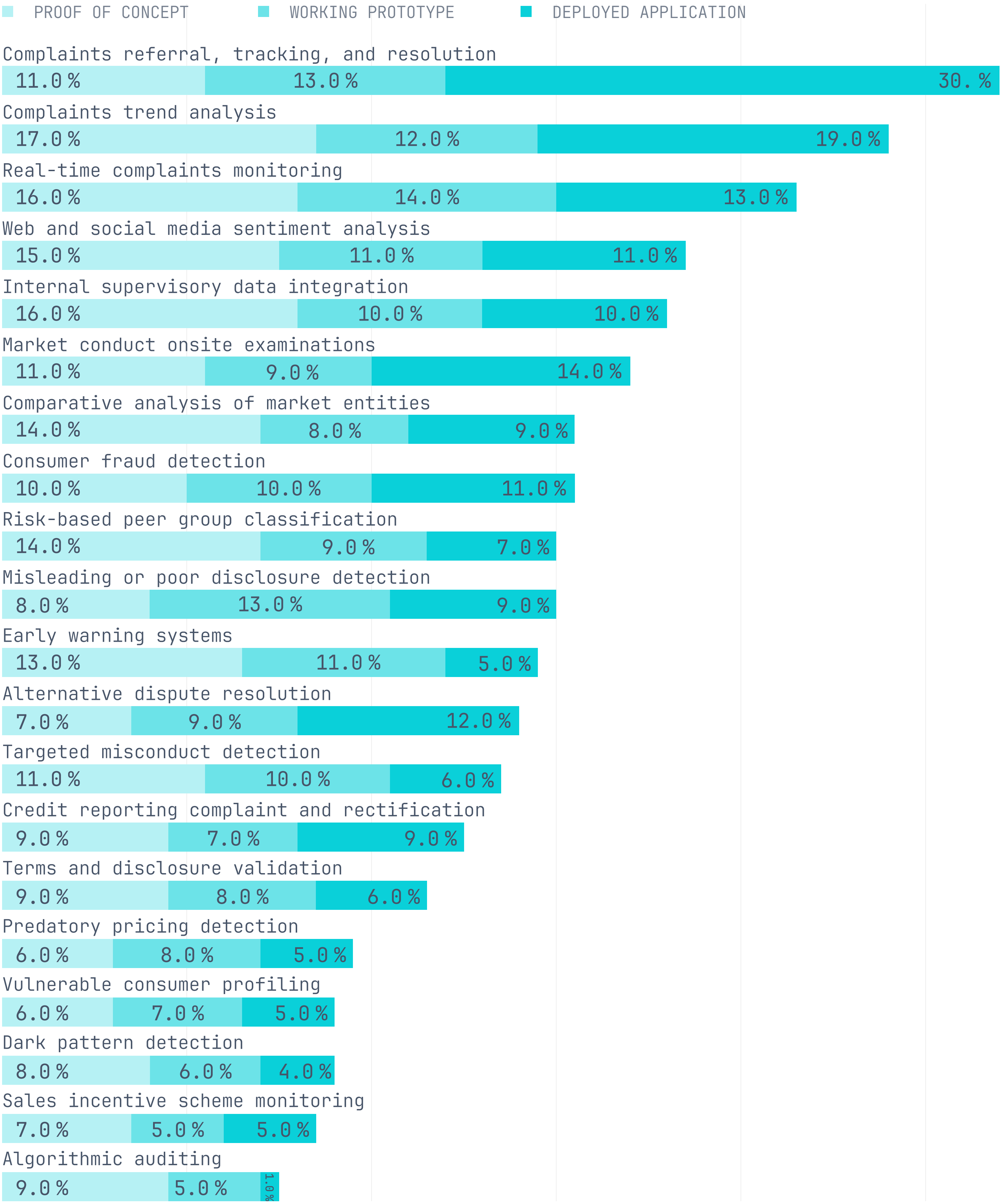
Across the survey sample, consumer protection remains one of the most widely adopted suptech domains, with AEs (48%) and EMDEs (52%) showing similar levels of activity (Figure 74). The most mature use cases relate to the processing and analysis of consumer feedback. Complaints referral, tracking, and resolution reach a combined maturity of 54%, followed by complaints trend analysis (48%) and real-time complaints monitoring (43%) (Figure 82). Authorities are integrating increasingly sophisticated tools: the Bank of Portugal's AI platform, Alya, classifies banking clients' complaints and information requests; Regxelerator as demonstrated GenAI-enabled workflows for classifying financial consumer complaints and assessing social media promotions.

Beyond complaints management, suptech applications address a wider range of conduct risks. Web and social-media sentiment analysis (37% combined maturity) is moderately developed, as are comparative analysis of market entities (31%), early warning systems (29%), and market conduct onsite examinations (34%). Established compliance-related tools such as disclosure quality analysis (30%) and consumer fraud detection (31%) show steady, though not widespread, uptake.

More advanced and forward-looking areas remain at early stages. Vulnerable consumer

FIGURE 82.

Prioritisation of SupTech Use Cases Under Consumer Protection And Market Conduct Supervision



profiling (18% combined maturity), dark-pattern detection (18%), and algorithmic auditing (15%) show limited progress. These gaps highlight two structural challenges: many authorities lack mandates to monitor firms' digital design practices, and supervisory datasets often do not capture the behavioural or algorithmic information needed to assess these risks effectively.

The convergence of digital channels, finfluencers, and cross-border fraud creates risks that exceed the reach of traditional supervisory models. Addressing these challenges will require authorities to reinforce foundational mechanisms for complaints and conduct monitoring while expanding advanced analytics, platform-level monitoring, ecosystem collaboration, and international information-sharing.

Decoding Complaints at Scale:

How a central bank in the Middle East in collaboration with secondees from fintech firm Abhi unlocked value from unstructured consumer data

Ejaz Anwer (Technical Lead & Deployment Architect, Abhi), Ahmad Butt (Solution Designer & Author of Technical Documentation, Abhi), and Burat Ahmed (NLP & Machine Learning Engineer, Abhi)

A central bank in the Middle East shared the challenge of receiving thousands of consumer complaints annually. This data represents a critical, yet often under-leveraged, source of supervisory intelligence. The primary hurdle was that these complaints arrived in unstructured formats, such as handwritten letters, scanned images, PDFs, and forms, often submitted in both Arabic and English. Manually reviewing, classifying, and acting upon this volume of data was time-consuming and susceptible to inconsistencies.

To address this, the central bank sought to leverage AI technologies to automate the extraction and structuring of this complaint data. Through the Public-Private Secondments in SupTech Innovation initiative, co-led by the Cambridge SupTech Lab and the World Economic Forum, a dedicated seconded team from Abhi, a fintech infrastructure company based in Pakistan, collaborated directly with the central bank's supervision and IT departments. The team comprised experts in Optical Character Recognition (OCR), natural language processing (NLP), and large language models (LLMs). The project's objective was to co-design a proof of concept aligned with the central bank's digital transformation strategy.

The resulting prototype has the potential to dramatically improve supervisory efficiency. Complaints that previously demanded manual reading and tagging can now be structured with high accuracy in seconds. This technological transfer built capacity within the central bank, as supervision and IT teams gained familiarity with modern AI tooling.

The immediate impact is improved operational efficiency. The long-term vision is to move from reactive complaint handling toward intelligent supervisory resolution. Following the proof of concept's insight, the central bank is exploring operational deployment and extending the system to link structured complaints to predefined resolution actions, improving consumer outcomes through consistent response strategies and faster triage. Furthermore,

CONTINUED ON NEXT PAGE

the modular design and open-source delivery of the solution enhance its replicability for other financial authorities dealing with similar multilingual and unstructured data challenges.

The solution delivered by Abhi was a modular, AI-driven pipeline designed to ingest and analyze consumer complaints. Key functional and technological components included:

Optical Character Recognition (OCR): The system utilized a custom-trained engine (Surya OCR) optimized for scanned Arabic text, including noisy or handwritten documents, achieving 91.6% character-level accuracy for low-resolution documents. Pre-processing steps, such as skew correction and noise filtering, improved OCR accuracy by 13%.

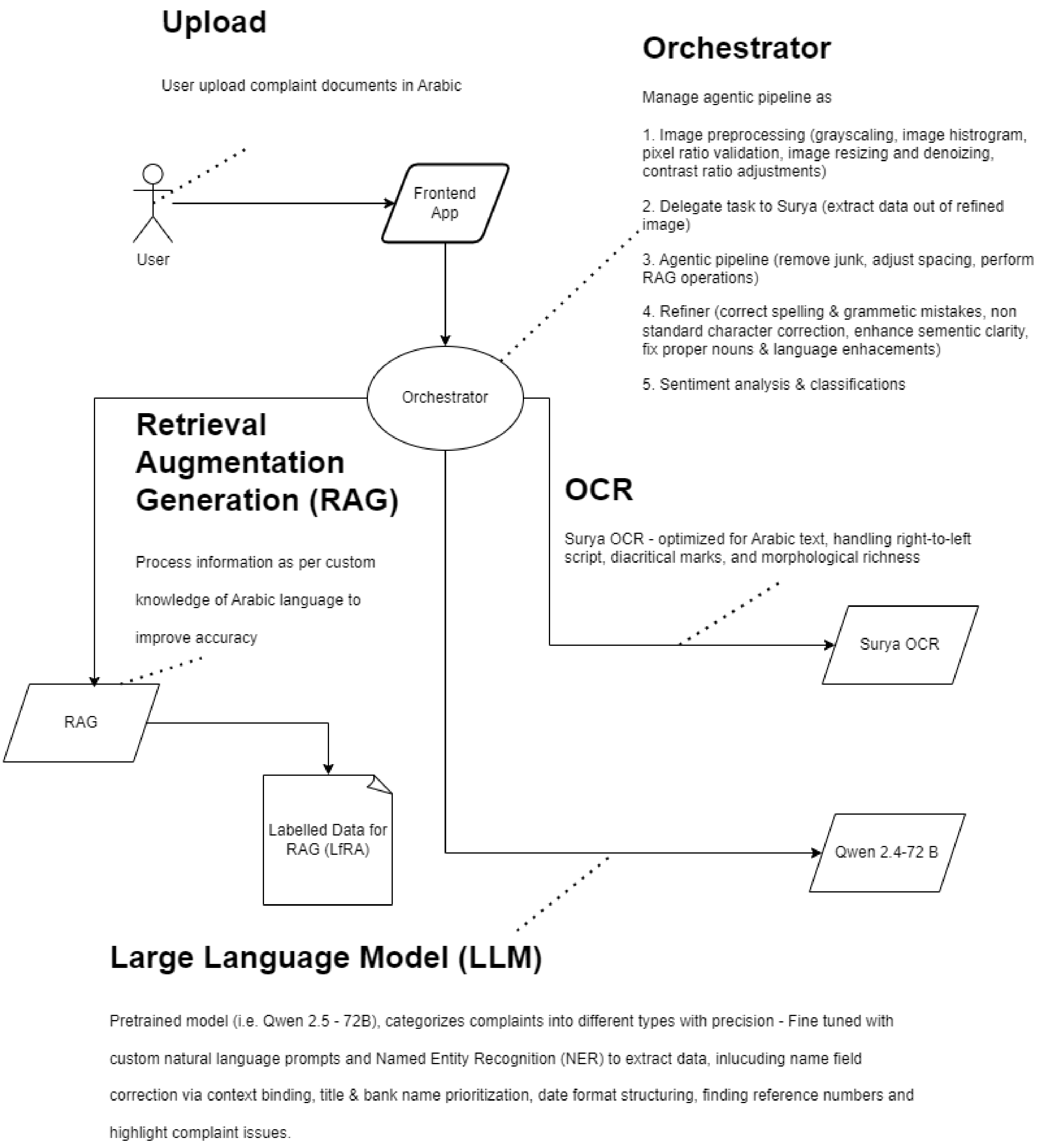
- **Multilingual NLP Pipeline:** The architecture supported a dual-language NLP pipeline for consistent semantic analysis across both Arabic and English inputs.
- **AI and Entity Recognition:** The system used rule-based matching and trained Named Entity Recognition (NER) models (e.g., Qwen-72B) to identify financial product types, complaint themes, and involved institutions.
- **Large Language Model (LLM) Integration:** A Retrieval-Augmented Generation (RAG) mechanism and Labeling for Retrieval Augmentation (LfRA) were integrated to enhance prediction accuracy and interpretability. This LLM module was fine-tuned to identify implied intent and disambiguate noisy OCR output.
- **Output Structuring:** All extracted data is transformed into a structured JSON format, mapping essential fields like the nature of the complaint, product type, and suggested next steps.

The project was executed through the Public-Private Secondments for SupTech Innovation initiative, a project of the Cambridge SupTech Lab with the World Economic Forum (WEF) which pairs technical experts from the private sector with financial authorities through short-term secondments.

A crucial requirement for the central bank was that the solution must be deployed on-premise, eliminating reliance on external cloud infrastructure to comply with data privacy and security policies. Abhi achieved this by delivering all outputs as open-source, mitigating concerns about vendor lock-in. The delivery package included a detailed on-premise deployment plan and containerized services (via Docker) to facilitate integration into the central bank's secure IT stack. The solution design was tested on real complaint documents and validated by native Arabic experts and central bank staff.

CONTINUED ON NEXT PAGE

HIGH LEVEL ARCHITECTURE DIAGRAM



Upload

User upload complaint documents in Arabic

Orchestrator

Manage agentic pipeline as

1. Image preprocessing (grayscaling, image histrogram, pixel ratio validation, image resizing and denoizing, contrast ratio adjustments)

2. Delegate task to Surya (extract data out of refined image)

3. Agentic pipeline (remove junk, adjust spacing, perform RAG operations)

4. Refiner (correct spelling & grammetic mistakes, non standard character correction, enhance sementic clarity, fix proper nouns & language enhacements)

5. Sentiment analysis & classifications

Retrieval Augmentation Generation (RAG)

Process information as per custom knowledge of Arabic language to improve accuracy

OCR

Surya OCR - optimized for Arabic text, handling right-to-left script, diacritical marks, and morphological richness

Large Language Model (LLM)

Pretrained model (i.e. Qwen 2.5 - 72B), categorizes complaints into different types with precision - Fine tuned with custom natural language prompts and Named Entity Recognition (NER) to extract data, inlucuding name field correction via context binding, title & bank name prioritization, date format structuring, finding reference numbers and highlight complaint issues.

3.8 Cyber risk supervision

Cyber risk supervision remains moderately developed within suptech portfolios, with 43% of authorities deploying or building applications in this domain. Most activity concentratesonfoundationalusecases–risk assessment, compliance monitoring, and incident reporting – while more advanced capabilities such as audit-trail verification, third-party cyber-risk oversight, and threat-intelligence integration remain comparatively limited. The pattern reflects a supervisory focus on compliance and post-incident workflows rather than proactive, system-level resilience, despite rising geopolitical tensions, growing third-party dependencies, and heightened cyber threats linked to digitalisation and AI adoption.

Cyber risk remains a central concern for financial authorities, amplified by geopolitical tensions, increasing reliance on third-party service providers, and the expanding attack surface from digitalisation and AI adoption. Supervisory responses continue to focus on establishing minimum resilience expectations, strengthening cross-sector intelligence sharing, and integrating threat-led testing and simulation exercises into supervisory practice. Globally, there is growing attention to emerging risks associated with quantum computing and AI-enabled attack vectors. Cyber-risk supervision also varies across institutional arrangements, with some authorities sharing responsibility with national cybersecurity agencies, which affects tooling, data access, and maturity.

Despite its strategic importance, cyber-risk supervision shows only moderate maturity in suptech adoption. Across the survey, 43% of authorities report deploying or developing applications in this domain (Figure 71). At the same time, 38% classify cyber suptech as "desired but not planned", indicating a persistent gap between supervisory priorities and institutional capacity to operationalise digital solutions.

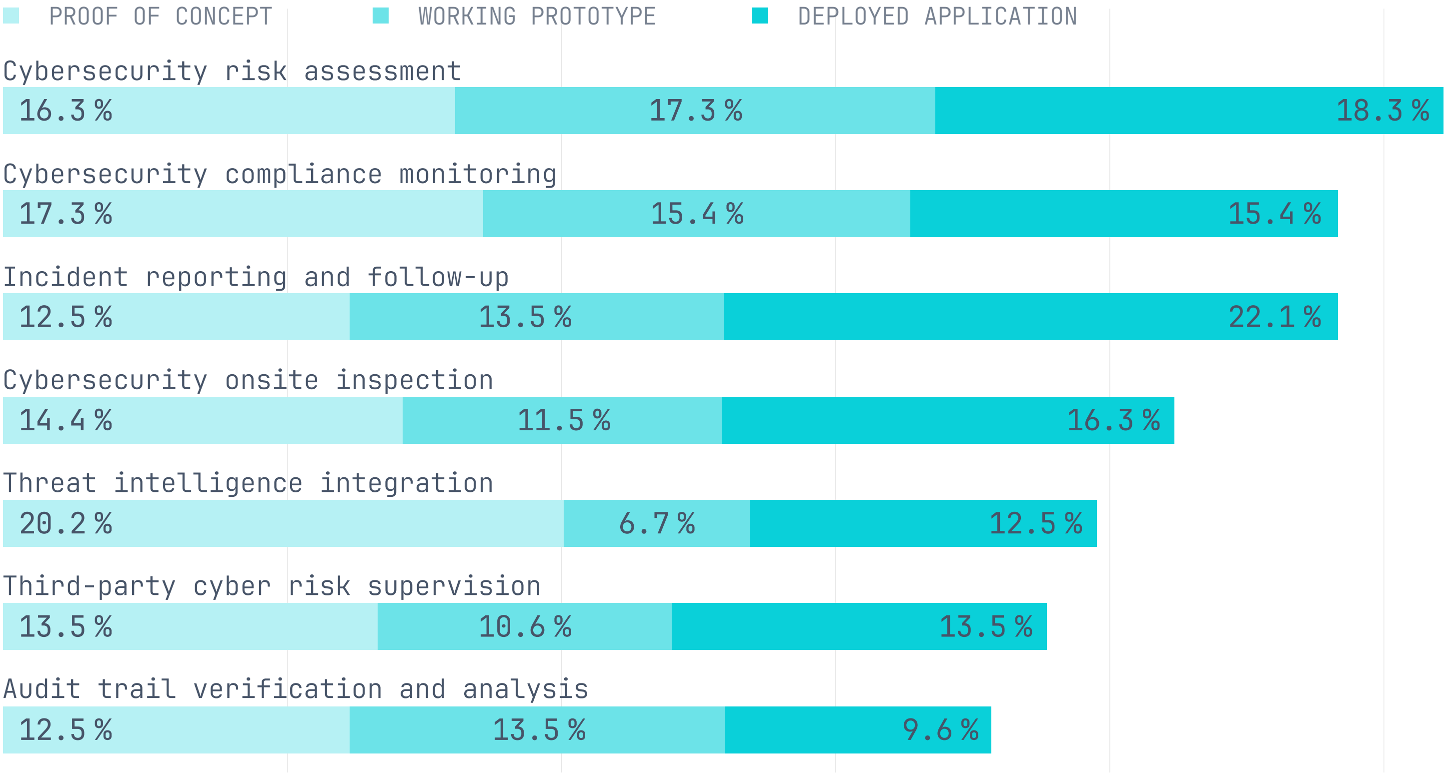
The most developed use cases are those aligned with established supervisory workflows. Cybersecurity risk assessment reaches 52% combined maturity, followed by cybersecurity compliance monitoring (48%) and incident reporting and follow-up (48%) (Figure 83). These patterns indicate that authorities are prioritising standardised data collection, verification of compliance with existing frameworks, and more structured reporting of cyber incidents. For example, the Financial Stability Board's FIRE framework (Format for Incident Reporting Exchange) supports more consistent incident-reporting practices across jurisdictions, while SFC Colombia's 360 Dashboard provides supervisors with streamlined compliance monitoring and vulnerability-detection tools (see case study).

Technological advances are also influencing supervisory interest in more forward-looking capabilities:

- **Quantum resilience:** The BIS Innovation Hub's Project Leap (Phase 2) is testing post-quantum signatures in European payment systems, and the Monetary Authority of Singapore (MAS) has conducted sandbox trials for Quantum Key Distribution to assess secure communication channels.
- **AI and threat intelligence:** Several authorities are developing shared intelligence platforms, including the Central Bank of Kenya's Banking Sector Cybersecurity Operations Centre and the Bank of Mauritius' forthcoming initiative. Korea's FSS is planning an integrated control system to aggregate cyber-threat information across the financial sector.

FIGURE 83.

Prioritisation of SupTech Use Cases Under Cyber Risk Supervision



- **Detection and response:** Supervisors increasingly explore AI-enabled threat-analysis techniques – for example, anomaly detection and behavioural analytics – though deployments remain limited and predominantly in exploratory or industry-pilot phases.

Critical gaps persist. Third-party cyber-risk supervision stands at 38% combined maturity, despite growing systemic dependence on cloud and outsourced ICT service providers. This exposure is receiving regulatory attention. For example, APRA has reinforced minimum expectations for cyber resilience in the superannuation sector following recent incidents, underscoring the need for stronger oversight of external service providers and the operational interdependencies they create. Similar policy developments, such as the EU's Digital Operational Resilience Act (DORA), aim to address this vulnerability, although supervisory suptech applications to support these expectations remain limited.

Other advanced areas also lag behind: audit-trail verification and analysis (35% combined maturity) and threat-intelligence integration (39%) are still at early institutional stages, reflecting constraints in analytics capability, data availability, and governance maturity.

Overall, cyber suptech is progressing but not yet keeping pace with the accelerating risk environment. Authorities continue to prioritise compliance-focused and incident-management tools, while more proactive, resilience-oriented capabilities remain constrained by resource, skills, and data limitations. Addressing these gaps will be essential as cyber threats become more complex and as financial systems deepen their reliance on interconnected digital infrastructures.

Financial Superintendency of Colombia:
360 dashboard for operational risk and cybersecurity

Tatiana Lorena Chaparro Pineda (Professional at the Directorate of Research, Innovation and Development), Mauricio Chaparro Benavides (Advisor, Delegation for Operational Risk and Cybersecurity), and Francisco Javier Duque Sandoval (Director of Research, Innovation and Development), Financial Superintendency of Colombia

In recent years, financial institutions have accelerated their digital transformation, adopting channels such as web portals and mobile applications to enhance customer experience and expand their reach. However, this evolution has increased exposure to increasingly sophisticated cyber threats, requiring proactive measures to protect information and ensure operational continuity.

In response, the Financial Superintendency of Colombia (SFC) strengthened its regulatory framework through External Circular 007 of 2018 and External Circular 033 of 2020, which set requirements for information security management, cybersecurity, and incident reporting. As part of this strategy, the SFC launched the 360 Dashboard for Operational Risk and Cybersecurity to assess the inherent cyber risk profile, cybersecurity maturity level, IT management, and business continuity plans of supervised entities based on international standards such as the NIST Cybersecurity Framework 2.0 — developed by the U.S. National Institute of Standards and Technology to guide organizations in identifying, protecting, detecting, responding, and recovering from cyber threats — and COBIT (Control Objectives for Information and Related Technologies), a globally recognized framework for IT governance and management that ensures technology supports business objectives and regulatory compliance.

In this context, the implementation of the 360 Dashboard for Operational Risk and Cybersecurity requires the active participation of several key stakeholders within the financial ecosystem. The Financial Superintendency of Colombia (SFC) leads the initiative as the regulatory authority, responsible for setting cybersecurity standards, monitoring compliance, and using the dashboard to strengthen supervisory capabilities and ensure systemic resilience. Supervised financial institutions play a fundamental role by providing data for risk and maturity assessments, implementing corrective measures based on supervisory feedback, and adopting best practices to improve

CONTINUED ON NEXT PAGE

their cybersecurity posture. Additionally, the technology, risk, and compliance departments within these institutions are essential for executing cybersecurity strategies, managing operational risk, and ensuring adherence to regulatory requirements and international frameworks such as NIST and COBIT.

Finally, the financial sector has experienced a significant increase in cyber incidents this year, particularly due to events affecting third-party providers that support the operations of supervised entities in Colombia. This trend underscores the need to measure cybersecurity maturity and operational resilience through internationally recognized standards such as the Digital Operational Resilience Act (DORA). Supervisors face the dual challenge of ensuring that institutions strengthen their resilience capabilities and comply with global best practices and regulatory requirements.

Supervisory relevance

The 360 Dashboard plays a critical role in strengthening the supervisory capabilities of the SFC. By providing a comprehensive view of cybersecurity, IT management, and business continuity maturity levels, the tool enables the SFC to monitor progress across supervised entities in a structured and consistent manner. This functionality not only supports compliance with emerging regulatory mandates on digital resilience and incident reporting but also facilitates early detection of potential vulnerabilities that could lead to cyber incidents. Furthermore, the dashboard helps identify gaps against international best practices, allowing the SFC to guide institutions toward corrective actions and improved resilience. Ultimately, this initiative promotes a proactive risk management culture within the financial sector, reduces the likelihood and impact of cyber threats, and strengthens the overall security posture of the Colombian financial system.

Key features

The solution is built upon globally recognized frameworks such as the NIST Cybersecurity Framework 2.0, COBIT, and guidelines from the Financial Services Sector Coordinating Council in the United States. Its design incorporates several functional modules that collectively provide a holistic assessment of operational and cyber resilience. These modules include the measurement of inherent cyber risk exposure, cybersecurity posture, and assessments of IT management and business continuity planning. Additionally, the dashboard offers automated reporting capabilities that highlight key indicators and gaps, enabling supervisors to make informed decisions quickly. From a technological perspective, the platform leverages a web-based interface for data collection and analysis, complemented by interactive dashboards that present results in a clear

CONTINUED ON NEXT PAGE

and actionable format. This combination of robust methodology and advanced technology ensures that the tool delivers accurate insights and supports effective supervisory interventions.

Development process

The development of the 360 Dashboard was a gradual and strategic process aligned with regulatory evolution. It began in 2018 with the issuance of External Circular 007, which established minimum cybersecurity requirements for supervised entities. This initial step laid the foundation for a more comprehensive approach, which was reinforced in 2020 through External Circular 033, introducing mandatory incident reporting and performance metrics. Building on these regulatory milestones, the SFC designed the dashboard by defining a methodological framework grounded in international standards and adapting it to the Colombian context. The implementation phase included the development of the technological platform and pilot testing with selected institutions to validate functionality and usability. Despite these achievements, the process faced challenges such as standardizing data from operational resilience assessments and ensuring that global best practices were effectively tailored to local regulatory requirements. Overcoming these obstacles was essential to delivering a solution that meets both international benchmarks and national supervisory needs.

Future vision

Building on the collection of cybersecurity maturity assessments, inherent risk evaluations, cybersecurity posture reviews, IT management analyses, and Business Continuity Plan (BCP) exercises, the next step is to apply AI, ML, and Big Data analytics. These technologies will be used to forecast potential cyber incidents and identify emerging vulnerabilities, enabling the generation of early-warning alerts to prevent the materialisation of threats. This predictive approach will strengthen risk-based supervision and help mitigate complex situations within the financial system.

The initiative includes the integration of the 360 Dashboard for Operational Risk and Cybersecurity as a core component of this strategy, leveraging its structured data and insights to feed advanced analytical models. This vision aligns with the Financial Superintendency of Colombia's mission to preserve stability and operational resilience, forming an integral part of its strategic roadmap for digital supervision.

3.9 Digital assets oversight

Digital-assets supervision is advancing, but suptech adoption remains limited. Authorities are concentrating on foundational investigative capabilities – such as transaction tracing, wallet forensics, and on-chain network analysis – while more advanced oversight functions, including stablecoin reserve verification, automated compliance checks, and algorithmic-asset monitoring, show minimal maturity. Strong policy activity contrasts with modest operational deployment, indicating that supervisory tools have not yet caught up with rapidly evolving regulatory frameworks.

Digital-asset supervision requires real-time on-chain analytics, wallet-forensics capabilities, and structured entity-licensing data, yet most authorities remain constrained by limited data access, uneven mandates, and early-stage technical tooling.

Supervision of digital assets is evolving against a backdrop of significant regulatory developments. Jurisdictions are moving to clarify the scope of regulated activities, define licensing regimes for stablecoin issuers, and strengthen enforcement relating to market integrity, consumer protection, and illicit finance. In 2025, this included the implementation of the EU's Markets in Crypto-Assets Regulation (MiCAR), continued supervisory actions by the U.S. SEC regarding asset classification and staking activities, and U.S. Treasury consultations on the proposed GENIUS Act for stablecoins. Globally, bodies such as the FSB and IOSCO continued monitoring the implementation of their crypto-asset and stablecoin recommendations to promote regulatory consistency across jurisdictions.

Stablecoins remain a central focus of regulatory activity, leading to new licensing regimes and enhanced cross-border collaboration. The Hong Kong Monetary Authority implemented a fiat-referenced stablecoin licensing regime in August 2025, mandating full backing by high-quality liquid assets and strict AML/CFT compliance. Other jurisdictions including the UK, Vanuatu and Australia are rolling out comprehensive frameworks for stablecoin issuers and Virtual Asset Service Providers (VASPs). Cross-border collaboration is also strengthening, exemplified by the Bank of England and NYDFS Transatlantic Regulatory Exchange, which fosters knowledge transfer and alignment on emerging payment and digital asset risks. At the same time, the Bermuda Monetary Authority (BMA) launched a call for proposals to pilot embedded supervision within decentralised finance, reflecting growing interest in supervisory models built directly into blockchain infrastructures.

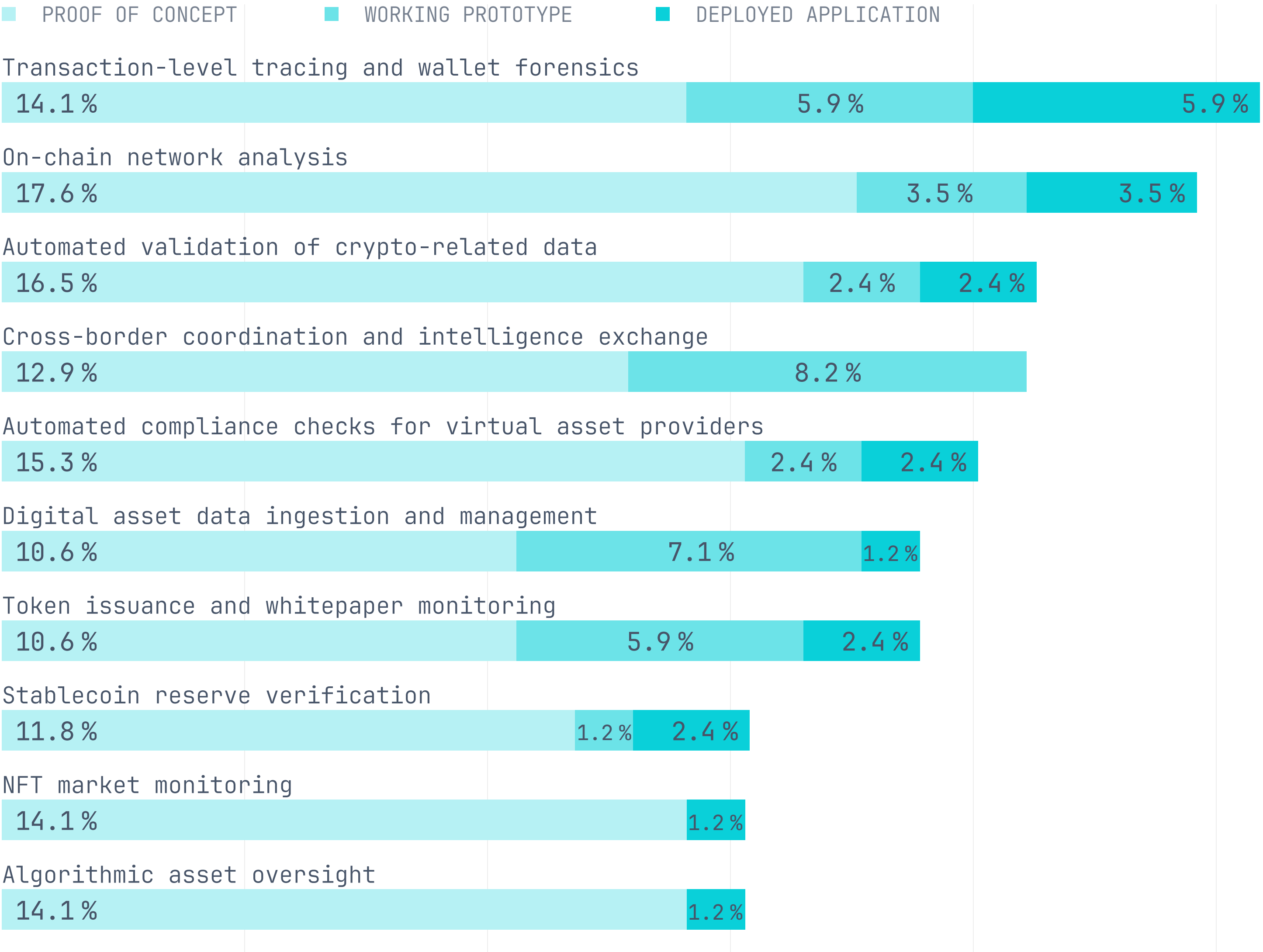
Despite this regulatory progress, digital asset suptech adoption remains modest. 29% of authorities indicate having deployed applications, working prototypes, and POCs.

However, a large proportion of authorities 37% indicate that these applications are 'Desired but not planned', suggesting a strong interest that has not yet translated into widespread implementation (Figure 71).

The development of suptech for digital assets is currently focused on core investigative and compliance activities, though overall maturity remains modest. The most developed use cases are centred on data analysis and forensics: Transaction-level tracing and wallet forensics (26% combined maturity) and on-chain network analysis (25%) (Figure 84). These tools are critical for tracing asset flows and detecting illicit activity, as evidenced by the Bermuda Monetary Authority's use of blockchain forensics for AML/CFT purposes and Nigeria's SEC partnership with Chainalysis to enhance crypto fraud detection. Notably, the FATF has observed a shift of illicit actors towards stablecoins, such as USDT on Tron, for obfuscation and money laundering.

FIGURE 84.

Prioritisation of SupTech Use Cases Under Digital Assets And Cryptocurrencies Oversight



Suptech is also emerging as a key tool for market and protocol monitoring. AI-driven market surveillance leverages machine learning to detect manipulation, such as pump-and-dump schemes, while smart contract auditing tools support DeFi monitoring by identifying vulnerabilities and ensuring compliance with AML and KYC requirements. Meanwhile, Project Pine, by the BIS Innovation Hub Swiss Centre and New York Fed's New York Innovation Center, has shown that central banks can conduct monetary policy in a tokenised environment by prototyping a flexible, cross-jurisdictional toolkit capable of supporting both standard and emergency operations.

Despite progress, several critical areas show low suptech maturity, including automated oversight tools: stablecoin reserve verification (around 15%), algorithmic asset monitoring (15%), automated compliance checks for virtual asset providers (20%), and automated validation of crypto-related data (21%). These gaps highlight the need for authorities to translate policy intent into operational capability. For instance, the Malta Financial Services Authority has identified multiple compliance shortcomings among crypto-asset service providers under MiCAR requirements.

Overall, digital-asset suptech is progressing but remains at an early stage. Supervisory efforts are strongest where data is structured and investigative workflows are well established; more complex, automation-intensive oversight functions lag significantly. As regulatory frameworks mature and cross-border collaboration deepens, bridging this operational gap will become essential to ensure effective, technology-enabled oversight of a rapidly evolving market.

3.10 Financial inclusion, financial health and gender monitoring

Financial-inclusion, financial health, and gender-equity measurement and supervision rely on timely, disaggregated datasets that capture usage, behaviour, vulnerability, and resilience across population groups, yet persistent disparities — across gender, geography, income, age, disability, and MSME segments — remain difficult to monitor due to fragmented reporting systems and limited analytical capacity. Surveys show that only 26% of authorities are developing or deploying inclusion-related suptech, and only 9% operate fully implemented tools.

Current uptake is concentrated in basic indicators, while advanced capabilities remain at early stages. Structural constraints, including fragmented data infrastructures, limited sex-disaggregated reporting, and weak analytical capacity, continue to impede progress. More advanced use cases – such as gender-impact analytics, geospatial mapping, and over-indebtedness risk detection – show minimal maturity. As inclusion policy shifts toward quality, resilience, and financial health rather than access alone, supervisors will require more robust digital capabilities to analyse behavioural patterns, detect disparities, and inform proportionate interventions.

Financial-inclusion and gender-equity supervision depends on timely, disaggregated datasets that capture usage, behaviour, vulnerability, and resilience patterns across population groups, yet most authorities lack the data infrastructures and taxonomies required for systematic analysis.

Financial inclusion and equity monitoring is an emerging but comparatively underdeveloped suptech domain. Global progress in account ownership – now at [79% of adults](), up from 74% in 2021 according to the World Bank Global Findex – masks persistent disparities across gender, geography, income, age, disability, and other demographic groups. Supervisors increasingly recognise the need for more granular, disaggregated monitoring, yet few have the data systems, supervisory frameworks, or gender-responsive strategies required to analyse outcomes beyond basic access metrics. As noted in Section 2.2, 71% of authorities lack a gender strategy, illustrating the institutional gap between policy intent and operational capability.

Global policy thinking has moved decisively towards financial health as a core dimension of inclusive finance. The UN Secretary-General's Special Advocate, Queen Máxima, has emphasised the importance of assessing whether people can meet daily expenses, absorb shocks, build resilience, and plan for the future. This shift requires supervisory approaches capable of analysing behaviour, vulnerability, resilience, and systemic fairness — domains where suptech can play a critical enabling role.

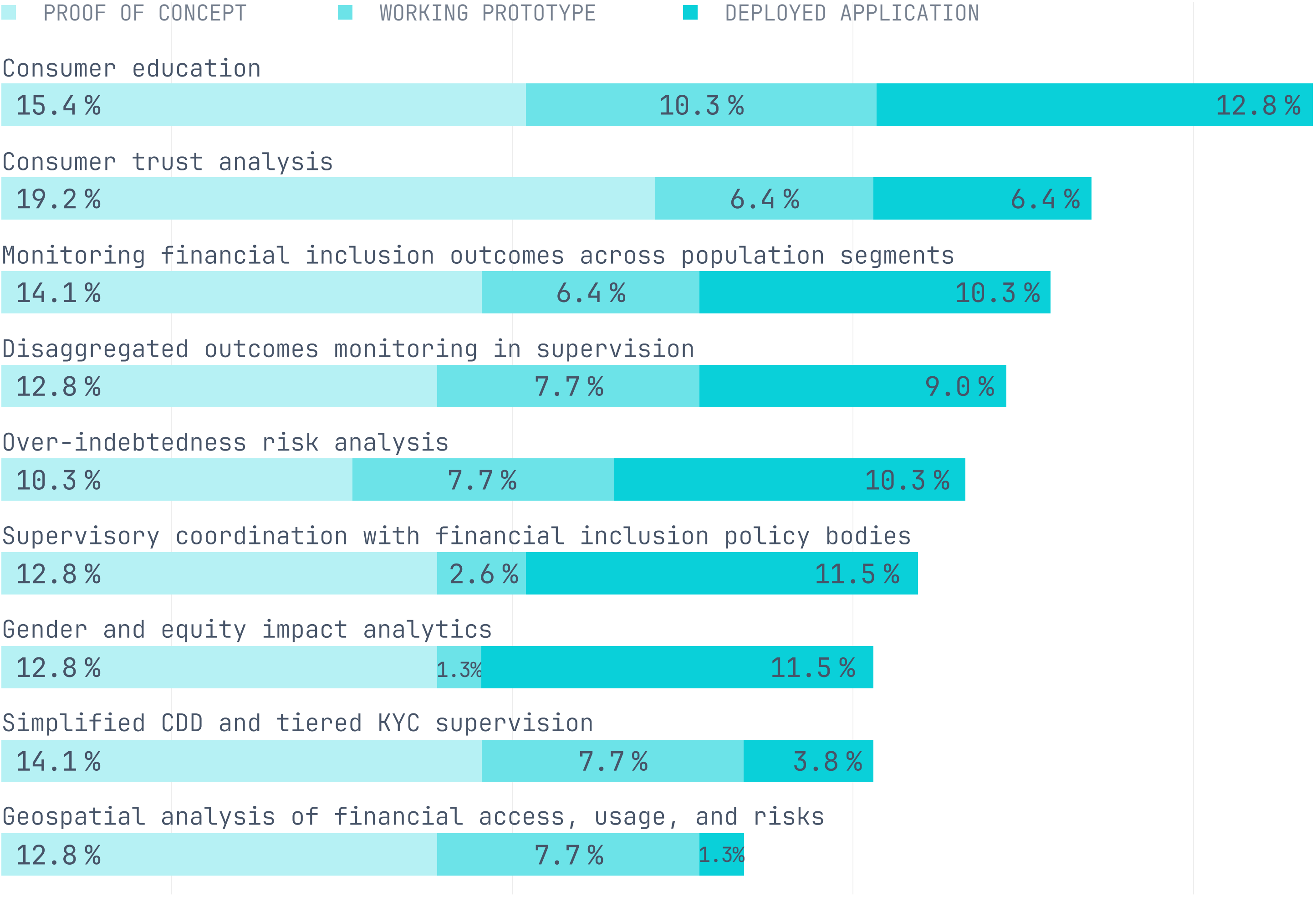
A number of financial authorities have begun to incorporate financial-health-aligned indicators into regulatory monitoring. The Bangko Sentral ng Pilipinas (BSP) publishes a Financial Inclusion Dashboard that includes indicators on usage depth, resilience, and behavioural patterns; these form part of its broader Data Framework for Financial Inclusion. The Banco Central do

Brazil has taken a leading role by launching the Indicador de Saúde Financeira do Brasileiro (ISFB) in 2023, the first nationwide financial-health indicator developed by a central bank. The measure provides structured insights into resilience, behaviour, and financial stress, and offers a concrete example of how financial-health monitoring can be embedded into supervisory practice. A notable example that demonstrates how suptech can directly support inclusion outcomes comes from the National Bank of Rwanda (NBR). NBR operates a Financial Inclusion Dashboard that draws regular data from banks, MFIs, SACCOs, insurers and mobile-money providers, producing weekly indicators on account ownership, savings, credit, insurance and service-point distribution. All metrics are disaggregated by gender, age, location, and institution type, enabling the central bank and ecosystem partners to identify underserved populations and track progress in near real time.

Despite such progress, suptech adoption in this domain remains limited. Only 26% of authorities report deploying or developing inclusion-related applications and just 9% have fully operational systems (Figure 71). Interest exceeds implementation capacity: 35% express demand but lack concrete plans, while POCs (10%) and prototypes (7%) remain modest. Engagement is significantly higher among EMDEs (33%) than AEs (7%) (Figure 74), reflecting stronger national mandates for inclusion and greater reliance on digital channels in service delivery.

FIGURE 85.

Prioritisation of SupTech Use Cases Under Financial Inclusion And Financial Health Monitoring

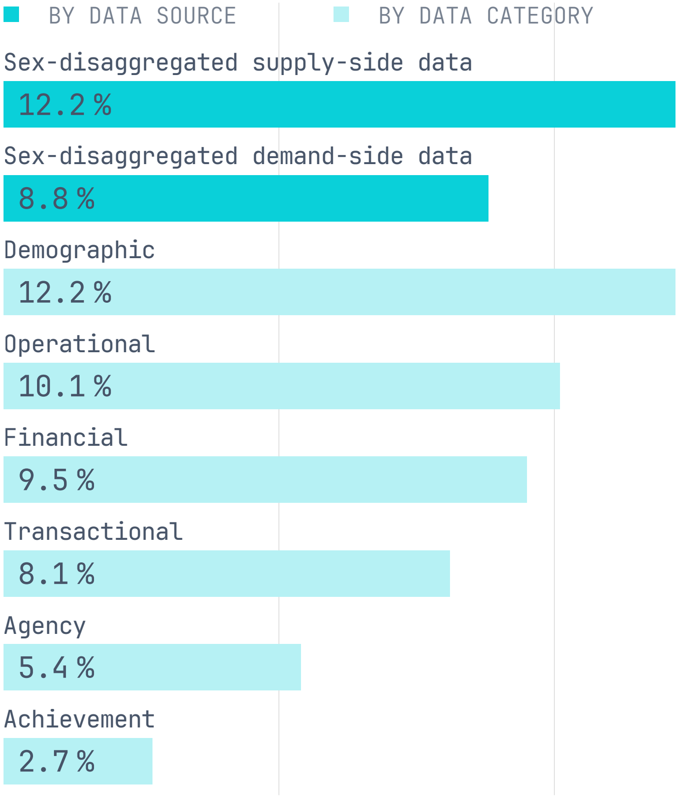


Adoption varies widely across use cases (Figure 85). Consumer education tracking shows the highest maturity at 39%, reflecting its prominent role in most national financial inclusion strategies. Consumer trust analytics reaches 32%, drawing on sentiment, complaints, and interaction data. Monitoring of financial-inclusion outcomes across population segments reaches 31%, enabling disaggregated analysis by gender, geography, age, income and MSME size. Authorities use these insights to map disparities and target proportionate interventions. Disaggregated outcomes monitoring reaches 30%, supporting integration of sex-, age-, and region-disaggregated metrics into supervisory risk models. Over-indebtedness risk analysis achieves 28%, helping detect harmful credit patterns among vulnerable groups. Coordination between supervisors and national financial inclusion policy bodies stands at 27%, while gender and equity impact analytics remain comparatively limited at 26%, with only 12% of authorities reporting fully deployed solutions.

More advanced applications still show minimal maturity. Simplified CDD and tiered-KYC supervision reaches 26%, despite its importance for balancing inclusion and AML/CFT safeguards. Geospatial mapping of financial access, usage, and risks is the least developed at 22%, even though it provides critical insights into agent networks, infrastructure gaps and regional disparities.

FIGURE 86.

Types And Categories Of Sex-Disaggregated Data Collected By Agencies

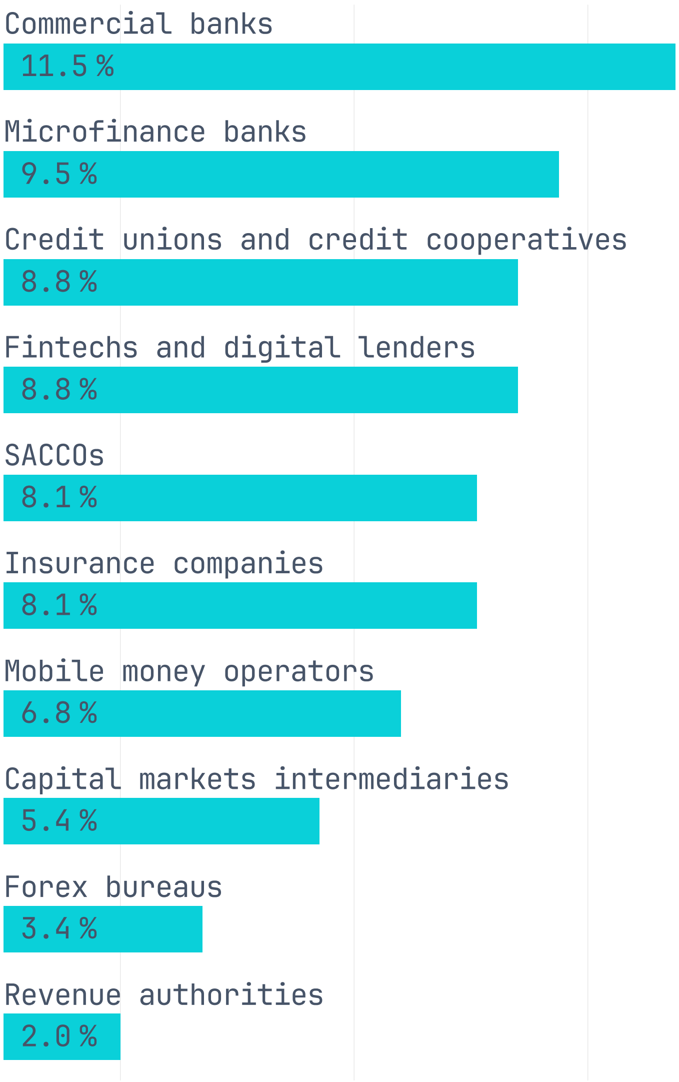


The rising importance of financial health provides a coherent anchor for future development of suptech in this domain. Financial-health monitoring requires timely, disaggregated data, behavioural analytics, and integrated supervisory dashboards – capabilities that suptech can enable. Yet the gap between ambition and operational capacity remains wide: fragmented data infrastructures, lack of standardised taxonomies, limited gender strategies, and insufficient analytical skills continue to constrain progress. As financial inclusion policy shifts toward quality and outcomes rather than access alone, supervisors will increasingly require digital tools capable of analysing behavioural patterns, resilience, and fairness at scale.

A central barrier to progress is the limited collection and use of sex-disaggregated data, which remains foundational for gender-responsive supervision. Only 12% of surveyed authorities collects such data from the industry, complemented by demand-side data from inclusion surveys (9%) (Figure 86). Most collection focuses on basic demographic attributes (12%), with narrower coverage of operational data (10%), financial data (10%), transactions (8%), institution-specific attributes (5%), or performance mvetrics (3%). This narrow scope constrains the ability of supervisors to detect disparities in usage, risk, pricing, misconduct exposure, or digital-channel behaviours.

FIGURE 87.

Producers Of Sex-Disaggregated Data Collected By Agencies



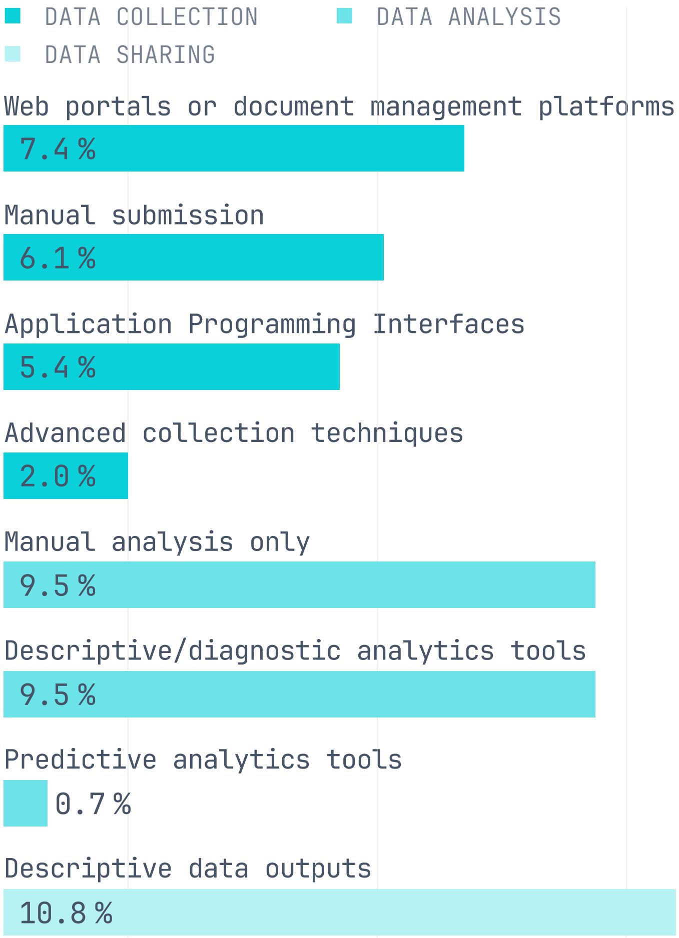
The producers of sex-disaggregated data are similarly concentrated. Commercial banks constitute the primary source (12%), followed by microfinance banks (10%), credit unions and cooperatives (9%), fintech lenders (9%), SACCOs (8%), insurers (8%) and mobile-money operators (7%) (Figure 87). Capital markets intermediaries, forex bureaux and revenue authorities contribute far less frequently. A few jurisdictions report innovative approaches using national ID systems to merge financial registries with civil registries, reducing compliance burdens and improving data quality through automated disaggregation.

Data infrastructure for collection, analysis and sharing remains weak. Web portals and document-management platforms dominate (7%), followed by manual submission (6%) and APIs (5%), while more advanced tools appear in only 2% of cases (Figure 88). Analytical sophistication is similarly limited: 10% rely on manual analysis and another 10% use descriptive or diagnostic analytics. Predictive analytics is virtually absent (<1%), representing a missed opportunity to anticipate emerging disparities or analyse financial-health trends. Dissemination largely consists of descriptive outputs (11%), with minimal evidence of data-sharing mechanisms that could support market transparency or public-sector collaboration.

Authorities that do collect sex-disaggregated data use it primarily to identify gaps in access,

FIGURE 88.

How Agencies Collect, Analyse, And Share Sex-Disaggregated Data

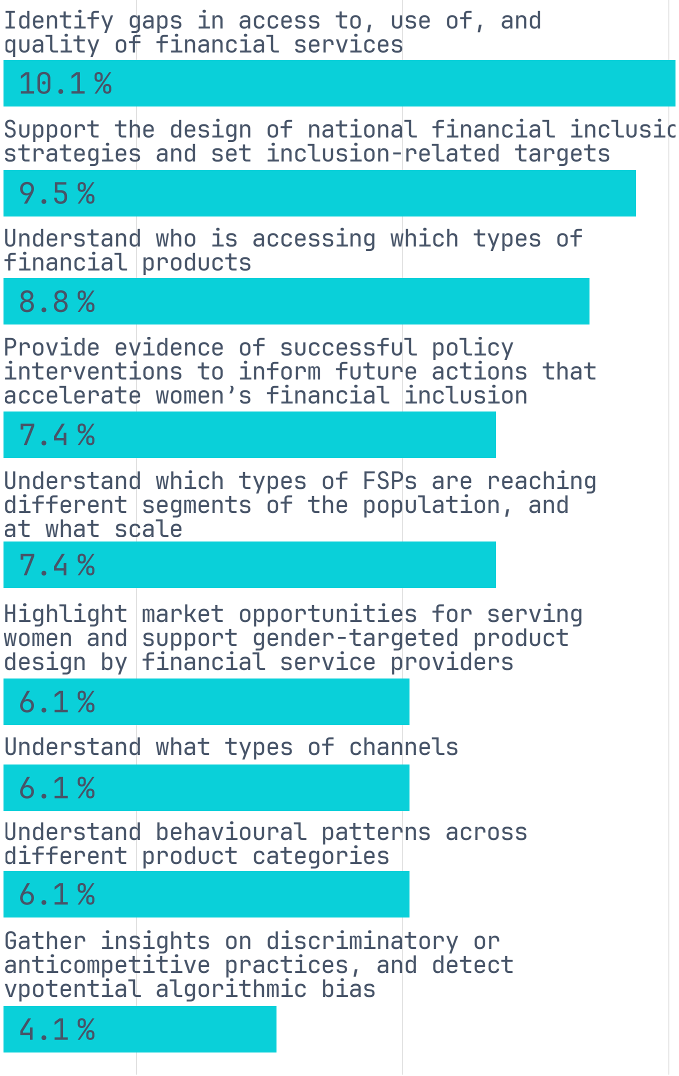


usage and service quality (10%) and to inform inclusion strategies and performance targets (10%) (Figure 89). Additional uses include mapping provider reach, understanding product uptake patterns, evaluating policy impacts on women and underserved segments, and identifying potential market opportunities. Less common applications include assessing behavioural preferences, detecting discriminatory practices, or analysing algorithmic bias—areas that are growing in importance as digital financial services expand. The Nigerian Women's Financial Inclusion Dashboard provides gender-disaggregated usage data for deposits, credit, payments and savings, supporting agencies and financial institutions in designing gender-sensitive interventions and monitoring access gaps.

Challenges remain significant. Internal obstacles include poor data quality, limited coordination with other government entities, low organisational awareness, inadequate technical systems, weak prioritisation by supervised entities, and restricted internal use. External constraints include high compliance costs, resource-intensive data management requirements, privacy concerns, fragmented reporting, and legal barriers that prevent compulsory or shared disaggregated reporting (Figure 90). In some jurisdictions, the absence of national ID systems prevents accurate disaggregation, illustrating the link between DPI readiness and inclusion-oriented supervision.

FIGURE 89.

Applications Of Sex-Disaggregated Data In Agencies



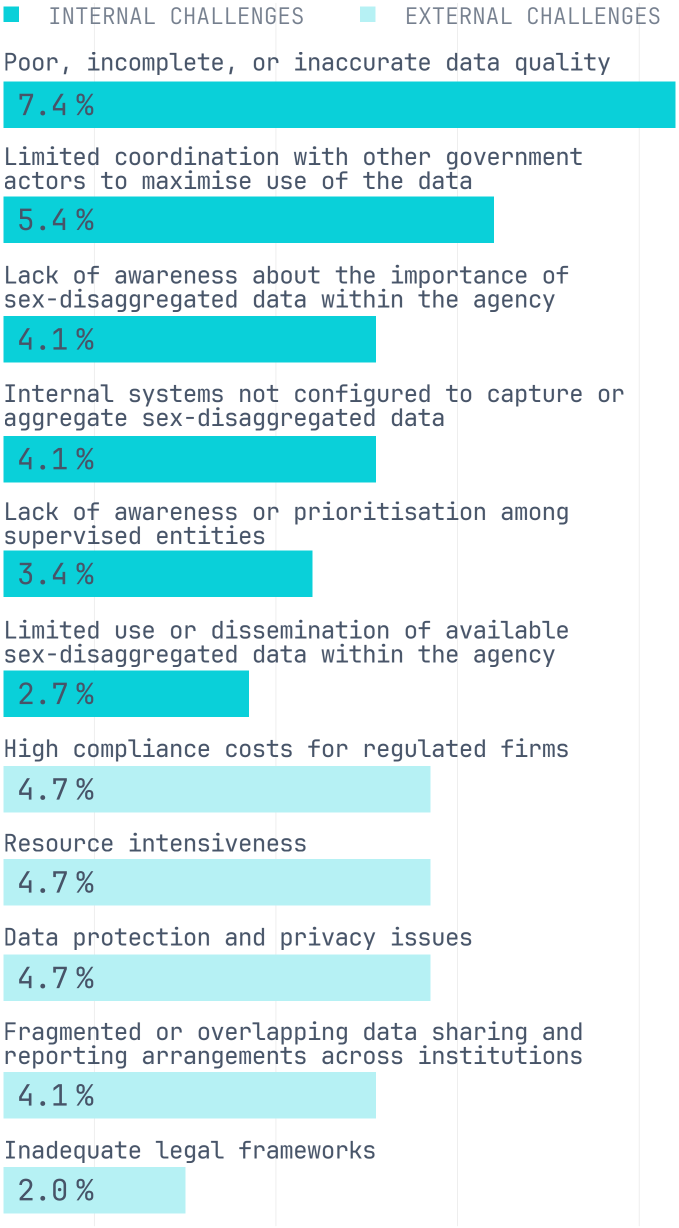
Overall, financial inclusion and gender monitoring continues to lag despite widespread policy interest, modest suptech uptake and persistent data challenges. Closing these gaps requires coordinated investment in data infrastructure, strengthened capacity for advanced analytics, clearer supervisory mandates for gender equality, and closer alignment between supervision and national inclusion strategies. As financial health becomes a central organising principle for inclusion policy, supervisors will need digital tools capable of analysing resilience, behaviour and fairness across diverse population groups, ensuring that progress extends beyond broad access metrics to equitable and sustainable financial outcomes.

3.11 Insurance supervision

Suptech adoption in insurance supervision is moderate, with about one-third of authorities deploying or developing tools. Core functions such as data ingestion and validation are the most advanced, while more sophisticated capabilities like real-time supervision and claims analytics remain limited.

FIGURE 90.

Challenges In Collecting And Using Sex-Disaggregated Data



Insurance supervision depends heavily on granular reporting, product-filing datasets, and claim-performance indicators, and suptech adoption is concentrated in automating data ingestion, validation, and entity-level profiling.

Suptech adoption in insurance supervision is moderate, with 33% of authorities deploying or developing solutions (Figure 77). 15% report fully deployed applications, higher than in newer areas such as digital assets or climate and ESG risks, but below traditional domains like prudential supervision and AML/CFT/CPF. Only 9% are testing POCs and 10% have prototypes, indicating modest experimentation. 18% of authorities express demand without concrete plans. Authorities in AEs (41%) exhibit more active engagement compared to those in EMDEs (30%) (Figure74).

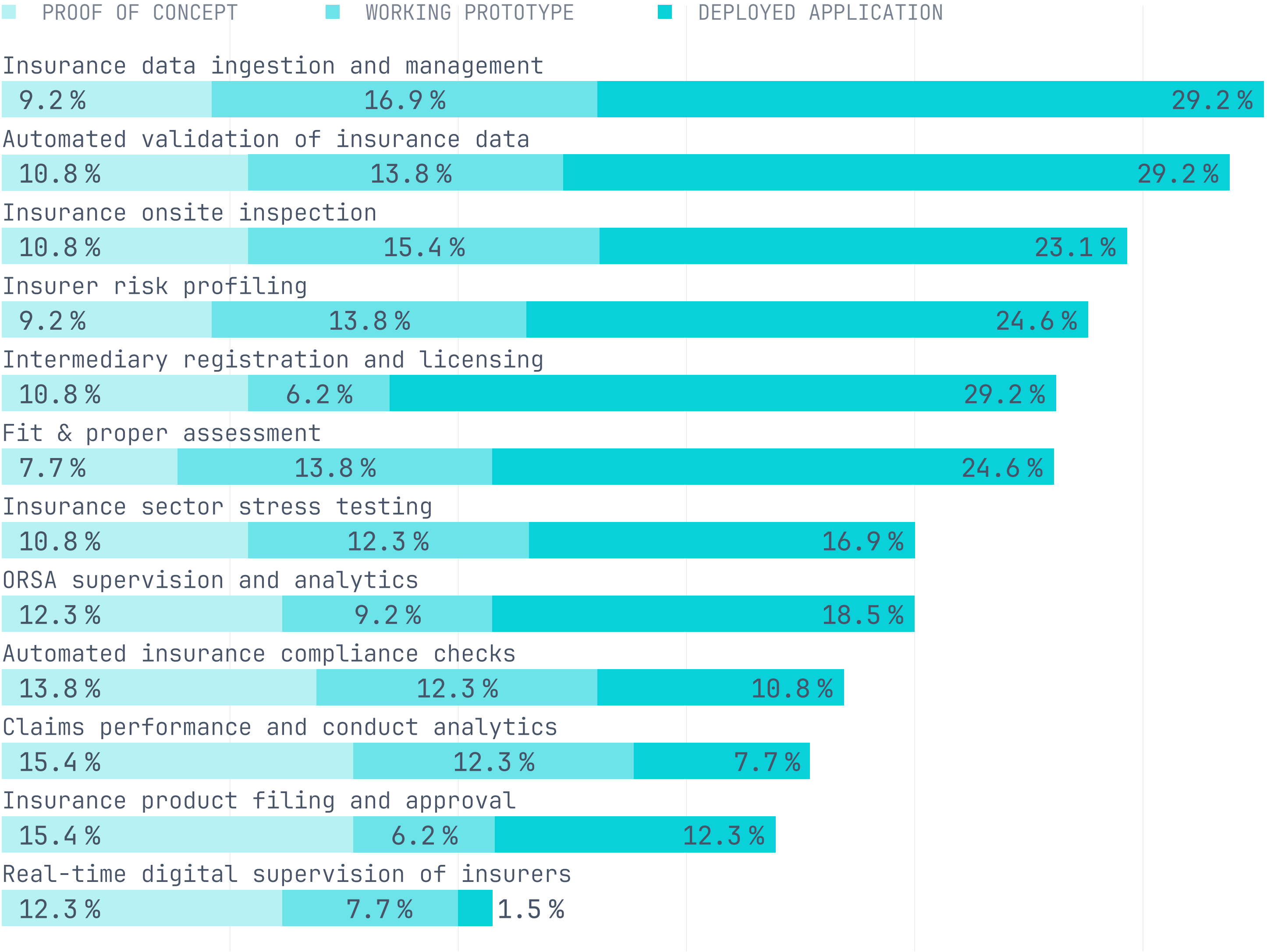
Use-case maturity varies widely. Foundational reporting and validation functions are the most advanced: data ingestion and management reaches 55% maturity, and automated validation 54%, reflecting the centrality of reliable regulatory reporting (Figure 91). Core supervisory processes also show moderate development: onsite inspection (49%), insurer risk profiling (48%), intermediary licensing (46%), and fit-and-proper assessments (46%) increasingly rely on digital workflows and automated checks.

More specialised analytics remain less developed. Stress-testing and ORSA analytics each reach 40% maturity, while automated compliance checks (37%) and claims-performance and conduct analytics (35%) show early but growing adoption. The least mature areas are those requiring continuous data or advanced analytical techniques: product-filing and approval processes remain at 34% maturity, and real-time digital supervision is nascent at 22%, with only 2% deployment.

Several authorities are piloting more innovative approaches. France's ACPR has developed "Veridic," an AI tool that extracts and classifies life-insurance product features from key information documents, enabling market-wide assessment of product complexity and supporting risk-based, proportionate supervision. Mozambique's insurance supervisor ISSM launched an upgraded digital platform in 2025 to standardise sector-wide data collection and reporting, strengthening the infrastructure needed for broader suptech adoption. The IAIS also relaunched its Insurance Core Principles Self-Assessment Tool in 2025, which, while

FIGURE 91.

Prioritisation of SupTech Use Cases Under Insurance Supervision



not a suptech application, helps supervisors benchmark their frameworks and identify priorities for future technological modernisation.

As insurance risks evolve — including climate-related exposures, conduct risks, and operational dependencies — supervisors will increasingly require predictive analytics, climate stress-testing tools, claims-behaviour analytics, and AI-enabled product-classification systems. Advancing these capabilities will depend on stronger data foundations, more sophisticated analytical tooling, and continued international cooperation.

3.12 Licensing and authorisation

Licensing and authorisation has become one of the most active areas of suptech adoption as authorities modernise entry and oversight processes for an increasingly diverse financial sector. Digital workflows, structured data collection, and automated assessments now underpin many application pipelines, reducing procedural bottlenecks and improving supervisory consistency. Survey results show that licensing has experienced the fastest growth in adoption since 2022, with foundational digitalisation widely deployed and more advanced capabilities moving through early development. These trends reflect the shift from manual, document-based review toward more standardised, data-driven, and proportionate licensing frameworks that support efficient market access and strengthen supervisory control.

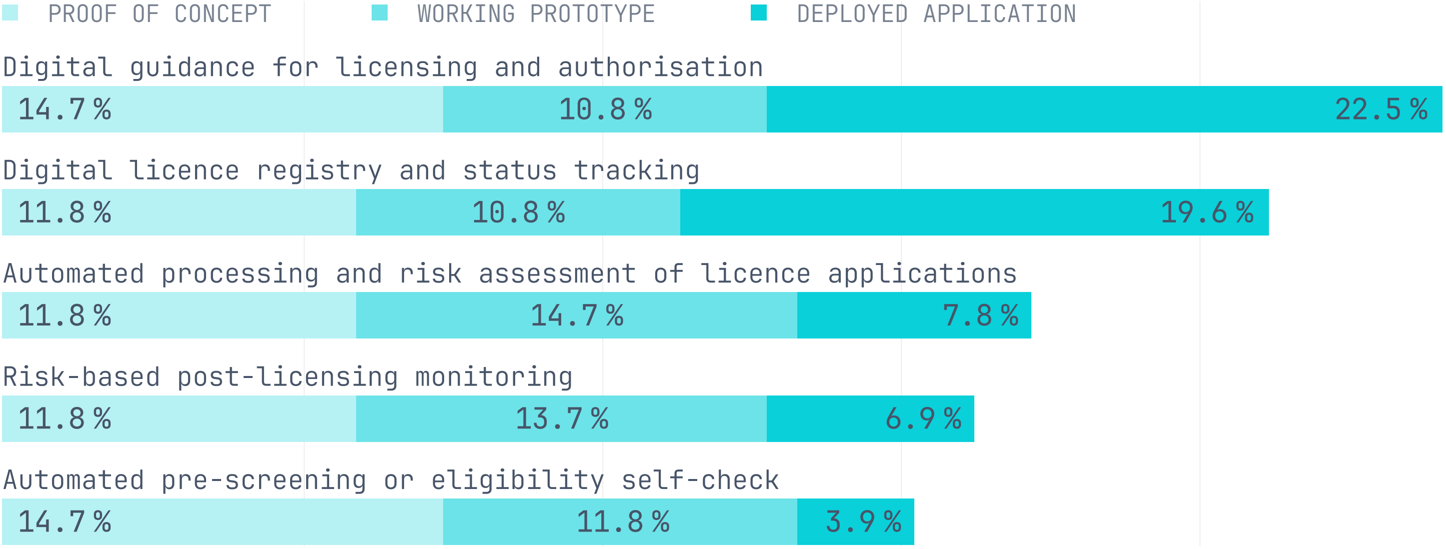
Licensing and authorisation systems are increasingly shaped by the need to evaluate more diverse, data-intensive, and digitally native applicants, making this one of the most rapidly evolving areas of suptech adoption. Supervisory authorities are replacing manual, document-heavy workflows with structured data pipelines, automated assessments, and AI-assisted analysis, enabling more consistent decision-making and stronger risk-based oversight. These capabilities are now central to managing the growing volume and complexity of applications from fintechs, digital banks, VASPs, and cross-border firms.

Suptech adoption in licensing has expanded markedly, rising from 19% of surveyed authorities in 2022 to 49% in 2024 and reaching 52% in 2025 (Figure 73). Deployment now stands at 23%, with an additional 29% in development stages (12% POCs and 17% working prototypes). Demand remains strong: 28% of authorities express interest in adopting solutions but have not yet planned implementation (Figure 71). EMDEs report slightly higher overall activity (53%) than advanced economies (48%) (Figure 74), reflecting both reform momentum and opportunities to modernise legacy processes.

Adoption is strongest for foundational digitalisation of licensing workflows. Digital licensing guidance leads with 23% deployment, followed by licence registries and application-status tracking at 20% (Figure 92). These tools standardise submissions, reduce procedural bottlenecks, and improve transparency for applicants. More advanced capabilities show steady progress: automated processing and risk assessment of licence applications (8% deployed; 27% in development) and risk-based post-licensing monitoring (7% deployed; 26% in development) indicate a gradual shift toward data-driven supervision. Automated pre-screening remains nascent (4% deployed) but has significant development momentum (27%), illustrating growing interest in front-end triage to reduce manual review workload.

FIGURE 92.

Prioritisation of SupTech Use Cases Under Licensing



Several authorities are testing or deploying more sophisticated approaches. Mozambique's ISSM expended its web-based Bank Supervision Application to include online licensing. Saudi Arabia's SAMA developed a Fintech Application Assessment tool that automates end-to-end analysis of sandbox submissions. Australia's ASIC launched an upgraded licensing portal with pre-filled forms, elimination of duplicate documentation, and granular classification of financial services. ADGM has piloted AI-enabled capabilities, including its RiskAnalyser pilot for assessing application completeness and a GenAI due-diligence tool developed with NUS AIDF that tailors onboarding documentation for Web3 projects. The ECB's IMAS portal provides a mature example of fully integrated licensing infrastructure, allowing institutions to submit applications, track progress, and respond to supervisory queries through structured online workflows.

Emerging capabilities — including AI-driven profiling to generate risk score, using machine learning to generate applicant risk scores, automated compliance checks linked to AML/KYC registries, and GenAI document analysis — reflect a shift from digitising existing processes toward intelligent, risk-based automation. This convergence of regulatory need and technological maturity positions licensing and authorisation at the forefront of suptech transformation, supporting more efficient market entry processes while enhancing proportionality and supervisory effectiveness.

3.13 Open banking and open finance supervision

Open banking and open finance are reshaping supervisory perimeters by enabling high-frequency data mobility across institutions, sectors, and technology intermediaries. These frameworks introduce new supervisory risks around API performance, data-sharing fairness, consent governance, and the emergence of powerful data-aggregator roles, yet suptech capabilities remain nascent: only 3% of authorities have deployed relevant tools, and 15% are piloting early solutions. The result is a widening gap between market innovation and supervisory readiness. Closing this gap will require stronger governance, clearer technical standards (including ISO 20022 alignment), and targeted suptech investment capable of monitoring real-time API ecosystems, enforcing data-usage rules, and ensuring safe, fair, and interoperable data mobility as open finance scales.

Open finance ecosystems are accelerating high-frequency, bidirectional data flows across banks, non-bank financial institutions, data aggregators, and third-party providers. This significantly expands the supervisory perimeter and introduces new oversight requirements around API performance, payload standardisation, consent-lifecycle governance, and operational resilience. As these data-sharing infrastructures increasingly converge with real-time account-to-account payment systems – such as Brazil's Pix, India's UPI, and Europe's SCT Inst – supervisors must monitor interconnected risks across payment execution, identity and consent artefacts, and shared API gateways. In parallel, the sector-wide adoption of ISO 20022 introduces structured message fields and harmonised semantics that offer new supervisory opportunities for automated validation, anomaly detection, and cross-system interoperability. Authorities such as the ECB, the BOE (CHAPS) and the Federal Reserve (Fedwire) have already migrated. Figure 43 shows that 14% of respondents have implemented or are planning to implement standardised data interoperability frameworks such as ISO 20022.

Open banking first created secure, standardised mechanisms for permissioned data access by third-party providers via APIs.

Open finance extends this infrastructure to a wider set of financial products – including credit, investments, pensions, and insurance – substantially increasing the volume, diversity, and sensitivity of data exchanged across regulated and non-regulated actors. As of 2024, around 70 jurisdictions have engaged in the development of open-banking or open-finance regulatory frameworks, using a mix of data-rights legislation, sectoral rule-making, and industry-led standards. This rapid proliferation expands the scope of supervisory oversight and increases the need for consistent approaches to accountability, technical standards, and governance.

This expansion introduces material supervisory risks, including uneven technical standards, fragmented data-sharing obligations, opaque consent-management practices, and increased exposure to privacy and cyber breaches. These issues are highlighted by the OECD and in BIS, both of which underscore the supervisory implications of divergent governance models and inconsistent implementation of technical standards.

Recent market events illustrate these risks. The Australian Office of the Australian Information Commissioner (OAIC) has issued determinations regarding invalid or overly broad consumer-consent practices under the Consumer Data Right. In the United States, enforcement actions by the Consumer Financial Protection Bureau (including the Plaid settlement) highlighted concerns around "dark consent patterns," opaque data-use notices, and challenges in monitoring consent withdrawal. In the United Kingdom, the FCA has also raised concerns about insufficient auditability of consent-revocation flows in several Account Information Service Providers. These cases demonstrate why consent governance has become a core supervisory focus as open-finance ecosystems scale.

Against this backdrop, the 2025 State of SupTech Survey shows that open-banking and open-finance supervision remains one of the least developed application areas (Figure 71). Only 3% of authorities report deployed tools, with 15% in active development (10% proofs of concept; 5% prototypes). A further 32% express demand without a concrete implementation pathway, indicating conceptual awareness but low operational readiness.

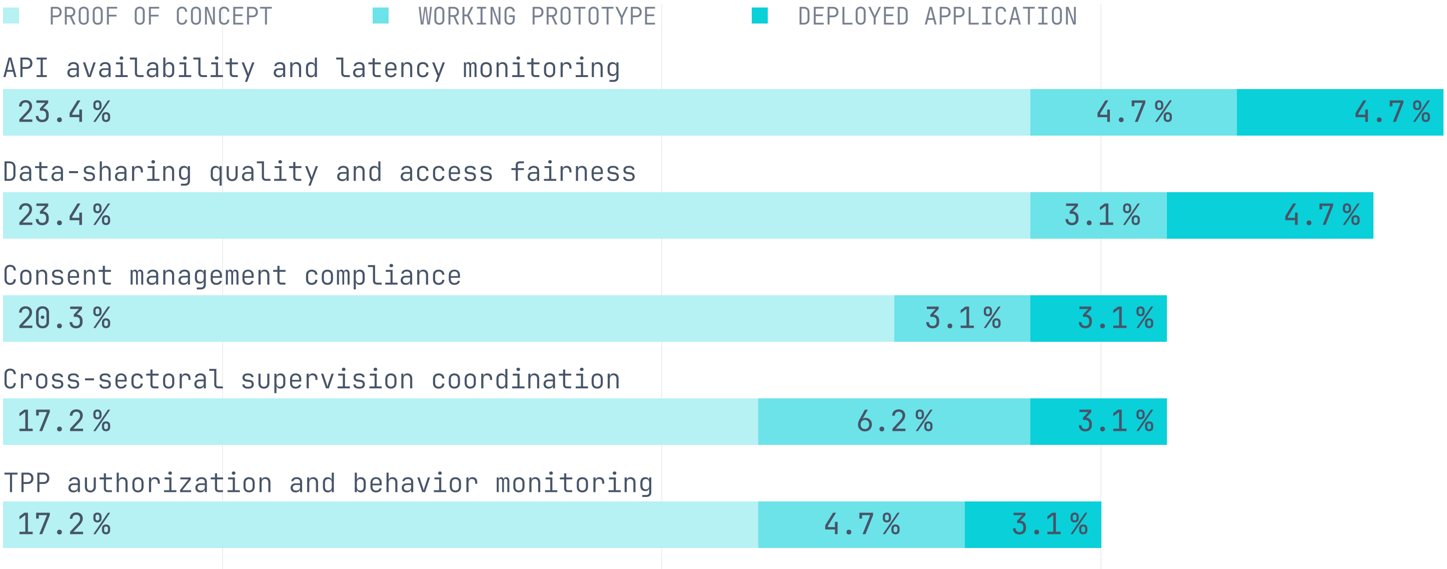
Use-case maturity remains limited (Figure 93). API availability and latency monitoring – the most technically straightforward oversight function – reaches only 5% deployment and 28% combined development. Data-sharing quality and access-fairness monitoring exhibit similar patterns (27%), while more complex supervisory activities such as consent-management auditing, cross-sectoral supervision coordination, and authorisation and behaviour monitoring for third-party providers remain at only 3% deployment. These findings point to a substantial gap between the pace of market innovation and supervisory capacity to monitor the full open-finance ecosystem.

The United Kingdom continues to be the most advanced case. In 2024–2025, the FCA accelerated open-finance infrastructure development through the Smart Data Accelerator and two open-finance TechSprints, building on recommendations from the Joint Regulatory Oversight Committee. The establishment of the "Future Entity" – an industry-led body with regulatory oversight to develop next-generation technical and governance standards – represents a substantive institutional development toward structured supervision of complex data-sharing ecosystems.

Global innovation programmes reflect similar momentum. The BIS Innovation Hub's Project Aperta – involving the UAE, Hong Kong, Brazil, and the UK – is developing a privacy-preserving data-sharing architecture using PETs and

FIGURE 93.

Prioritisation of SupTech Use Cases Under Open Banking And Open Finance Supervision



advanced consent-management tooling. The 2025 G20 TechSprint prioritised credit-data portability and verification use cases, demonstrating expanding international interest in secure, standards-based open-finance frameworks.

Financial authorities such as Phillipines' BSP, and the State Bank of Pakistan (SBP) are using regulatory sandboxes and hackathons to co-develop proportionate approaches to open-finance oversight and support national roadmaps.

This aligns with findings from the American Bankers Association (ABA), which notes that fragmented APIs, opacity in the data-sharing chain, and intermediary concentration create new supervisory risks and necessitate stronger monitoring tools.

Despite this policy momentum, supervisory capacity still lags behind market innovation. Fragmented standards, limited access to API performance data, immature consent-auditing tooling, and the difficulty of supervising non-regulated intermediaries restrict the ability of authorities to ensure fair, safe, and accountable data sharing. Without the rapid strengthening of governance frameworks, alignment of technical standards, and investment in suptech, open-finance data-mobility frameworks risk reinforcing market-power imbalances, exposing consumers to inappropriate data use, and undermining trust in digital financial ecosystems.

3.14 Operational risks supervision

Operational risk supervision remains a central component of financial oversight, with a combined suptech adoption rate of 47%, reflecting a mix of deployed applications, proofs of concept, and working prototypes. Interest is high across jurisdictions, but significant capability gaps persist, particularly in third-party risk analytics and staff-conduct monitoring. The growing scale and complexity of operational dependencies – including ICT infrastructure, cloud service providers, and outsourced processes – underscore the need for more systematic, real-time supervisory tools.

Operational-risk supervision requires structured, high-frequency incident, ICT, and third-party dependency data, and suptech adoption reflects authorities' need to systematise incident ingestion, map concentration exposures, and benchmark operational resilience across institutions. Mandates for operational-risk oversight differ across jurisdictions, particularly regarding third-party and ICT-risk supervision, which influences the scope and maturity of digital tools adopted.

Operational risk has strengthened its prominence as digitalisation, cyber incidents, and geopolitical tensions increasingly expose financial institutions to non-financial shocks. Supervisory frameworks are expanding to address these evolving risks, with many authorities shifting from retrospective loss-data monitoring toward proactive assessments of operational resilience, ICT risk, and concentration risk associated with critical third parties. Financial authorities are also adopting broader incident-reporting expectations and structured data-collection regimes, recognising that operational disruptions can now pose systemic rather than institution-specific consequences. Growing alignment with ISO 20022 and other structured messaging standards also affects operational-risk supervision, as richer message fields and harmonised identifiers make incident reporting, loss-event classification, and third-party dependency mapping more automatable across institutions.

Recent policy developments illustrate this shift toward forward-looking resilience supervision. The EU's Digital Operational Resilience Act (DORA) introduces detailed expectations for ICT governance, testing, incident reporting, and oversight of critical third-party providers. In the United Kingdom, the Bank of England's 2024 consultation outlines a future regime requiring financial market infrastructures to submit structured operational-incident reports through the FCA's Connect portal and detailed disclosures of material third-party arrangements via RegData no earlier than 2026. The BOE has also begun exploring stress-testing approaches that model severe cyber and operational disruptions to assess potential impacts on financial stability. International standard-setting bodies – including the BCBS, IOSCO, and CPMI-IOSCO – continue to provide principles for outsourcing, third-party risk management, and operational resilience, reinforcing the move toward more harmonised global expectations.

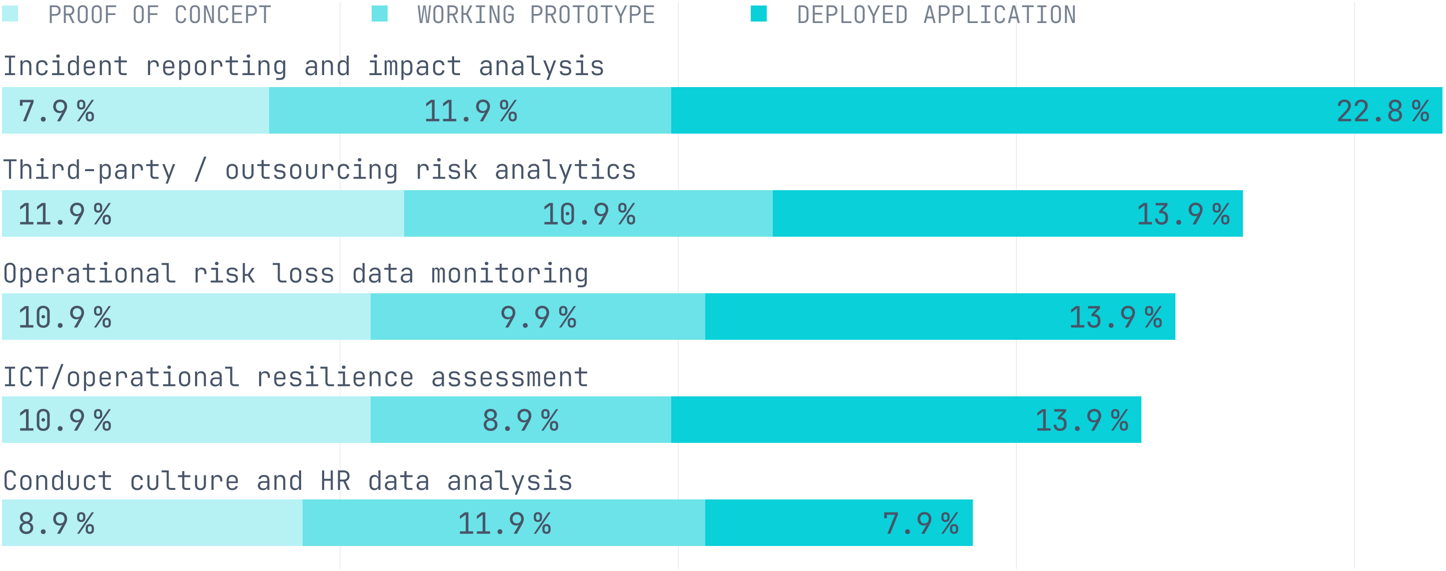
Suptech adoption patterns reflect this policy trajectory. Operational risk supervision ranks fifth globally among all supervisory domains. Although 47% of authorities have deployed or are developing tools, 30% remain in the "desired but not planned" category, suggesting that conceptual awareness outpaces operational capacity. Resource constraints, emerging mandates, and the technical complexity of resilience assessment all contribute to this implementation lag.

Use-case maturity is concentrated in core incident-data collection and analysis, which forms the backbone of operational-risk assessment. Incident reporting and impact analysis is the most advanced use case at 43% combined maturity, enabling supervisors to ingest structured reports on outages, cyber events, fraud, or operational disruptions, assess causes, and monitor recurrence patterns.

Other use cases show moderate but closely aligned development. Third-party and outsourcing risk analytics (37%) is gaining traction as authorities seek to map concentration exposures – particularly to cloud and ICT providers – and evaluate compliance with DORA-style frameworks. Operational risk loss-data monitoring (35%) and ICT/operational resilience assessment (34%) also show meaningful development, supporting supervisors in benchmarking firms' loss events, internal control deficiencies, and adherence to ICT-risk expectations.

FIGURE 94.

Prioritisation of SupTech Use Cases Under Operational Risks Supervision



By contrast, forward-looking and behavioural elements of operational risk are underdeveloped. Conduct-culture and HR-data analytics display the lowest maturity at 29%. This area involves analysing metrics such as staff turnover, whistleblower activity, or conduct-risk indicators to identify internal vulnerabilities that may contribute to broader operational failures. Adoption is limited, reflecting the complexity of combining qualitative datasets with quantitative analytics and the sensitivity of HR-related supervisory interventions.

Overall, operational-risk suptech is advancing but continues to centre on foundational data-collection processes rather than predictive analytics or systemic-risk mapping. As digital ecosystems expand and institutions become more reliant on critical service providers, supervisory demand is likely to shift toward more integrated, real-time monitoring capabilities capable of supporting forward-looking resilience assessments.

3.15 Payments

Payments oversight is increasingly shaped by real-time data flows, interoperability requirements, and the rapid expansion of instant and cross-border connectivity. As payment infrastructures modernise, supervisory attention is shifting toward system performance, fraud detection, liquidity and settlement risk, and the integrity of data flowing through high-value and retail payment systems. The global migration to ISO 20022 represents a structural shift in supervisory data, enabling richer, standardised transaction fields that support automated monitoring, anomaly detection, and more granular systemic-risk analysis.

Global payments modernisation continued in 2025, driven by instant-payment expansion, strengthened cross-border connectivity, and early experimentation with tokenised settlement assets. Central banks are responding to the G20 roadmap for enhancing cross-border payments, deepening collaboration on data quality, messaging standards, and operational resilience. The Financial Stability Board's new workstream on payments data and CPMI's accelerated ISO 20022 (see Introduction and Section 3.13) harmonisation agenda underscore the sector's shift toward structured, interoperable data as a prerequisite for supervisory insight.

Retail fraud remains a defining risk. The EBA's Consumer Trends Reports identify payment fraud — particularly APP fraud, social-engineering attacks, and digital impersonation — as one of the most significant risks for EU consumers. Authorities worldwide are reinforcing fraud-response frameworks and building real-time analytics capabilities for fast retail payment systems.

Central banks also expanded efforts on digital-money experimentation. CBDC research remains widespread though live deployments are limited, while tokenisation initiatives such as BIS Project Meridian, Mandala, and Rialto are testing cross-border settlement models with direct supervisory implications. Regional schemes including Pan-African Payment and Settlement System (PAPSS) and Asian payment-connectivity initiatives advanced real-time settlement and QR-interoperability frameworks. Oversight developments included the Bank of Canada's implementation of the Retail Payments Activities Act, the UK's review of payments regulatory consolidation, and strengthened EU rules on fraud, cyber resilience, and payment-system governance.

Payments oversight remains a moderately developed suptech area (combined maturity around 30%, Figure 77). Only 9% of authorities report deployed tools, while 26% indicate demand without planned implementation — suggesting conceptual awareness but uneven operational readiness. Progress may also reflect institutional arrangements, as payment oversight is often handled by dedicated operator teams within central banks or specialised regulators. EMDEs (33%) show higher engagement compared with AEs (19%) (Figure 80).

Use-case maturity is concentrated in core monitoring functions. The most developed area is real-time monitoring of payment volumes and values (42% combined maturity), a prerequisite for detecting anomalies, liquidity pressures, or operational bottlenecks (Figure 95). Moderately developed use cases (25–30%) include retail payment-fraud surveillance, payment-system performance analytics, and resilience assessments. The HKMA's recent tender for payment-data fraud analytics and the National Bank of Hungary's AI-driven detection of fraudulent transfer patterns illustrate early supervisory applications enabled by richer transaction data. Project Hertha, led by the BIS Innovation Hub and BOE, demonstrates the feasibility of using payment-system analytics to support anomaly detection across banks and payment service providers.

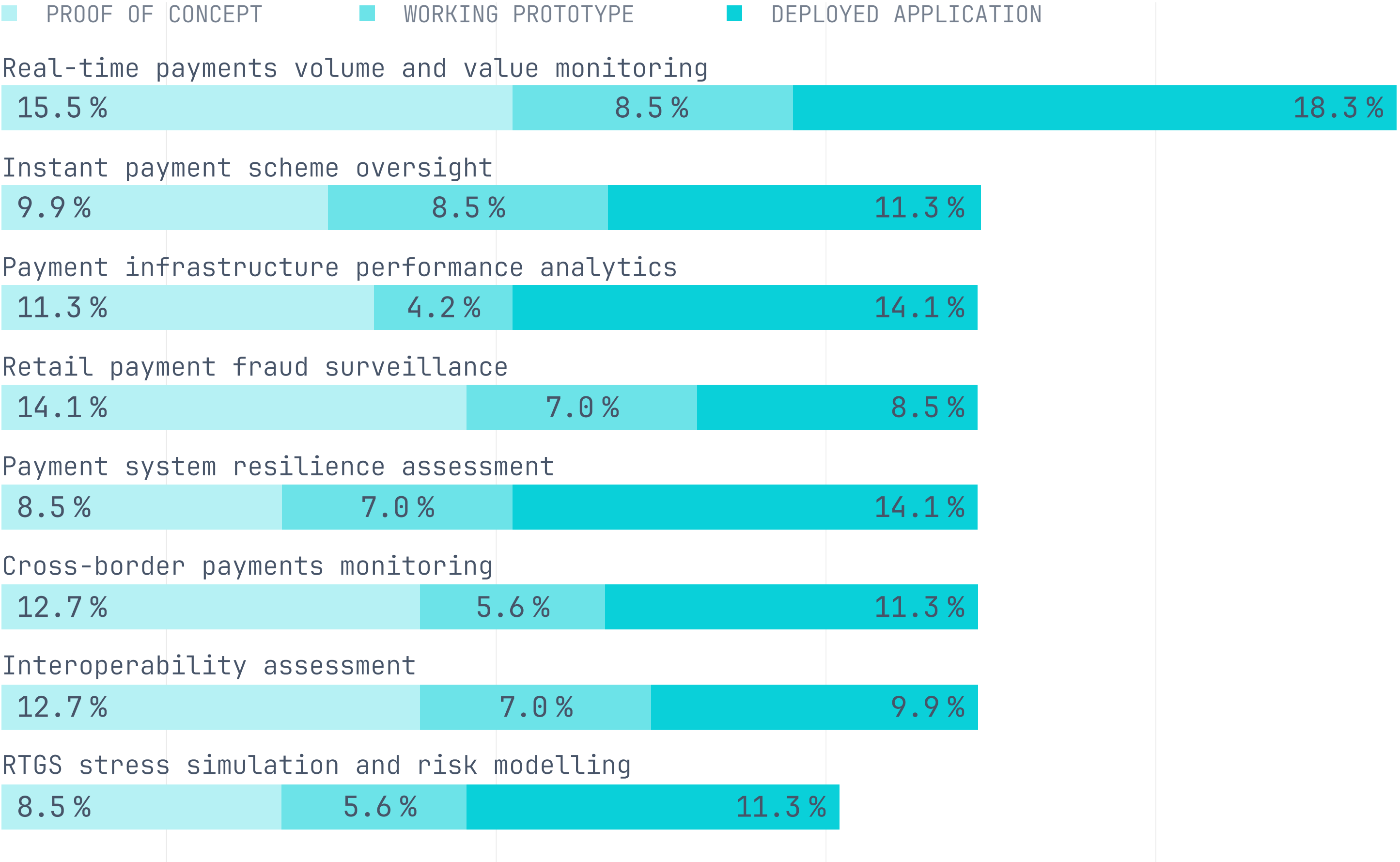
Cross-border and interoperability-related oversight capabilities are emerging but uneven. Projects such as BIS Nexus and the Regional Payment Connectivity initiative aim to operationalise seamless, multi-jurisdictional retail payments. Through Project Meridian, the BIS and partner central banks demonstrated that RTGS systems can interoperate for FX transactions, offering a blueprint for future supervisory data pathways.

The least developed area is systemic risk modelling. RTGS stress simulation and liquidity-risk modelling show only 25% combined maturity, reflecting limited adoption of advanced suptech tools for proactive, scenario-based oversight. This gap persists despite BIS research (e.g., Nexus and Mariana experiments) demonstrating the supervisory value of simulation frameworks for understanding large-value payment flows and settlement interdependencies.

Finally, several frontier initiatives illustrate growing recognition of the supervisory value of payments data. BIS Project Mandala and Rialto examine CBDC-based cross-border settlement with embedded compliance logic. India's

FIGURE 95.

Prioritisation of SupTech Use Cases Under Payments Oversight



Fraud Risk Indicator enhances real-time scam detection. Open-source infrastructure efforts, such as Mojaloop for instant payments, and RegTech Africa's work on cross-border payment data, further demonstrate a shift toward more data-intensive oversight.

Overall, payments oversight is progressing but remains early in its suptech journey. Real-time monitoring, fraud analytics, and system-performance tools are maturing, while advanced systemic-risk modelling and cross-border supervision capabilities continue to lag — highlighting a growing need for structured data, interoperable standards, and ISO 20022-enabled analytical capacity.

3.16 Prudential supervision

Prudential supervision remains one of the most established suptech domains, with authorities primarily using digital tools to strengthen data collection, validation, and baseline risk monitoring. In 2025, adoption continues to centre on foundational capabilities such as automated reporting, liquidity analytics, and cross-submission checks, while more advanced applications — including stress-testing, systemic-risk analytics, and forward-looking scenario tools — remain limited. A small group of jurisdictions is beginning to deploy AI-enabled platforms and integrated supervisory data architectures, yet most authorities remain in early or incremental stages of adoption, reflecting uneven data readiness and persistent structural constraints.

Prudential supervision remains one of the most established areas of suptech adoption, with authorities primarily using digital tools to strengthen data collection, validation, and ongoing risk monitoring. In 2025, 28% of surveyed authorities report deployed prudential applications, while early-stage exploration continues through POCs (about 11%) and working prototypes (under 10%). Interest outpaces implementation: roughly 19% of agencies express demand without concrete plans, and 32% still classify prudential suptech as not planned or not desired, underscoring uneven institutional readiness across jurisdictions.

The most mature applications continue to cluster around core supervisory processes. Automated prudential reporting and liquidity risk analytics show the highest uptake (just above 30%), reflecting long-running investment in structured templates and early-stage XBRL-type systems. The parallel transition toward ISO 20022–based reporting in several jurisdictions is also expanding the availability of structured, machine-readable data fields, which supports more automated validation and cross-entity reconciliation. Cross-validation of regulatory submissions and tools supporting onsite examination and sectoral or cross-entity analysis follow closely in the low-30% and high-20% ranges. More sophisticated capabilities — including stress testing, systemic risk analytics, model-risk assessment, and aggregation dashboards — exhibit moderate maturity (17–22%), signalling gradual but uneven expansion beyond foundational reporting tools.

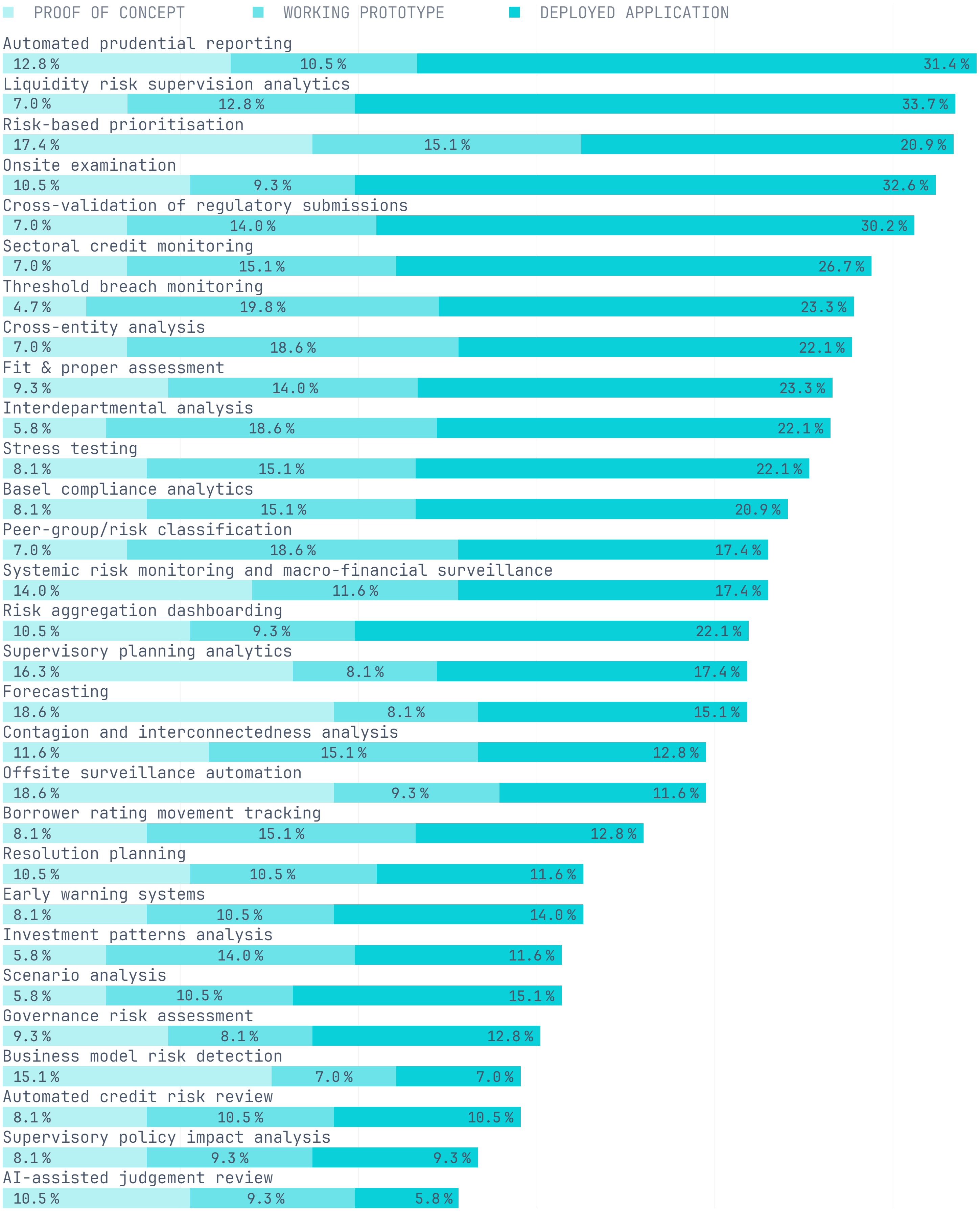
A growing set of jurisdictions are investing in integrated data platforms and advanced analytics to improve continuous risk assessment. In Japan, the Financial Services Agency (FSA) and Bank of Japan (BOJ) launched a joint data platform in 2024 to centralise high-granularity bank data, improving risk monitoring and reducing reporting burdens. Indonesia's OJK has implemented an integrated GRC system to consolidate audits, risk, and compliance for continuous oversight. Machine learning is also used to enhance data quality, detecting anomalies in credit registers in Brazil, while Reserve Bank of Australia (RBA) deploys an AI tool to enhance business liaison intelligence. The HKMA applies generative-AI models to analyse banks' earnings-call transcripts for emerging risk indicators. These initiatives demonstrate a broader shift from periodic reporting cycles toward more continuous, data-driven prudential surveillance supported by improved data architectures and AI-enabled insights.

Higher-complexity prudential applications remain nascent. Business-model risk detection, AI-assisted review of supervisory judgements, forward-looking scenario analysis, and resolution-planning analytics all show reported deployment rates below 15%. The Netherlands Bank's Radar tool — which identifies and monitors emerging technologies and their implications for banking risks — illustrates how authorities are beginning to operationalise structured, forward-looking models, but such initiatives are not yet widespread.

Overall, suptech is strengthening the foundations of prudential supervision, particularly in reporting, validation, and baseline analytics. Yet higher-order applications necessary for predictive risk assessment, model oversight, and stress testing remain underdeveloped. Progress in 2025 therefore reflects incremental institutionalisation rather than a structural shift — with a small but growing set of authorities pioneering more advanced data and AI capabilities while many others remain constrained by data fragmentation, limited analytical capacity, or legacy reporting architectures.

FIGURE 96.

Prioritisation of SupTech Use Cases Under Prudential Supervision



The SSM Trend Radar of De Nederlandsche Bank (DNB):

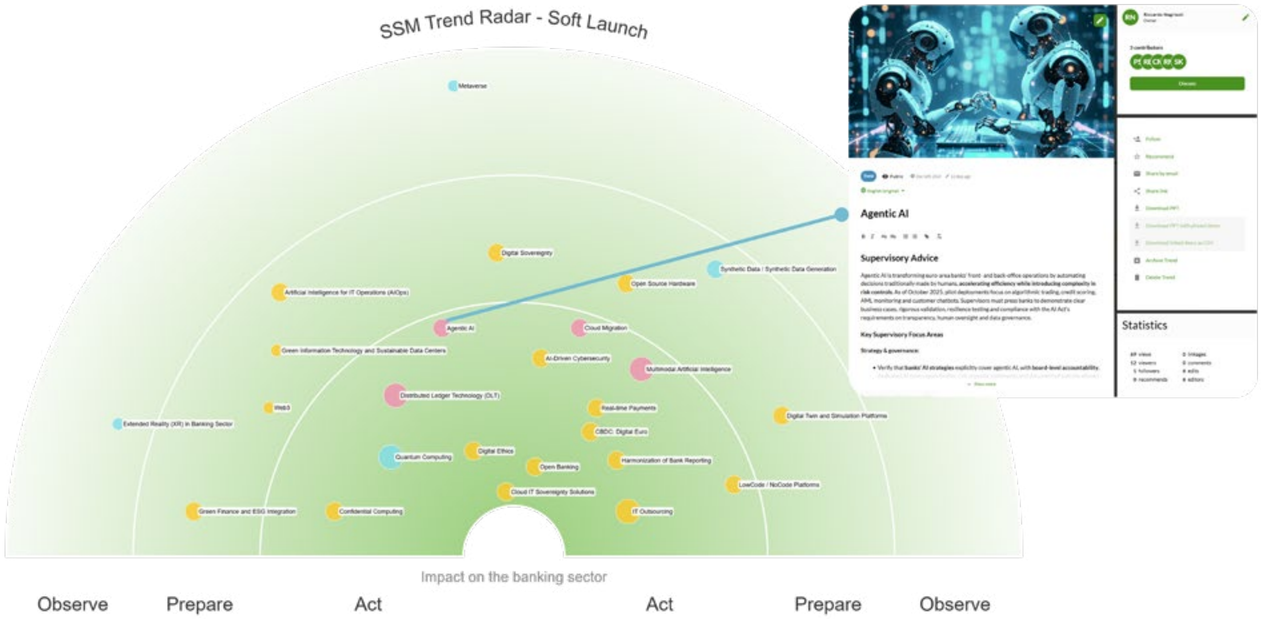
Empowering supervisors with an SSM wide platform on technology trends and associated risks

Ruben ten Berge (SupTech Advisor), Sebastian Kavelin (seconded SupTech Advisor), Friso van der Meyden (seconded SupTech Advisor), Digital Agenda Supervision Department, De Nederlandsche Bank

The SSM Trend Radar is a SupTech initiative developed by De Nederlandsche Bank (DNB) in close collaboration with our partners at the European Central Bank (ECB) and the broader Single Supervisory Mechanism (SSM). Designed as a forward-looking strategic tool, the Radar aims to identify, monitor and evaluate emerging technology trends, such as Agentic AI and Quantum Computing, that may impact banking supervision across the SSM. The SSM Trend Radar supports banking supervisors in the SSM in asking the right questions, at the right time to supervised institutions.

Supervisors face increasing pressure to keep pace with fast-moving technological developments, often with limited time, resources, and communication channels to assess tech-related banking risks. Furthermore, the complexity of banks' digital initiatives makes it difficult to fully grasp their implications and to assess disruption risks. The SSM Trend Radar addresses these challenges by applying a structured methodology that combines AI-based analysis with SSM wide supervisory expertise and delivering periodic updates to all technology trends relevant for supervisors. Trends are identified through a multi-step process that includes AI-based pre-selection, expert validation — experts from National Competent Authorities (NCAs) throughout the SSM will be consulted leading to a weighted and curated set of technology trends relevant to the banking sector — and scoring across dimensions such as impact, velocity, and supervisory relevance. These trends are then described in a standardized factsheet that offers actionable supervisory advice, and further deep dives into the trend. The trend factsheet also includes a dedicated risk lens helping supervisors to focus their dialogue with supervised institutions. In doing so, the Radar contributes to the development of SSM Future Intelligence throughout the system by bringing together technological expertise and enhancing technology literacy.

CONTINUED ON NEXT PAGE


SSM Trend Radar - Soft Launch
Metaverse
Digital Sovereignty
Artificial Intelligence for IT Operations (AIOps)
Synthetic Data / Synthetic Data Generation
Open Source Hardware
Agentic AI
Cloud Migration
Green Information Technology and Sustainable Data Centers
AI-Driven Cybersecurity
Multimodal Artificial Intelligence
Distributed Ledger Technology (DLT)
Web3
Real-time Payments
Extended Reality (XR) in Banking Sector
Digital Twin and Simulation Platforms
CBDC: Digital Euro
Quantum Computing
Digital Ethics
Open Banking
Harmonization of Bank Reporting
LowCode / NoCode Platforms
Cloud IT Sovereignty Solutions
Green Finance and ESG Integration
Confidential Computing
IT Outsourcing
Impact on the banking sector
Observe
Prepare
Act
Act
Prepare
Observe
Public
English (original)
Follow
Recommend
Share by email
Share link
Download PPT
Archive Trend
Delete Trend
Statistics
Show more

Agentic AI

Supervisory Advice

Agentic AI is transforming euro area banks' front- and back-office operations by automating decisions traditionally made by humans, **accelerating efficiency while introducing complexity in risk controls**. As of October 2025, pilot deployments focus on algorithmic trading, credit scoring, AML monitoring and customer chatbots. Supervisors must press banks to demonstrate clear business cases, rigorous validation, resilience testing and compliance with the AI Act's requirements on transparency, human oversight and data governance.

Key Supervisory Focus Areas

Strategy & governance:

- Verify that **banks' AI strategies** explicitly cover agentic AI, with **board-level accountability**.

The Radar offers an intuitive digital interface that presents a curated shortlist of emerging technology trends, each assessed for relevance to banking supervision. Trends are scored across multiple dimensions using the structured methodology co-developed with SSM stakeholders. The platform includes:

- A dynamic dashboard with interactive filtering and drill-down capabilities.
- Leveraging (gen)AI capabilities, including AI picks and an Agentic AI for foresights workflow.
- Embedded supervisory guidance and potential actions tailored to each trend.
- Integration via APIs with existing SupTech tools and supervisory workflows.
- A feedback mechanism allowing supervisors to contribute insights and refine trend assessments collaboratively.
- A collaborative commenting function enabling users to discuss individual trends and to build a network across the SSM.
- Availability in all languages of SSM member countries.
- Regular updates twice a year in line with the SREP cycle.

CONTINUED ON NEXT PAGE

The development of the SSM Trend Radar follows a phased approach and started with a Minimum Viable Product (MVP). Initial scoping and design were conducted with input from the ECB and national competent authorities (NCAs), ensuring alignment with the SSM's digital strategy. Challenges during the development process of the Radar range from setting up a robust trend scoring methodology and fact sheet design to engaging a sufficient number of stakeholders across the SSM. The MVP was launched in early 2025 with subsequent iterations incorporating real trend data and supervisory feedback. The Radar is currently being refined and is on track for its first official publication in 2026.

Publication is initially aimed for all supervisors across the SSM, while options for extending access to external stakeholders are currently being explored.

4.

The Supervisory Data Lifecycle

Suptech effectiveness ultimately depends on how well supervisory authorities manage data across the entire lifecycle, yet most still operate with a mix of legacy infrastructure and incremental upgrades. Survey results show continued reliance on 1G and 2G tools, cautious experimentation with 3G and 4G capabilities, and persistent bottlenecks in collection, governance, integration, and access that constrain the impact of advanced analytics and AI.

Supervisory authorities continue to rely on proven 1G and 2G data tools while expressing strong interest in more advanced 3G and 4G technologies. Data effectiveness remains central to suptech performance, yet authorities face persistent challenges at every stage of the data lifecycle, from collection and validation through storage, analytics, and dissemination (see Sections 1.3 and 2.4).

This section uses the SupTech DataStack framework to examine how financial authorities currently manage data and where they see demand for future capabilities. While there is growing interest in more sophisticated analytics, predictive technologies, and AI, progress is measured. Authorities are prioritising secure, well-governed foundational systems and only gradually layering in more automated, AI-enabled tools.

4.1 Data management

Across the SupTech DataStack, authorities continue to rely on conventional tools for collection, validation, storage, and reporting, with advanced capabilities deployed selectively at the margins. The framework highlights a clear implementation gap: foundational layers are only partially modernised, and most agencies are still at an early stage in building the modular, interoperable architectures required for scalable, AI-enabled supervision.

Effective data management remains a systemic constraint. Authorities struggle to handle diverse and legacy data sources, ensure timely and complete reporting, and automate core processes such as validation and reconciliation. Unstructured data is particularly difficult to exploit due to limited tooling and skills. Although many agencies consider their data broadly adequate for present needs, gaps in granularity, governance, and integration continue to limit the impact of suptech investments.

Operationalising robust data management is a widespread challenge (Figure 97). Among surveyed authorities, 64% report difficulties managing diverse, unstructured, and legacy data sources; 60% struggle to ensure timely, complete, and validated submissions across multiple reporting entities; and 57% find it difficult to manage high-volume, dynamic data in fast-changing digital environments. Limited automation for validation and reconciliation (57%) and heavy reliance on manual processes for cleaning and transformation (45%) compound these constraints.

Some authorities are now tackling these issues through targeted upgrades to their supervisory data platforms. For example, the Bank of Uganda has developed a new supervisory data platform with support from Digital Transformation Solutions and Financial Sector Deepening

FIGURE 97.

Challenges In Operationalising Effective Data Management Across Diverse Sources

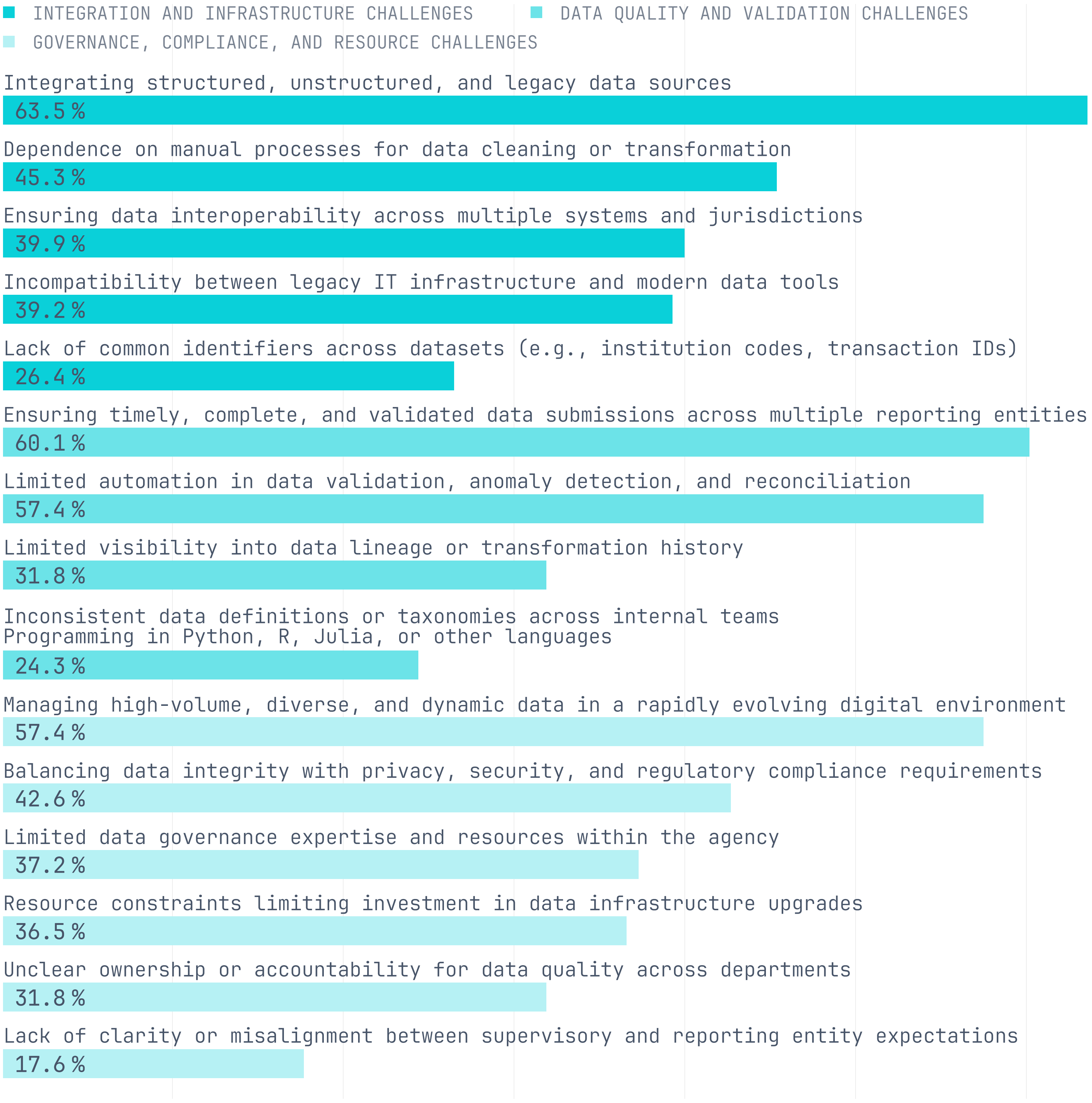
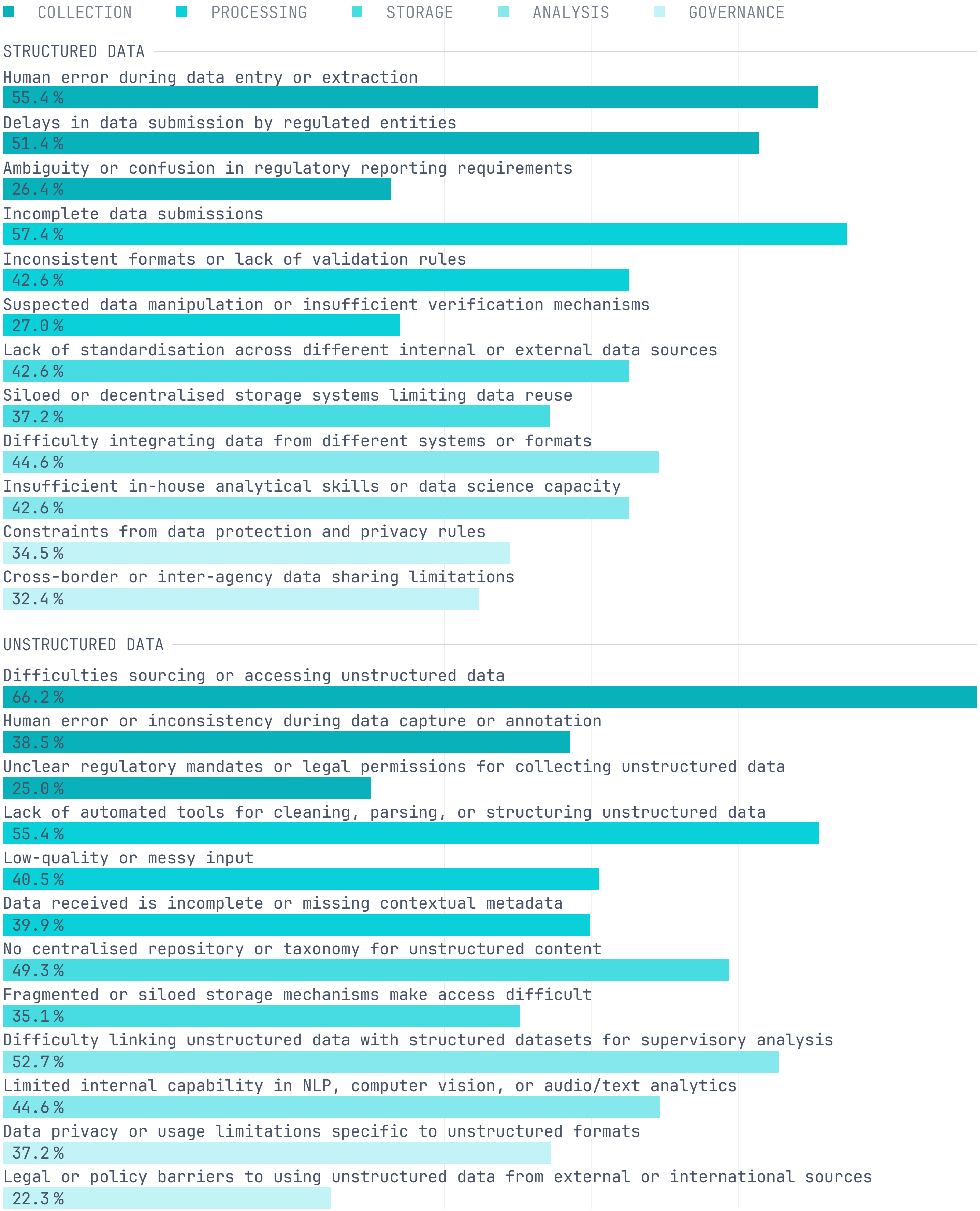


FIGURE 98.

Challenges Faced In Using Structured And Unstructured Data

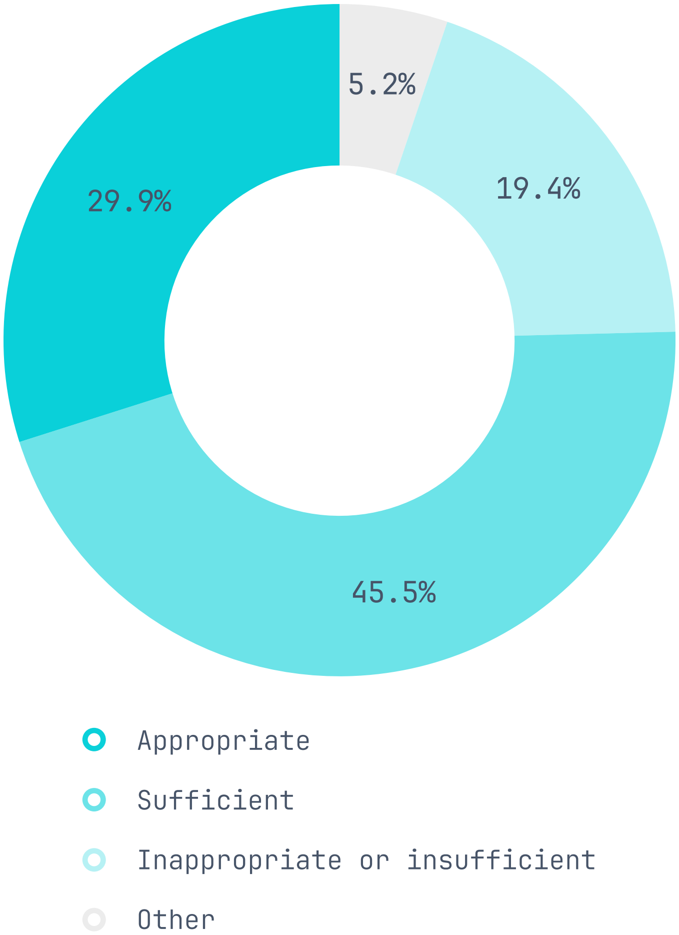


Uganda (FSDU) using the GovSpace tooling for diagnostic, use cases analysis, and POC development. The new supervisory platform strengthens data ingestion and analysis, improves integration across reporting streams, and introduces structured workflows for risk identification and escalation. This illustrates how authorities in emerging markets can use modern data infrastructure and diagnostic-driven design to close foundational data governance and analytics gaps.

Other authorities are using structured initiatives to improve data quality at source. The Reserve Bank of India's Supervisory Data Quality Index (sDQI), for instance, systematically tracks and scores the quality of supervisory submissions across dimensions such as accuracy, completeness, timeliness, and consistency. Publishing aggregate scores and methodology incentivises firms to improve internal data governance and allows supervisors to monitor progress over time (see case study below).

FIGURE 99.

Usefulness Of Agency's Currently Collected Data, Given The Granularity Of The Data Sources



Structured data issues are concentrated around quality and integration. Authorities cite incomplete submissions (57%), human error during entry or extraction (55%), reporting delays (51%), and challenges integrating data from disparate systems or formats (45%). Inconsistent formats, insufficient internal analytical skills, and limited standardisation across sources each affect 43% of agencies (Figure 98).

Unstructured data presents even greater barriers. Agencies report difficulty sourcing or accessing unstructured data (66%), limited automated tools for cleaning or structuring it (55%), challenges linking it with structured datasets (53%), absence of centralised repositories or taxonomies (49%), and limited internal capabilities in NLP, computer vision, or audio/text analytics (45%).

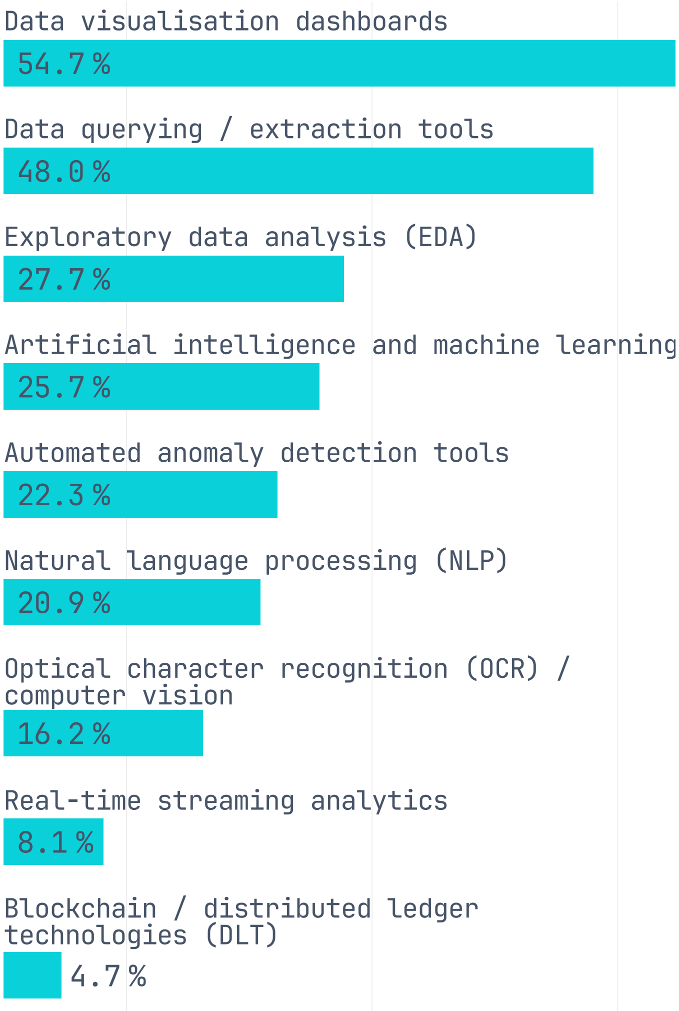
Perceptions of data usefulness have improved modestly between 2024 and 2025 but remain uneven. In 2025, 75% of agencies consider their data sufficient or appropriate for general supervisory use (up from 71% in 2024). Yet only 46% report collecting data with adequate granularity (down from 52% in 2024) and just 30% have governance frameworks that are appropriate and regularly reviewed. Nearly one-fifth of agencies (19%) still report fundamental data problems (Figure 99). Strengthening basic data governance and architecture is therefore a prerequisite for more advanced suptech adoption.

Authorities are gradually expanding their data-processing toolkits. Data visualisation dashboards are the most widely used technology (55%), followed by core querying and extraction tools such as SQL or GraphQL

(48%) (Figure 100). Around a quarter of agencies report using exploratory data analysis techniques (28%) and AI or machine learning (26%). Automation is present but not yet pervasive, with automated anomaly detection at 22% and natural language processing at 21%. Use of next-generation technologies remains limited: real-time streaming analytics is reported by 8% and blockchain or distributed ledger technologies by 5%. These patterns confirm that most agencies are still consolidating foundational capabilities while selectively testing more advanced tools.

FIGURE 100.

Technologies And Tools Used To Process And Analyse Granular Financial Data



Reserve Bank of India:

Supervisory Data Quality Index

By Dr. Jugnu Ansari (General Manager) & Geetha Giddi (Deputy General Manager), Department of Supervision (CO), Reserve Bank of India

The Supervisory Data Quality Index (sDQI) is a standardised metric for assessing the quality of data submitted by banks and non-bank entities through supervisory returns. It is a suptech tool that measures the bank's adherence to the principles outlined in the regulatory directions. The sDQI is an important step toward ensuring transparency, accountability, and continuous improvement in the way financial institutions manage and report their data. The index measures the quality of supervisory data across four crucial dimensions, i.e. Accuracy, Completeness, Timeliness and Consistency. The detailed Methodology and the aggregate sDQI score are published every quarter on the RBI website.

Practical Benefits

The sDQI has enabled improvements in supervisory assessments and in reporting on institutions' internal practices and procedures for risk data aggregation.

Enhanced Supervision

- **Better Risk Assessment:** High-quality, accurate, and timely data enables supervisors to conduct a more effective and reliable Supervisory Review and Evaluation Process. This leads to more precise identification and measurement of risks (e.g., credit, market, operational risks) within the financial system.
- **Informed Policy Decisions:** Regulators rely on aggregate, high-quality data to understand the broader financial landscape. The sDQI supports evidence-based policy formulation, enhancing financial stability and systemic risk management.
- **Efficiency in Monitoring:** A standardized, reliable data submission process reduces the need for constant back-and-forth for clarification, improving the efficiency of the supervisory monitoring process.

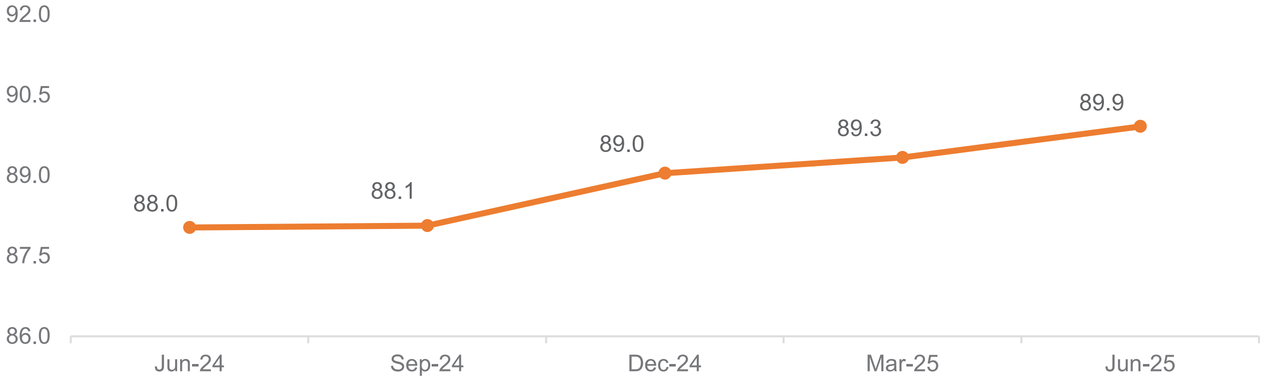
CONTINUED ON NEXT PAGE

Improved Institutional Practices

- **Strengthened Compliance:** By establishing clear benchmarks for data quality—based on parameters like accuracy, timeliness, completeness, and consistency—the sDQI mandates that financial institutions adhere strictly to regulatory reporting guidelines.
- **Operational Excellence:** The process of improving an sDQI score forces institutions to cleanse their data and streamline internal data management and governance frameworks. This enhances the overall quality and reliability of data used for all internal decision-making, not just regulatory reporting.
- **Reduced Operational Risk:** Poor data quality is a significant source of operational risk. A focus on sDQI helps mitigate this risk by ensuring that critical business processes and risk models are built on sound, verifiable data.
- **Increased Stakeholder Trust:** Demonstrating a consistently high sDQI score can serve as an external indicator of a financial institution's strong internal controls and commitment to accurate reporting, thereby building trust with investors and the public.
- **BASEL Pillar III — Market Discipline:** With the publication of sDQI scores, the reporting entities are able to compare their score with peers and industry benchmarks. A relatively high sDQI score indicates that the bank's underlying data governance and reporting controls are robust, which is essential for producing the truthful, comprehensive, and timely public disclosures required by Basel Pillar 3. It helps the regulator and the market trust the bank's information.

Since its commencement, it is seen that most of the reporting institutions have been proactively working on improving their scores, especially on timeliness.

SDQI SCORE



CONTINUED ON NEXT PAGE

Challenges encountered

In the process of preparing sDQI, two significant challenges were faced: change management and technology.

- **Change Management:** As sDQI was a new supervisory tool, its implementation required robust and straightforward design, standardised implementation and clear communication with all stakeholders. Hence, the initial few months of sDQI preparation were dedicated to obtaining approvals from the Supervisory Board, model development and testing, publication procedures, workshops/conferences for supervised entities, etc.
- **Technology:** The data for each of the four parameters required extensive data extraction from the reporting system (Centralised Information Management System) for each entity for each return. The data handling procedures, the index computations, the audit trails for validation, the automation of publication of entity-wise scores along with instances, etc, required a mix of IT and processes.Challenges encountered

4.2 The suptech DataStack

The current state of suptech reveals a sector in measured transition, where traditional tools dominate across the SupTech DataStack framework's layers while advanced capabilities remain largely aspirational. Agencies continue to rely on conventional tools for collection, validation, storage, and reporting, with advanced capabilities deployed selectively at the margins. The framework highlights a clear implementation gap: foundational layers are only partially modernised, and most agencies are still at an early stage in building the modular, interoperable architectures required for scalable, AI-enabled supervision.

The current suptech landscape shows a sector in measured transition. Across the SupTech DataStack layers, most authorities still rely on conventional technologies for collection, validation, storage, and reporting, while advanced capabilities remain emergent. Web portals, Excel-based validation, relational databases, and static reports are still dominant. Predictive analytics, cloud-native architectures, and generative AI are being explored, but adoption remains limited.

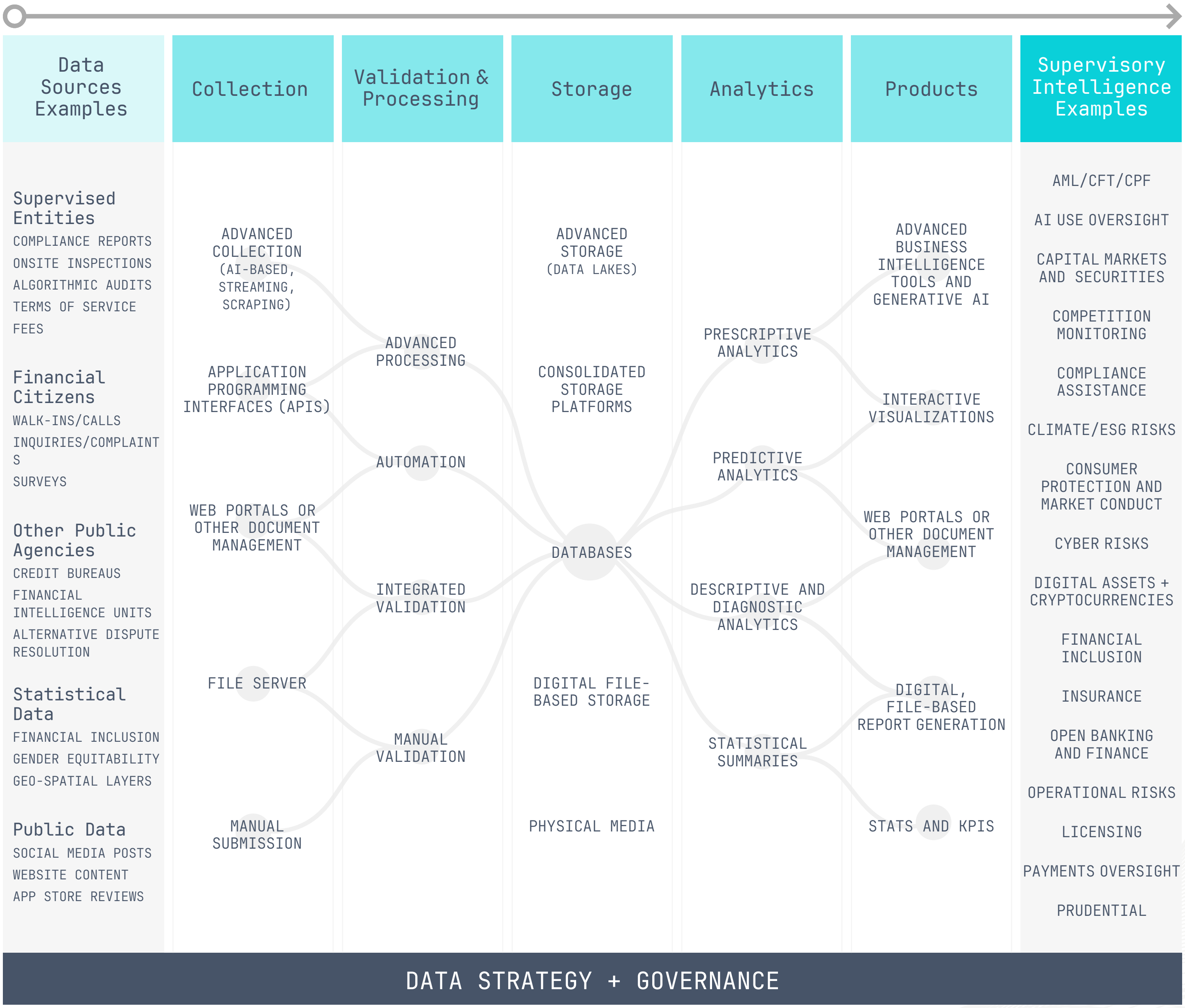
The SupTech DataStack framework provides a modular, technology-agnostic architecture that maps the full supervisory data lifecycle: from raw inputs and collection interfaces, through validation and transformation, to storage, analytics, and supervisory intelligence products such as dashboards and structured alerts. It is aligned with the SupTech Taxonomy used in the survey, providing a common reference for diagnosing current capabilities and planning upgrades.

Modularity is central to the framework. Each layer can be equipped with different tools depending on cost, functionality, and organisational capacity. This allows authorities to progress unevenly across layers – for example, strengthening internal collection and storage while relying on external providers for advanced analytics – without losing sight of the end-to-end architecture.

By emphasising interoperability and the integration of heterogeneous data sources, the framework directly addresses many of the coordination failures highlighted elsewhere in the report. It recognises that advanced analytics and AI will only be effective if built on solid foundations in data collection, validation, and storage, and provides a structured path for authorities to move from fragmented, legacy systems towards more automated, AI-enabled environments.

FIGURE 101.

Layering Of The Supervisory Datastack: End-To-End Data Architecture For Modern Supervision



Data Sources Examples

Supervised Entities
- COMPLIANCE REPORTS
- ONSITE INSPECTIONS
- ALGORITHMIC AUDITS
- TERMS OF SERVICE
- FEES

Financial Citizens
- WALK-INS/CALLS
- INQUIRIES/COMPLAINTS
- SURVEYS

Other Public Agencies
- CREDIT BUREAUS
- FINANCIAL INTELLIGENCE UNITS
- ALTERNATIVE DISPUTE RESOLUTION

Statistical Data
- FINANCIAL INCLUSION
- GENDER EQUITABILITY
- GEO-SPATIAL LAYERS

Public Data
- SOCIAL MEDIA POSTS
- WEBSITE CONTENT
- APP STORE REVIEWS

Collection

- ADVANCED COLLECTION (AI-BASED, STREAMING, SCRAPING)
- APPLICATION PROGRAMMING INTERFACES (APIS)
- WEB PORTALS OR OTHER DOCUMENT MANAGEMENT
- FILE SERVER
- MANUAL SUBMISSION

Validation & Processing

- ADVANCED PROCESSING
- AUTOMATION
- INTEGRATED VALIDATION
- MANUAL VALIDATION

Storage

- ADVANCED STORAGE (DATA LAKES)
- CONSOLIDATED STORAGE PLATFORMS
- DATABASES
- DIGITAL FILE-BASED STORAGE
- PHYSICAL MEDIA

Analytics

- PRESCRIPTIVE ANALYTICS
- PREDICTIVE ANALYTICS
- DESCRIPTIVE AND DIAGNOSTIC ANALYTICS
- STATISTICAL SUMMARIES

Products

- ADVANCED BUSINESS INTELLIGENCE TOOLS AND GENERATIVE AI
- INTERACTIVE VISUALIZATIONS
- WEB PORTALS OR OTHER DOCUMENT MANAGEMENT
- DIGITAL, FILE-BASED REPORT GENERATION
- STATS AND KPIS

Supervisory Intelligence Examples

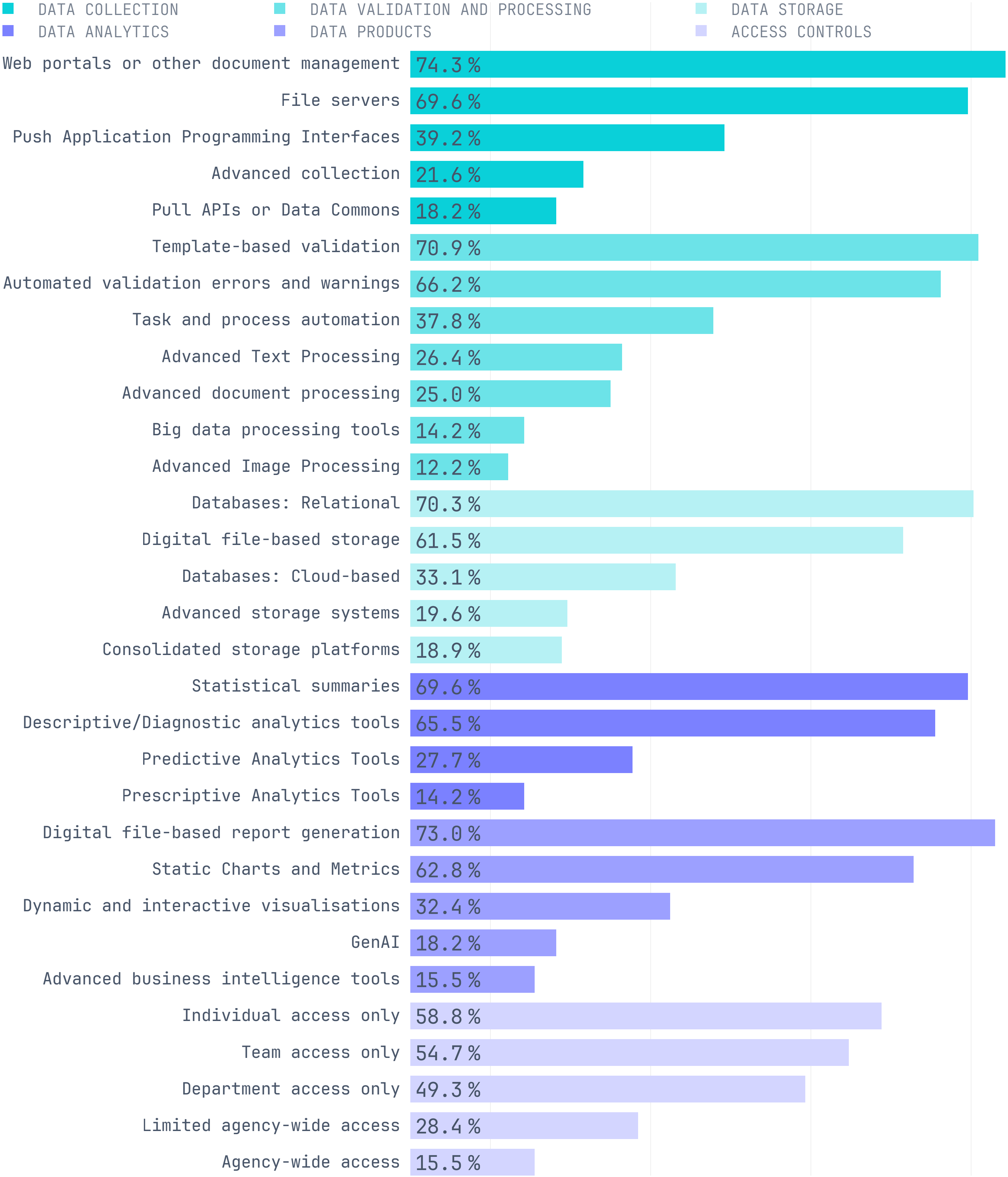
- AML/CFT/CPF
- AI USE OVERSIGHT
- CAPITAL MARKETS AND SECURITIES
- COMPETITION MONITORING
- COMPLIANCE ASSISTANCE
- CLIMATE/ESG RISKS
- CONSUMER PROTECTION AND MARKET CONDUCT
- CYBER RISKS
- DIGITAL ASSETS + CRYPTOCURRENCIES
- FINANCIAL INCLUSION
- INSURANCE
- OPEN BANKING AND FINANCE
- OPERATIONAL RISKS
- LICENSING
- PAYMENTS OVERSIGHT
- PRUDENTIAL

DATA STRATEGY + GOVERNANCE

FIGURE 102.

Underpinning Technologies Used By Agencies To Enable Supervisory Processes

According To The Supervisory Stack Layers Of The SupTech Taxonomy



Survey responses for 2025 illustrate how agencies are positioned along this architecture (Figure 102):

- **Collection** is dominated by web portals and document-management systems (74%) and file servers (70%). Push APIs are used by 39% of agencies, but more advanced techniques such as web scraping (22%) and pull APIs (18%) remain niche.
- **Validation and processing** rely heavily on template-based checks, predominantly in Excel (71%), and automated validation with integrated warnings (66%). Task automation is reported by 38%. More advanced capabilities – including text processing (26%), document processing (25%), and big data tools (14%) – are used by a smaller subset. Image processing (12%) is even less common, reflecting a continued focus on structured data.
- **Storage** are anchored in relational databases (70%) and file-based storage (62%). Cloud adoption stands at 33%. Data lakes (20%) and data warehouses (19%) remain relatively uncommon.
- **Analytics** rely on statistically oriented and descriptive methodologies and tools (70% and 66%, respectively), while predictive analytics (28%) and prescriptive tools (14%) are still limited.
- **Data products** and access are delivered primarily through file-based reports (73%) and static metrics (63%), with dynamic visualisations (32%) and advanced business intelligence tools (16%) less prevalent. Generative AI is reported by 18% of agencies, consistent with early-stage experimentation rather than operational deployment.
- **Access controls** remain relatively restrictive: individual (59%) and team-level (55%) access dominate over broad, agency-wide permissions (16%).

Taken together, these findings depict authorities that are consolidating baseline capabilities while cautiously piloting selected advanced and AI-enabled tools, in line with a risk-averse and resource-constrained operating environment.

4.3 Data collection

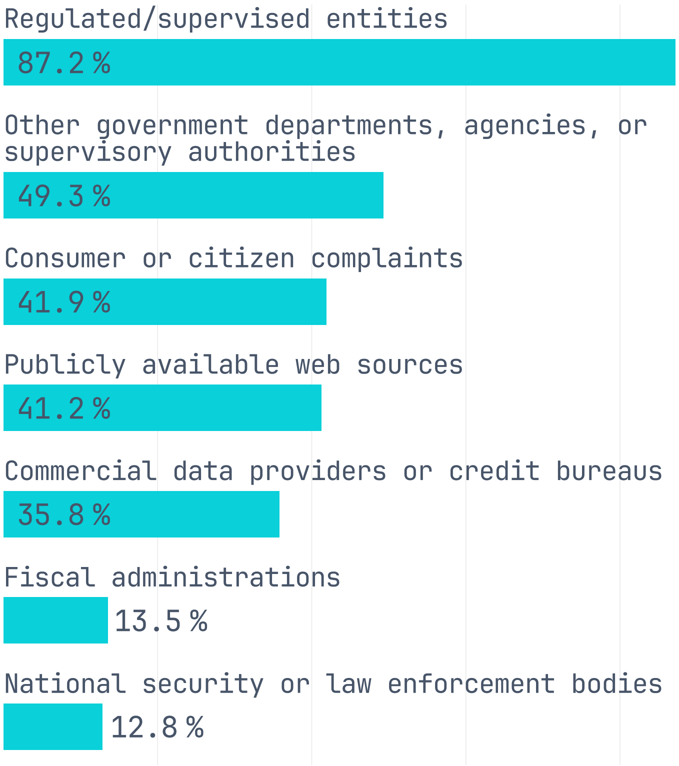
Supervisory data collection remains anchored in traditional regulatory reporting from supervised entities, complemented by government sources and consumer channels, while only a minority of authorities systematically integrate alternative or high-frequency datasets. Limited use of machine-readable APIs and continued dependence on semi-structured and unstructured formats create friction for automation and slow progress towards real-time, suptech-ready data ingestion.

Data collection practices are still centred on traditional regulatory reporting from supervised entities, supplemented by government sources and direct public inputs. Integration of alternative and non-traditional data remains limited and experimental.

Regulated entities are the primary source of data for 87% of authorities (Figure 103). Nearly half of agencies (49%) also obtain data from other government departments and supervisory authorities, reflecting the importance of inter-institutional cooperation. Consumer complaints and publicly available web sources each contribute to around 41% of agencies' data, underlining the value of direct citizen feedback and open-source intelligence. Commercial data providers and credit bureaus are used by 36% of agencies. More specialised sources – fiscal administrations and national security bodies – each contribute to data collection in around 14% and 13% of cases, respectively.

FIGURE 103.

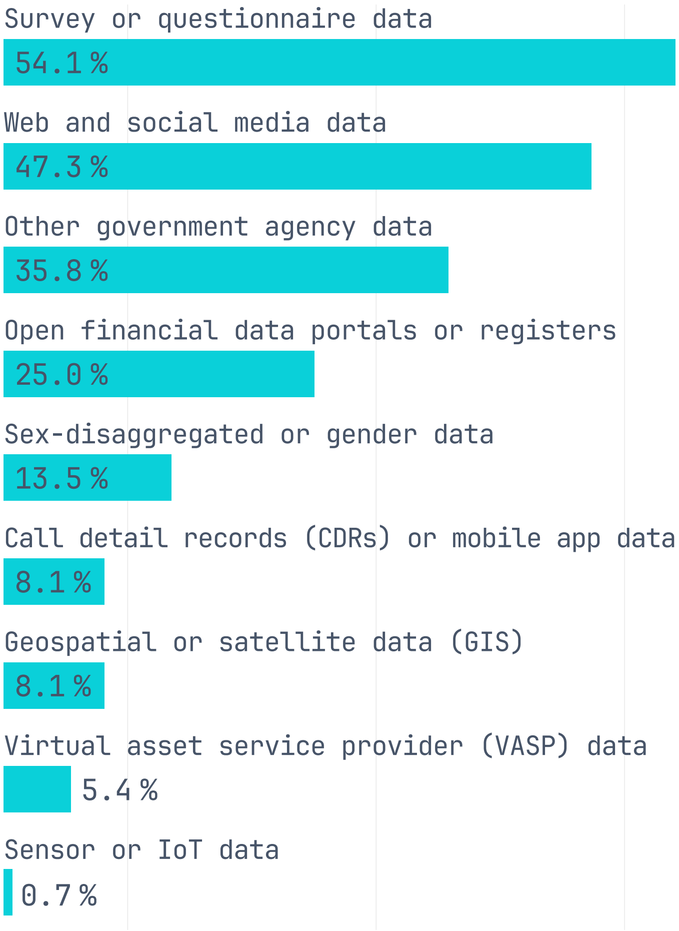
Data Sources For Collected Data



Authorities are also exploring alternative data sources relevant for supervision and intelligence, but adoption remains selective (Figure 104). Survey and questionnaire data is the most common non-traditional input (54%), followed by web and social media monitoring (47%). Data from other government agencies (36%) and open financial portals (25%) are used more sporadically. Sex-disaggregated datasets, call detail records, geospatial data, virtual asset service provider data, and sensor or IoT data remain niche inputs, each reported by fewer than 14% of agencies. The limited use of these datasets reflects both the absence of established reporting frameworks and persistent concerns around privacy, proportionality, and data-sharing arrangements with non-financial actors, which are central considerations in supervisory data strategies such as the European Banking Authority's (EBA) Data Strategy, the Bank of England's Data and Analytics Strategy.

FIGURE 104.

Collected Alternative Data Sources Relevant To Supervision And Intelligence

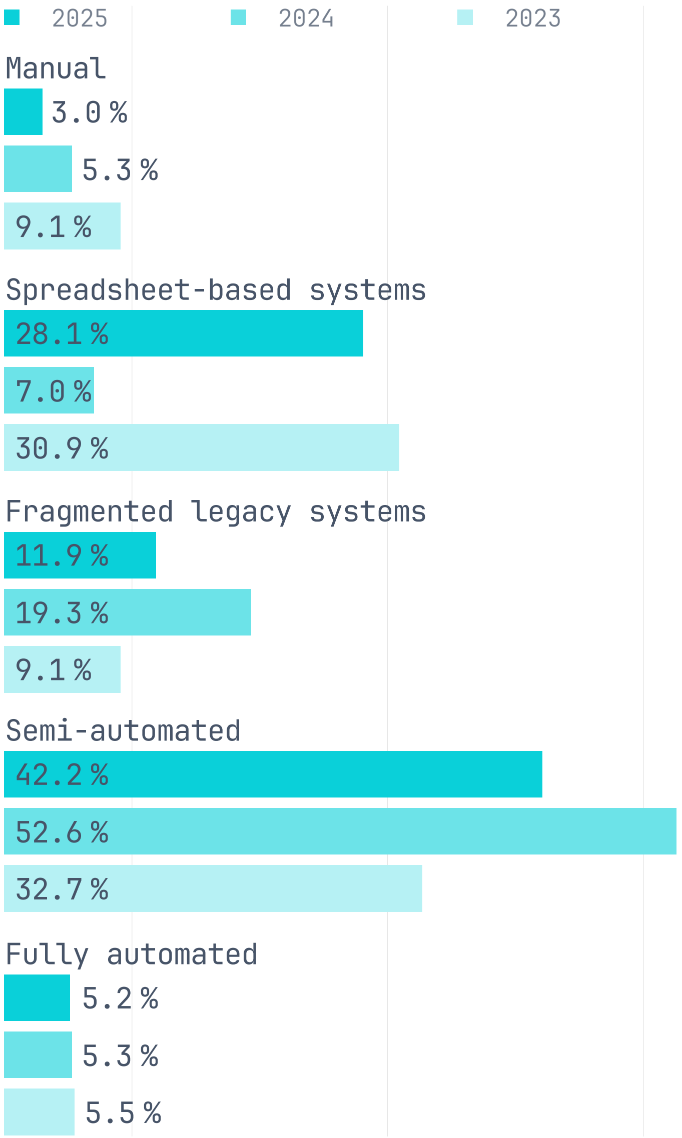


The digital capabilities of reporting entities remain mixed. In 2025, semi-automated systems – typically ETL/ELT-type pipelines feeding supervisory templates – are the most common setup, used by 42% of authorities (Figure 105). Spreadsheet-based systems still account for 28% of reporting, while fragmented legacy systems and fully manual processes, although declining, are reported by 12% and 3% of authorities, respectively. Fully automated direct pulls by supervisors from entities' systems remain rare at a little over 5%, indicating that continuous or event-driven reporting is not yet common practice.

Data formats and protocols reinforce these patterns. Semi-structured formats are used by 74% of agencies, unstructured formats by 55%,

FIGURE 105.

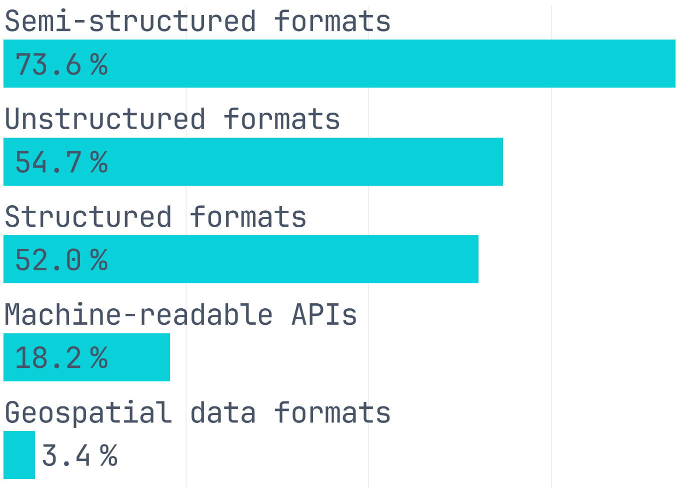
Digital Data Capabilities Of The Entities From Which Data Are Collected 2023–2025



and traditional structured formats by 52% (Figure 106). Machine-readable APIs – critical for high-volume, low-latency data exchange – are used by only 18% of agencies. This dependence on formats requiring extensive manual preparation and cleansing, combined with limited API use, is a key bottleneck for automated suptech data ingestion. The absence of shared technical standards and metadata conventions across reporting entities further contributes to fragmentation, reducing supervisors' ability to integrate data efficiently across functions and sources.

FIGURE 106.

Formats And Protocols Used For Data Collection Or Exchange



4.4 Data processing

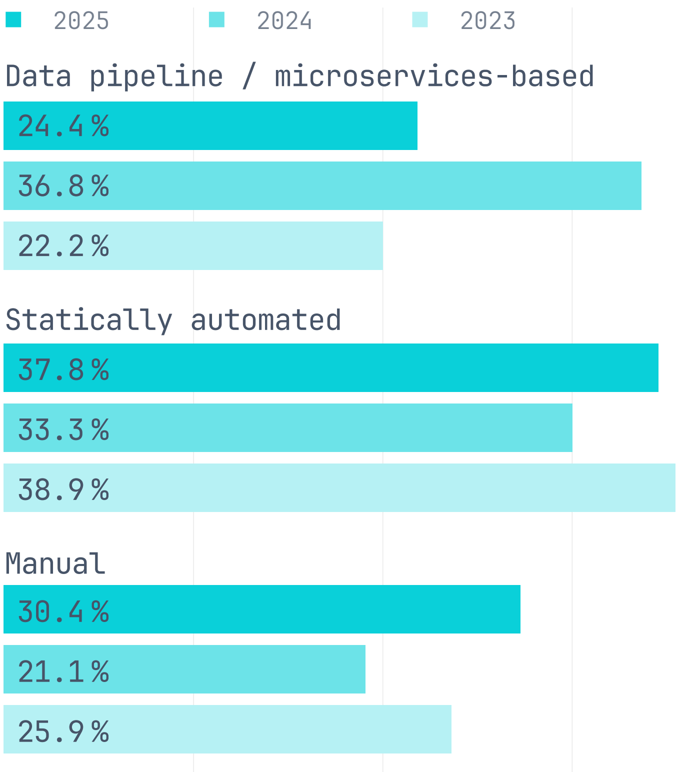
Data processing workflows are still dominated by manual handling and static automation, with pipeline-based architectures present but not yet transformative. This reliance on hands-on intervention constrains scalability and makes it difficult to absorb growing data volumes, limiting the extent to which authorities can embed continuous, automated analytics into supervisory practice.

Data processing remains dominated by static automation and manual handling, with modern pipeline-based workflows rising but not yet displacing legacy methods. In 2025, 38% of agencies report relying primarily on static automation using scripts, macros, or RPA (Figure 107), while manual processing remains high at 30%. Pipeline-based workflows – including ETL/ELT pipelines, workflow orchestration tools, and microservices-based architectures – are used by 24% of agencies, with the remaining 7% employing hybrid models that combine manual, automated, and pipeline-based methods.

Compared with earlier periods, static automation has remained relatively stable,

FIGURE 107.

Data Processing 2023–2025



while manual handling has rebounded, indicating persistent operational dependence on spreadsheets, ad hoc scripts, and locally executed processes within supervisory teams. Pipeline-based methods, which rose sharply to 37% in 2024, declined to 24% in 2025. This shift suggests that authorities experimented with pipeline modernisation but encountered structural barriers such as legacy system integration challenges, limited engineering capacity, and the absence of enterprise data platforms capable of supporting persistent, end-to-end automation.

These dynamics also highlight the bottlenecks that arise when data ingestion, validation, and transformation remain compartmentalised across teams rather than orchestrated through shared infrastructure. As a result, modern workflow techniques have not yet meaningfully reduced the sector's underlying reliance on manual or basic automated processes. This limits scalability, constrains adoption of continuous or event-driven data feeds, and slows progress towards real-time or high-frequency supervisory analytics. Without investment in engineering capability, metadata governance, and interoperability layers, pipeline-based automation is unlikely to displace static or manual processes at scale.

4.5 Data storage and the cloud

Cloud adoption is advancing cautiously, with private-cloud deployments preferred where used and a significant share of authorities yet to begin migration. While cloud infrastructure is increasingly recognised as a prerequisite for scalable analytics and AI, concerns about security, compliance, legacy integration, and governance continue to slow the transition away from purely on-premises environments.

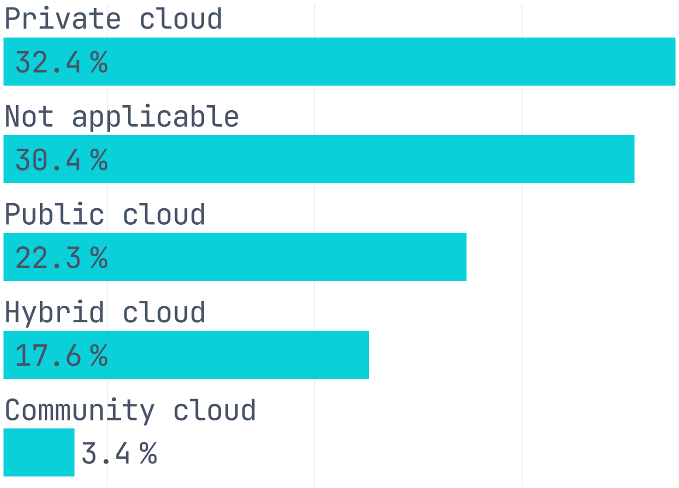
Private cloud environments are the preferred cloud computing and storage model for supervisory agencies, reflecting a priority (and in some cases a regulatory requirement) for control and security. Moving beyond local servers and legacy databases has become essential as data volumes rise, reporting frequencies increase, and supervisors seek to integrate more granular and unstructured data into their workflows. While traditional 2G relational databases can still support core reporting, scaling to 3G and 4G AI-enabled suptech requires more elastic, resilient infrastructure that can support high-volume ingestion, cross-domain linkage, and advanced analytics.

Supervisory authorities are therefore progressively complementing low-resilience storage, such as local drives and on-premise servers, with more robust cloud-based solutions. Secure transfer protocols (HTTPS, SFTP) are now standard, and many agencies are piloting or expanding use of commercial cloud platforms to improve reliability and failover. For example, Banco de España has described its progressive migration of analytical workloads to cloud environments as part of a broader data-platform modernisation; the Bank of England has publicly confirmed expansion of its cloud usage to support data and analytics functions (see case study below); and the Reserve Bank of India has announced plans for cloud-based architectures in selected supervisory domains. In parallel, market infrastructures and shared reporting utilities are moving to cloud-native architectures, such as the migration of Austria's regulatory reporting infrastructure operated by Oesterreichische Kontrollbank (OeKB) and A-Reg in partnership with Nasdaq's AxiomSL platform (see case study below), and the adoption by the Andorran Financial Authority (AFA) of Regnology's cloud-native Supervisory Hub on Rcloud to support scalable, secure regulatory data collection and analysis. These examples illustrate how both authorities and reporting utilities are using cloud architectures to increase scalability and reduce operational risk in regulatory data flows.

Survey results for 2025 confirm that cloud adoption remains cautious and security-driven. Private cloud solutions are the most common model, used by 32% of surveyed agencies, reflecting institutions' preference for dedicated environments with strong control over sensitive supervisory data (Figure 108). Public cloud adoption stands at 22%, often for development, testing, or non-confidential workloads, while hybrid cloud arrangements are used by 18% to balance on-premise systems with external capacity. A substantial portion of the sector has yet to begin its transition, with 30% reporting that cloud computing is not yet applicable to their operations.

FIGURE 108.

Types of Cloud Computing That Agencies Have Adopted

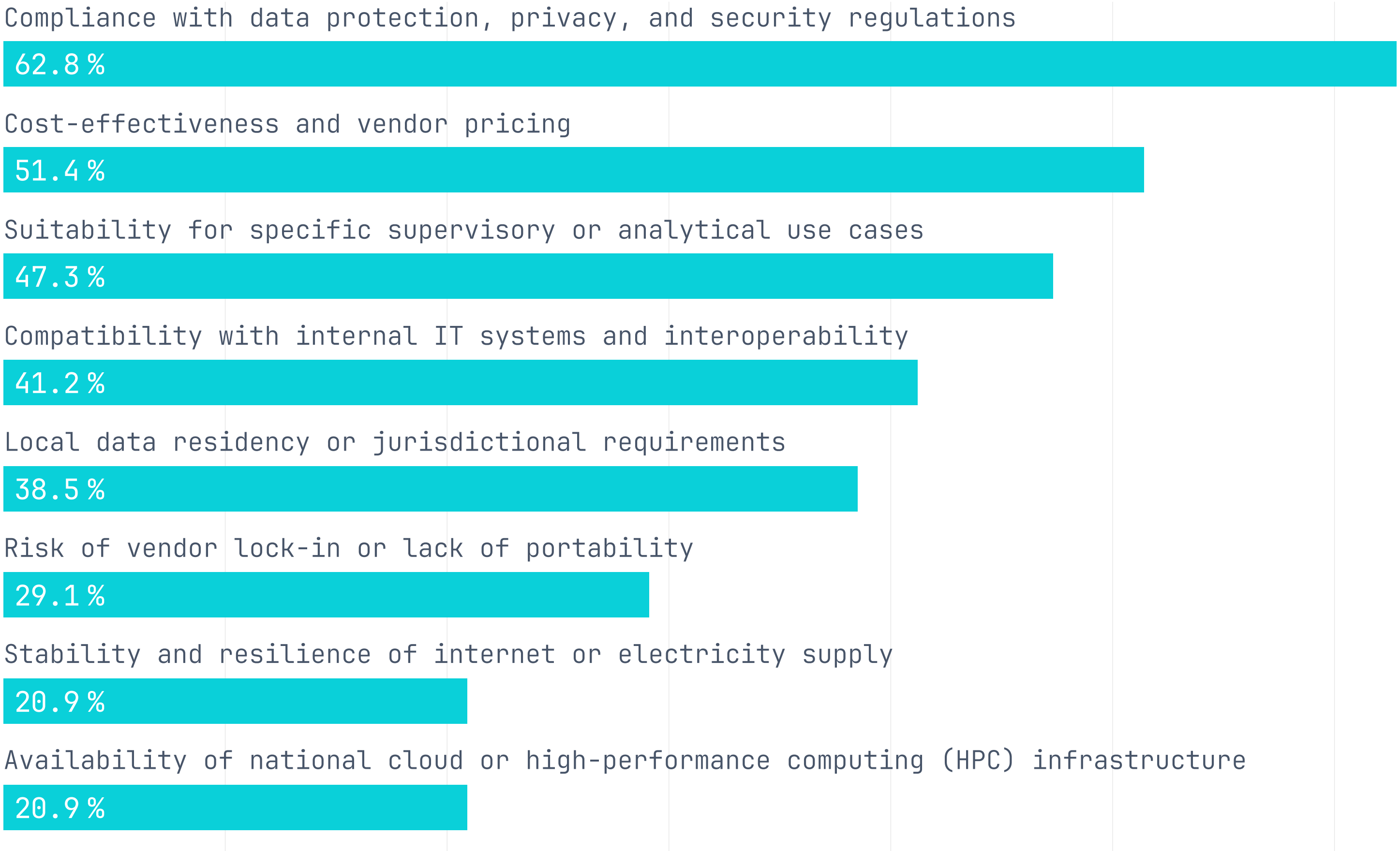


When assessing cloud-based computing or storage services, supervisory authorities prioritise data protection, compliance, and cost-effectiveness (Figure 109). The most frequently cited factor is compliance with data-protection, privacy, and security regulations (63%), followed by cost and vendor pricing (51%), and suitability for specific supervisory or analytical use cases (47%). Local data-residency and jurisdictional requirements (39%) and the risk of vendor lock-in (29%) also feature prominently, particularly where authorities must comply with domestic localisation rules or ensure exit options from particular providers. In contrast, external infrastructural considerations such as internet or electricity reliability and national cloud or high-performance computing infrastructure are referenced by around one-fifth of agencies, indicating that internal governance and regulation remain the main determinants of cloud strategy.

Despite the potential benefits, cloud adoption introduces non-trivial governance challenges. Security, privacy, and data protection are perceived as the most pressing issues, with 88% of agencies agreeing that they are major concerns (Figure 110). Compliance with legal and regulatory obligations (84%) is similarly prominent. Internally, integration with legacy systems (81%) and managing change and organisational culture (81%) pose major obstacles, while cost management remains a significant concern for 78% of respondents. Taken together, these results suggest that

FIGURE 109.

Factors Considered Most Applicable In Assessing Cloud-Based Computing Or Storage Services



barriers to cloud adoption are driven less by technology availability than by institutional risk appetite, regulatory constraints, and the complexity of modernising entrenched architectures.

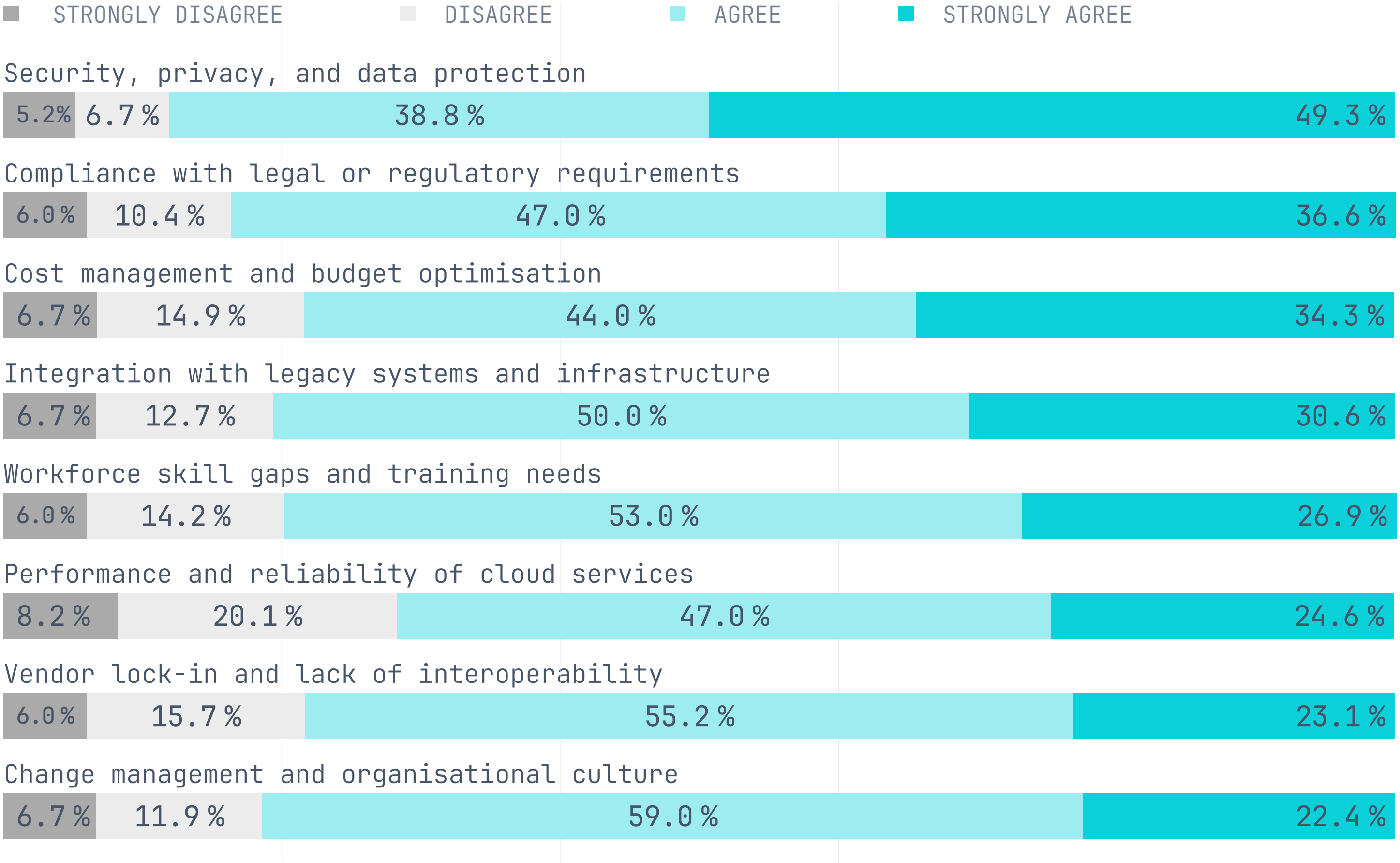
When these hurdles are managed effectively, cloud computing provides critical enablers for modern supervision: elastic storage and compute capacity, more robust disaster recovery, and access to advanced analytical and AI capabilities without large up-front infrastructure investments. In particular, cloud-delivered AI services and managed data platforms can lower entry barriers for authorities experimenting with machine learning, generative AI, or high-frequency analytics. For many agencies, especially in resource-constrained settings, carefully governed cloud adoption will be a necessary precondition for moving beyond pilot-scale suptech applications towards sustained, production-grade digital supervision.

Bank of England's transition to a hybrid and multi-cloud supervisory architecture

The Bank of England is modernising its supervisory and operational infrastructure through a hybrid and multi-cloud strategy that blends private, on-premises systems with public-cloud services. Rather than relying on a single provider, the Bank uses a diversified cloud model that incorporates Microsoft Azure and other commercial platforms, alongside its internal data centres, to enhance resilience, flexibility, and interoperability. This approach supports the modernisation of core systems,

FIGURE 110.

Significant Challenges For Cloud Adoption



including the Real-Time Gross Settlement (RTGS) service, and underpins the development of a new Enterprise Data Platform designed to improve data quality, accessibility, and analytical capability.

To enable cloud-native development, the Bank is adopting containerisation technologies such as Kubernetes. Throughout the transition, the Bank maintains a strong focus on security, compliance, and governance, recognising the sensitivity of supervisory and payments-system data.

Overall, the BOE's hybrid and multi-cloud model demonstrates a measured but forward-leaning approach that strengthens operational resilience while creating the technical foundations for more advanced data management and supervisory innovation.

Transforming Regulatory Reporting in Austria with AuRep and Nasdaq AxiomSL

Ed Probst, Senior Vice President, Regulatory Technology, Nasdaq

Austria's financial sector operates within a complex regulatory landscape shaped by both European Union (EU) and local requirements. The central bank of the Republic of Austria (OeNB) has created an advanced, data first approach to local reporting which has made automated reporting solutions a necessity for the regulated banks. While the existing solution implementation has been refined over the last decade, the evolving regulatory environment and expectations —with frameworks like the ECB's Integrated Reporting Framework (IReF), increasing data granularity, and the need for faster adaptation — highlighted the need for a flexible, future-ready approach. The future of regulatory reporting in Austria is not just about handling new regulatory frameworks with greater data requirements, but also about enabling faster turnaround for regulatory changes, providing flexibility for diverse bank requirements, and preparing for the AI-driven era.

With the OeNB (Austrian Central Bank) combining EU EBA reporting and local requirements — often with additional ten-fold increase in the number of validation rules and enhanced data definitions — banks needed a solution that could go beyond incremental improvements. AuRep, a service provider owned by seven banking groups and covering 90% of all regulated banking entities in Austria, recognized the need for an innovative reporting software that i) is operated in the optimal Target Operating Model on an innovative, scalable, and fully compliant Public Cloud Infrastructure, ii) is) tailored to the Austrian use case of granular reporting based on OeNBs Integrated Reporting Data Model to continue the success story of standardized granular reporting, and at the same time utilize a future-proof standard software for our platform service, and iii) allows banks to generate and submit all reports mandated by Austrian and European regulations in a uniform and thoroughly standardised fashion, helping to achieve significant economies of scale.

Nasdaq AxiomSL, hosted on AxiomSL's RegCloud, is designed to deliver flexible, controlled and highly scalable functionality to the member banks and future-proof Nasdaq - Internal Use: Distribution limited to Nasdaq personnel and authorized third parties subject to confidentiality obligations regulatory reporting for new requirements such as IReF. The project, which began in February 2025 and is

CONTINUED ON NEXT PAGE

scheduled to go live in 2027, will serve 7 banking groups and over 800 reporting entities, submitting approximately 24,000 reports monthly and handling massive data volumes.

Key features of the Nasdaq AxiomSL solution:

- Cloud-native architecture for scalability, performance and resilience.
- Strong data management platform to build and maintain durable and seamless integration pipelines
- Visual business rules and lineage for intuitive and transparent compliance with evolving regulations.
- Regulatory monitoring capabilities, enabling proactive identification of upcoming regulatory changes and early adaptation.
- Support for both EU and local reporting requirements, including granular data set reports (SmartCubes) and prescribed calculation and allocation logic.

Innovation for the AI Era

As regulatory reporting enters the AI era, the landscape is set to change dramatically. Regulations are expected to evolve faster, become more data-driven, and potentially require near-real-time compliance. AxiomSL's platform offers open architecture and robust data integration that can incorporate AI-driven features. This positions Austrian banks to:

- Automating complex data validation and anomaly detection
- Enabling explainable, auditable, and transparent compliance processes
- Ensure transparency and explainability, which are becoming regulatory expectations in the AI era.

Impact and Strategic Significance

The migration to Nasdaq AxiomSL marks a significant transformation, enabling future-proof compliance, operational efficiency, scalability, and enhanced security. AuRep's approach demonstrates how industry-wide cooperation and innovation can simplify compliance and reduce costs. The collaboration exemplifies how cloud-based RegTech, with built-in regulatory monitoring and AI-readiness, can transform regulatory reporting and equip Austria's financial sector to navigate complex compliance landscapes for decades to come.

4.6 Data access

Data access remains tightly restricted and largely file-based, with many datasets locked in siloed systems and only limited use of internal or external APIs. This access model hampers reuse, cross-team collaboration, and real-time analytics, reinforcing fragmentation and delaying the shift towards more integrated, service-oriented supervisory data architectures.

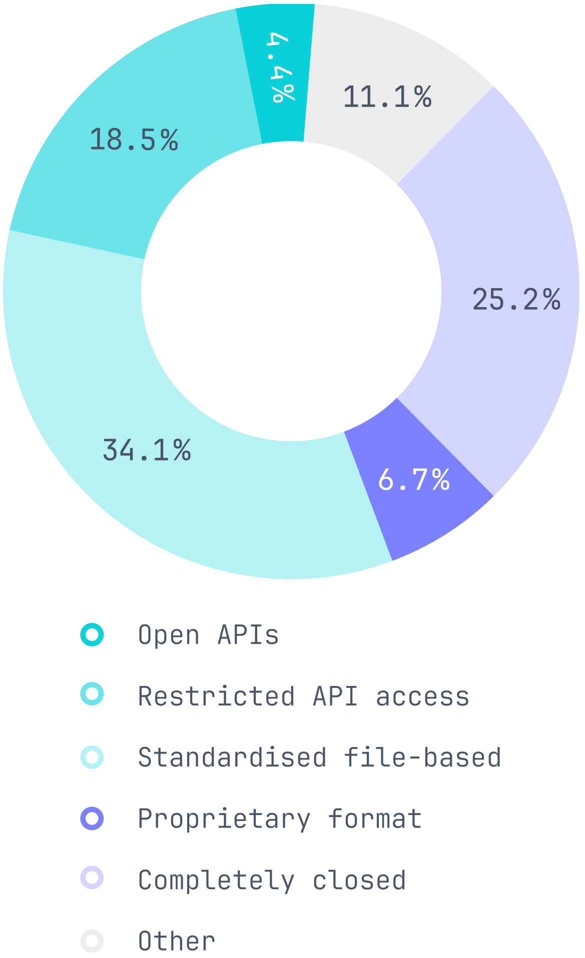
Data access remains tightly controlled and often constrained by legacy formats and siloed systems. Limited use of open APIs restricts the ability of authorities to enable dynamic, cross-team use of data and to support more advanced 3G and 4G suptech applications.

Most supervisory datasets are stored in file-based formats and are subject to restrictive access controls. Standardised file-based formats account for 34% of reported access methods, while 25% of data is described as being in completely closed systems, inaccessible even internally (Figure 111). Restricted APIs used for specific partners or use cases are available in 19% of cases. Open APIs – which would allow broader, auditable, and controlled reuse of supervisory data – remain rare at 4%.

A comparison between 2024 and 2025 shows only gradual change. Completely closed systems declined from 32% to 25%, suggesting that some siloed datasets are being integrated into more accessible environments. Standardised file-based formats decreased from 37% to 34%, while restricted APIs rose from 16% to 19%. Open API adoption increased only marginally from 2% to 4%.

FIGURE 111.

Data Accessibility



Limited adoption of modern access patterns constrains next-generation supervision. Real-time analytics, AI-assisted workflows, and cross-departmental collaboration require robust, well-governed API layers and shared data services. Some authorities like BOE are piloting internal APIs and data-fabric-style approaches to enable secure, traceable data flows. More broadly, progress will depend on upgraded infrastructure, clear interoperability policies, and capacity building to ensure that teams can safely exploit more open, service-based architectures.

4.7 Data analytics and data products

Analytical environments are built primarily around visualisation suites and general-purpose programming tools, with only selective uptake of advanced machine-learning platforms, investigative systems, or automation tooling. As a result, most authorities are still focused on descriptive reporting and ad hoc analysis, with relatively few having embedded scalable, repeatable analytics pipelines that can systematically inform risk-based supervision.

Analytical environments remain dominated by foundational tools, with only selective uptake of advanced, automated, or specialised platforms. This reflects a heterogeneous but still early-stage maturity profile across the sector.

Visualisation and reporting tools (such as Tableau or Power BI) are the most widely used category, reported by 61% of agencies (Figure 112). They play a central role in translating raw data into supervisory dashboards, scorecards, and standard reports. Programming languages and development environments (Python, R, Java, and similar) are used by 51% of authorities for custom analysis and model development.

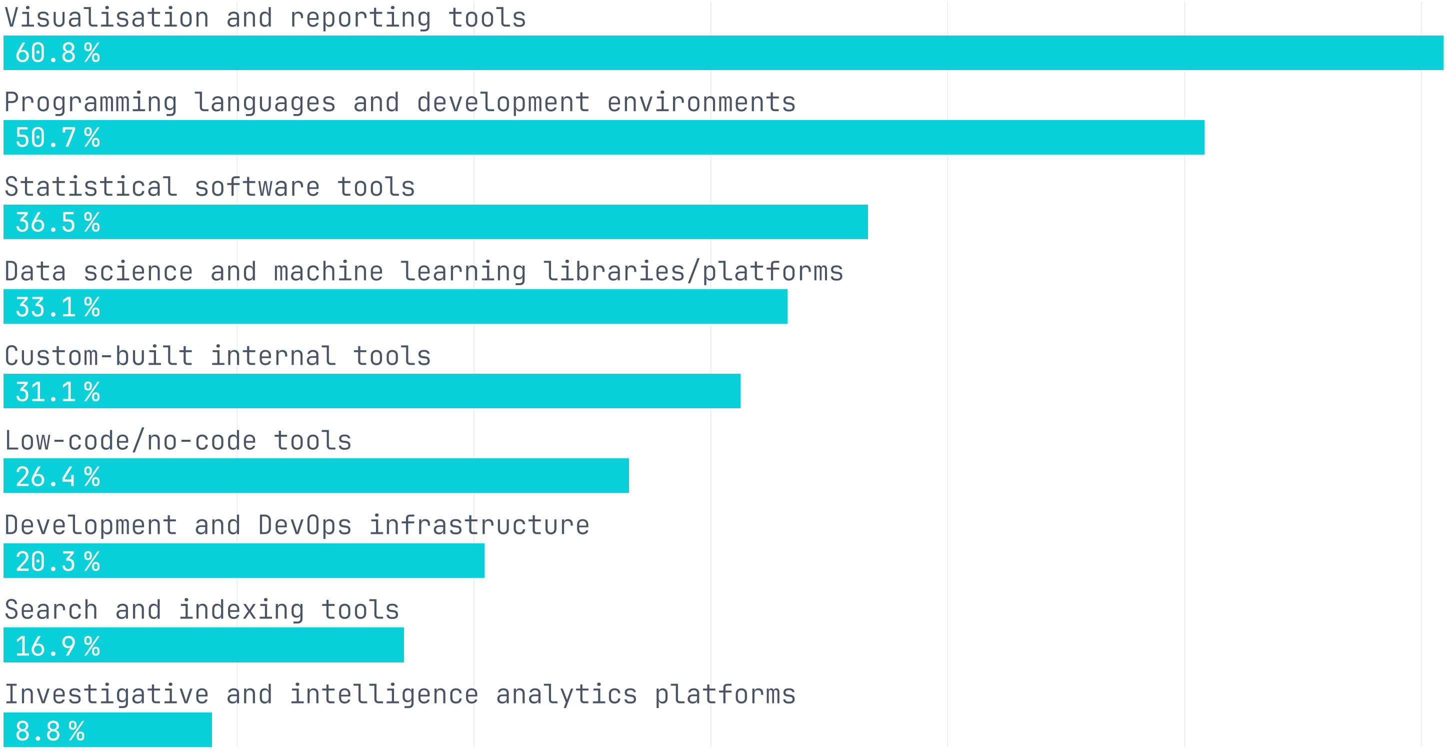
Traditional statistical software (e.g. Stata, SPSS) is used by 37% of agencies, while more modern data-science and machine-learning libraries or platforms (e.g. TensorFlow, PyTorch) are used by 33%. Around 31% of authorities report having built custom internal tools for specific supervisory use cases.

Tools that could significantly increase analytical throughput and automation are less widely adopted. Low-code or no-code tools are used by 26% of agencies, and development or DevOps infrastructure by 20%. Specialised investigative and intelligence platforms (such as goAML) are reported by only 9%, and search and indexing tools (e.g. Elasticsearch) by 17%.

Overall, authorities are still building out core analytical capabilities. The widespread use of visualisation suites and programming environments is a positive foundation, but limited adoption of more automated, scalable, or specialised platforms constrains the extent to which authorities can fully exploit growing data volumes or integrate advanced analytics and AI into day-to-day supervisory decision-making.

FIGURE 112.

Analytical Tools Used to Optimize Data Output



5.

The Tech in SupTech

The technological base of financial supervision in 2025 is defined by a tension between dependence on first- and second-generation tools and growing ambitions for advanced analytics and AI. Authorities are strengthening data and infrastructure layers while cautiously experimenting with 3G and 4G capabilities. The result is an ecosystem where task automation and workflow modernisation are advancing, but predictive analytics, generative AI, and complex business-intelligence environments remain far from mainstream. This section examines the underlying technology stack, AI and genAI adoption, the role of AI regulation, and emerging ethical and governance frameworks that shape how suptech evolves.

5.1 The technologies powering the digital transformation of financial supervision

Core supervisory processes continue to run on web portals, file servers, and template-based validation, while authorities express strong demand for APIs, automation, advanced analytics, and generative AI. Progress is incremental and path-dependent: most agencies are consolidating foundational systems before scaling higher-generation tools, and are prioritising capabilities that improve data quality and operational efficiency over more speculative AI applications.

Technology-specific year-on-year analysis for 2024–2025 shows a rebalancing away from complex analytics and towards task automation and targeted improvements in data collection and text processing. This suggests that authorities are consolidating operational gains and focusing on technologies that deliver immediate efficiency benefits, while large-scale big data and BI initiatives remain difficult to operationalise.

Supervisory agencies predominantly rely on earlier-generation tools while signalling clear aspirations to adopt more advanced technologies. Within the SupTech Generations 2.0 framework (see Survey scope and methodology), 1G and 2G capabilities still dominate daily operations, even as 3G and 4G tools become the focus of future investment plans.

First- and second-generation applications remain the backbone of most supervisory environments. Web portals are used by 74% of agencies, digital file-based report generation by 73%, template-based validation by 71%, and file servers by 70% (Figure 116). These tools are reliable for basic data ingestion and quality checks and have supported the transition away from purely manual processes. However, their future role is largely stabilising rather than expanding: only 29% of agencies express future demand for file servers and 24% for template-based validation, indicating that authorities see these capabilities as necessary but insufficient for modern, data-intensive supervision.

Third-generation technologies show more balanced patterns of current use and future demand, marking them as the main frontier for near-term modernisation (Figure 113). Push APIs are already used by 39% of agencies, with a further 47% expressing interest, while task automation tools are used by 38% and desired by 49%. Cloud databases are deployed by 33% of agencies and wanted by 41%, reflecting growing recognition of their cost and collaborative advantage despite persistent legal, security, and legacy-IT constraints. Dynamic visualisation tools are used by 32% and desired by 37% as agencies move from static reporting to more interactive, real-time decision

FIGURE 113.

Underpinning Technologies Used By Agencies To Enable Supervisory Processes

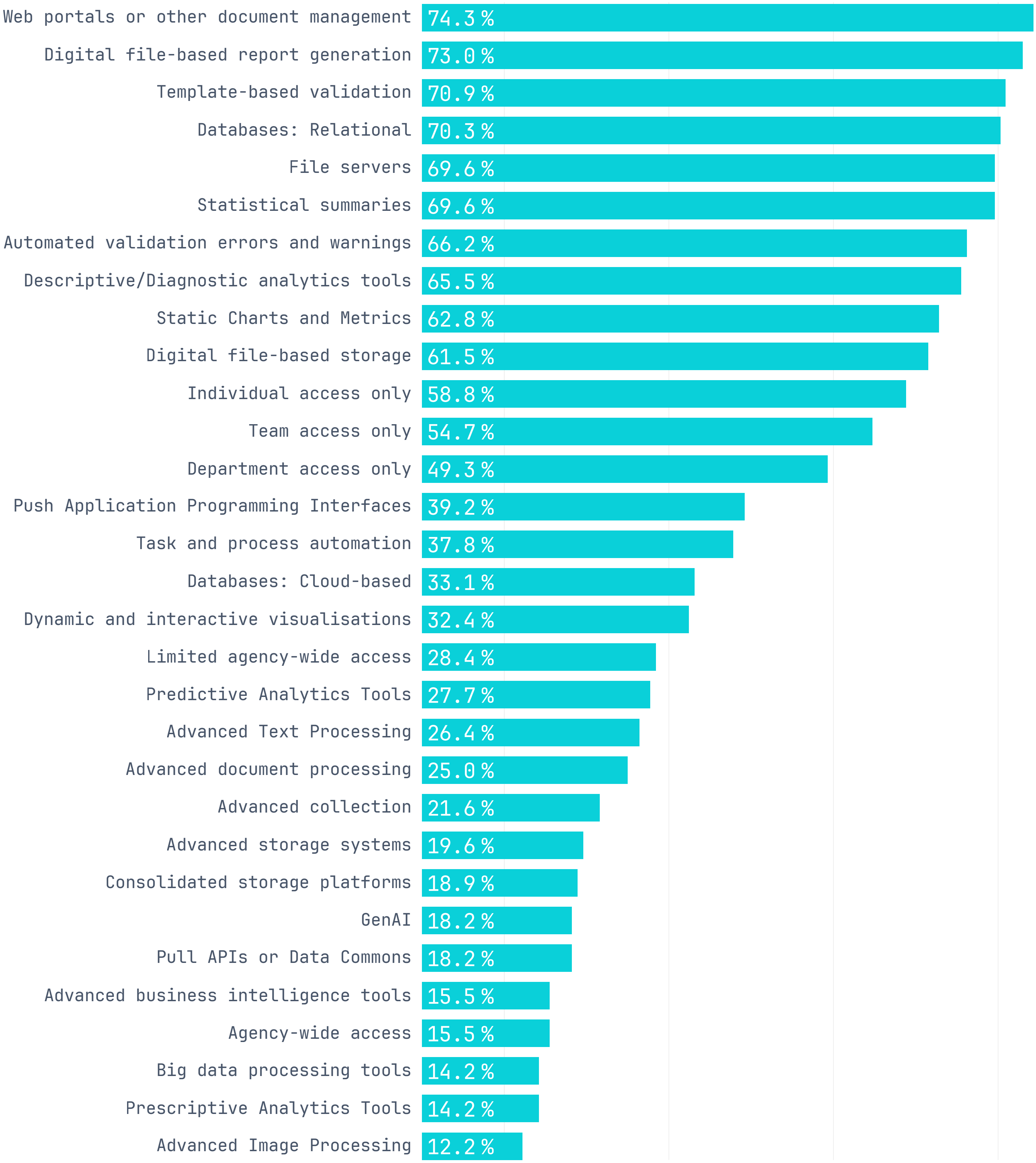
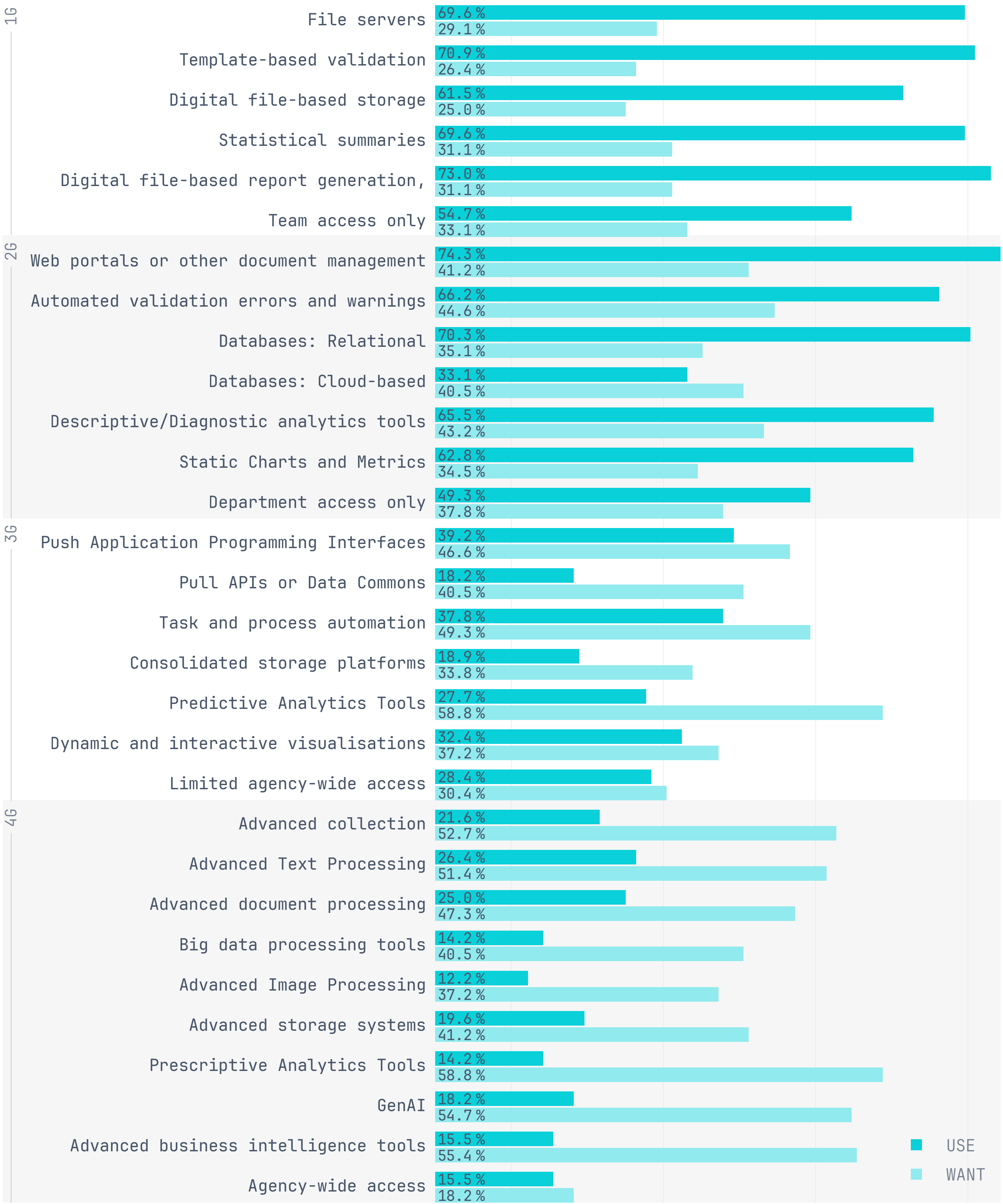


FIGURE 114.

Underpinning Technologies Used Versus Desired By Agencies To Enable Supervisory Processes By SupTech Generation



support. Predictive analytics stand out: 28% report current use, but 59% express demand, making this the most prominent 3G capability where ambition clearly exceeds current deployment.

Fourth-generation technologies display the largest gaps between aspiration and implementation. Advanced business-intelligence platforms are used by only 16% of agencies but desired by 55%. Generative AI follows a similar pattern, with 18% of agencies reporting current use but 55% expressing demand. Advanced text-processing tools for unstructured data (often a prerequisite for effective genAI) are used by 26% and wanted by 51%. By contrast, prescriptive analytics have the lowest uptake at 14%, reflecting the complexity of embedding model outputs directly into decision-making and workflow orchestration. Across these tools, the common constraint is not only computational capacity but also data readiness, integration with legacy systems, and the need for robust governance and skills.

Looking forward, agencies' stated ambitions confirm a stepwise, pragmatic approach to digital transformation. Authorities are not attempting to leap directly from manual processes to fully AI-enabled supervision. Instead, they are reinforcing foundational layers – improving data quality, expanding API-based ingestion, and automating repetitive tasks – before scaling predictive, prescriptive, and generative AI capabilities. This sequencing is broadly consistent with the data-governance and data-stack gaps identified in Section 4 and suggests that advanced 4G capabilities will remain contingent on sustained investment in underlying infrastructure.

The analysis of changes in underlying technologies between 2024 and 2025 reveals a volatile landscape, with several reversals compared with 2023–2024 trends (Figure 115). Agencies appear to be shifting from broad experimentation towards selective implementation of tools that improve day-to-day operations.

Task automation is the clearest success story, registering a 12% growth after near stagnation in the previous period. This aligns with agencies' stated priorities around workload reduction, standardisation of repetitive tasks, and freeing specialist staff for higher-value analytical work. Advanced collection tools also rebounded strongly, with a 12% while advanced text-processing and natural language processing gained 5%, recovering from earlier declines as authorities began to address unstructured-data bottlenecks identified in Section 4.

By contrast, big data tools recorded a 15% decline and advanced business-intelligence platforms continued their downward trajectory with a further 6% drop. These patterns suggest persistent implementation challenges for complex analytical environments that require significant integration, data-engineering capacity, and sustained governance attention. Generative AI adoption edged down slightly after a sharp initial surge, indicating that early enthusiasm is being tempered by the realities of model integration, control, and resourcing.

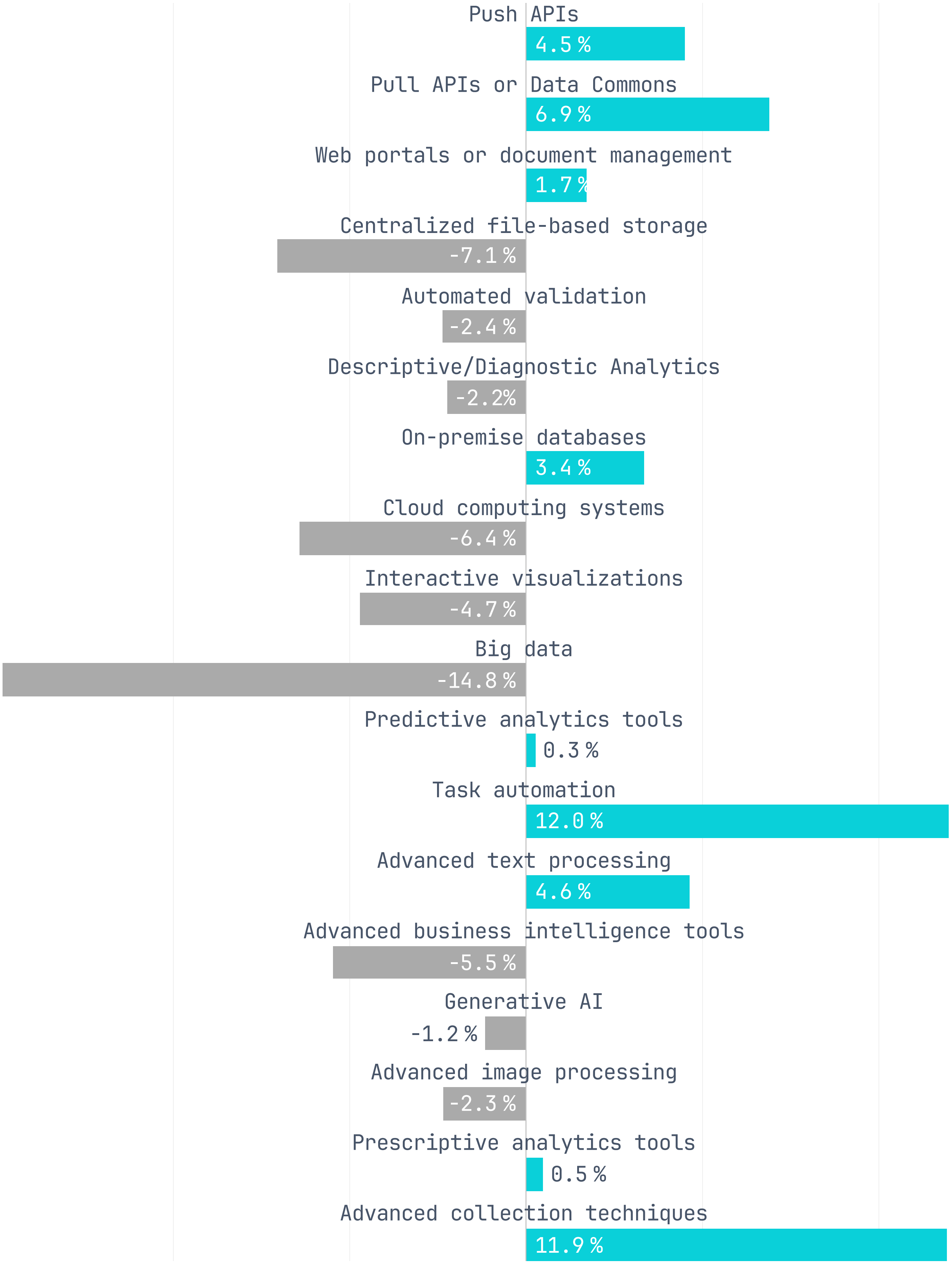
On the infrastructure side, a modest increase in on-premise databases points to a move towards hybrid architectures rather than rapid, wholesale migration to the public cloud. Overall, the data portray a sector that, in 2025, concentrated on consolidating basic automation and improving data flows, while encountering greater difficulty in scaling big data and advanced BI systems.

SupTech Generations Index: Regional evolution of suptech maturity

The SupTech Generations Index provides a cross-sectional view of how far authorities have moved along the technology spectrum. Results for 2025 show most agencies operating in the 2G–3G band, with

FIGURE 115.

Underpinning Technologies Used By Agencies To Enable Supervisory Processes 2024–2025



notable regional variation and substantial heterogeneity within regions. The index captures the composition of deployed tools rather than outcomes, and should be read as a snapshot of digital maturity rather than a linear ranking of supervisory effectiveness.

To assess the technological maturity of supervisory authorities, we apply the Suptech Generations 2.0 Framework to compute an "average suptech generation" score for each agency (Figure 116). This index, ranging from 0 to 4, estimates the sophistication of an authority's supervisory technology environment based on the mix of tools currently in use. It reflects the technologies deployed, not their effectiveness or integration.

Each technology reported by an authority is mapped to a generation category (0G to 4G). The agency-level indicator is the weighted average of these categories. For example, an authority using an AI-enabled chatbot (4G) and an automated reporting dashboard (2G) would score 3. Another using manual submissions (0G), a 1G web portal, and a 2G push API would score 1. Intermediate and lower-generation tools continue to serve essential functions: AI and other advanced applications depend heavily on reliable data ingestion, validation, and governance mechanisms often delivered through 1G–2G infrastructure.

CROSS-SECTIONAL RESULTS FOR 2025

The 2025 dataset includes 105 financial authorities. Regional profiles reveal meaningful variation in technological maturity, shaped by institutional capacity, investment patterns, digital infrastructure, and the breadth of supervisory mandates.

FIGURE 116.

Regional Trends In SupTech Maturity: Average Generation Index By Region

	AVERAGE GENERATION
East Asia & Pacific	2.13
Europe & Central Asia	2.25
Latin America & Caribbean	2.02
Middle East & North Africa	2.02
North America	2.36
South Asia	1.82
Sub-Saharan Africa	1.73
Global	2.04

Europe and Central Asia (ECA) reports the highest regional maturity with an average generation score of 2.25 across 29 authorities. This suggests relatively broad deployment of 2G–3G capabilities and selective experimentation with AI-enabled tools.

- **North America** also exhibits high maturity at 2.36, reflecting established infrastructures, but the small sample size limits generalisation.
- **East Asia & Pacific (EAP)** shows strong adoption momentum, with an average score of 2.13. Many agencies in the region have invested in modern data infrastructure and workflow automation.
- **Latin America & the Caribbean (LAC)** and **Middle East & North Africa (MENA)** both show comparable maturity levels (2.02), indicating broad uptake of foundational tools with emerging adoption of advanced analytics.

- **South Asia** registers 1.82, a moderate level of maturity reflecting foundational investments with early-stage AI experimentation.
- **Sub-Saharan Africa (SSA)** registers 1.73, demonstrating strengthening adoption of 1G–2G infrastructures and selective deployment of more advanced tools.

At the global level, the 2025 average generation score stands at 2.04, indicating that most authorities have progressed beyond basic digitalisation and are transitioning toward intermediate digital capabilities, notably automated validation, dashboards, data querying tools, and early-stage machine-learning applications. Yet the distribution shows substantial heterogeneity across regions and within them, reflecting uneven institutional capacity, resource constraints, and varying supervisory mandates.

INTERPRETATION AND LIMITATIONS

The 2025 results should be interpreted as a snapshot of global supervisory digital maturity, not as a linear measure of progress. Because the score reflects the portfolio of tools currently deployed, it may capture peak investment cycles, ongoing modernisation programmes, or transitional phases where foundational systems are being upgraded.

A higher average generation score does not directly imply stronger supervisory outcomes. Many 3G–4G tools are effective only when supported by high-quality data, stable infrastructure, and strong governance—areas where 1G–2G tools are indispensable. Conversely, authorities with lower scores may be consolidating foundational infrastructure before advancing to more sophisticated capabilities.

Future iterations of the index will be strengthened through greater methodological consistency, enhanced metadata on tool integration and use intensity, and more granular tracking of how supervisory outcomes evolve as agencies reconfigure their technological architectures.

5.2 AI in suptech

AI adoption in suptech remains at an early stage, with most authorities still exploring use cases or piloting applications. Advanced economies are starting to embed AI into supervisory workflows, while many emerging markets are constrained by infrastructure, skills, and data quality. Across all regions, the main barriers are not compute capacity but privacy, integration, and governance.

Artificial intelligence is changing financial supervision from primarily retrospective compliance checking to more proactive, data-driven oversight. AI technologies help address three structural challenges: rapidly growing data volumes from digital financial services, increasingly complex market structures, and the need for timelier identification of emerging risks. Authorities documented by the BIS and the IMF now use AI to automate routine monitoring, detect market manipulation, and spot early signs of systemic stress.

Applications span foundational and advanced functions. Natural language processing is used to process large volumes of regulatory submissions, supervisory correspondence, and public disclosures. Machine-learning models support risk-based surveillance by prioritising cases, flagging anomalies in transactional or market data, and predicting credit deterioration or operational fragility. Central banks and supervisors are experimenting with AI for real-time transaction monitoring, anomaly detection in trading patterns, and automated assessments of thematic risks. Evidence from initiatives such as the Banca d'Italia's work on AI/ML for data management and the BIS's Project Aurora on anti-money-laundering surveillance points to significant efficiency gains and reductions in false positives, although benefits remain context-specific and contingent on data quality and governance.

At the same time, these advances create new supervisory challenges. AI systems can introduce or amplify bias, are often difficult to interpret, and may encourage over-reliance on automated outputs. Authorities must therefore develop governance frameworks ensuring that AI used both by supervised entities and by supervisors themselves is secure, reliable, privacy-compliant, transparent, and aligned with regulatory objectives. Trustworthy AI in supervision is not only a technical challenge but also an organisational one, requiring clear accountability structures, robust validation and testing, and sustained investment in skills.

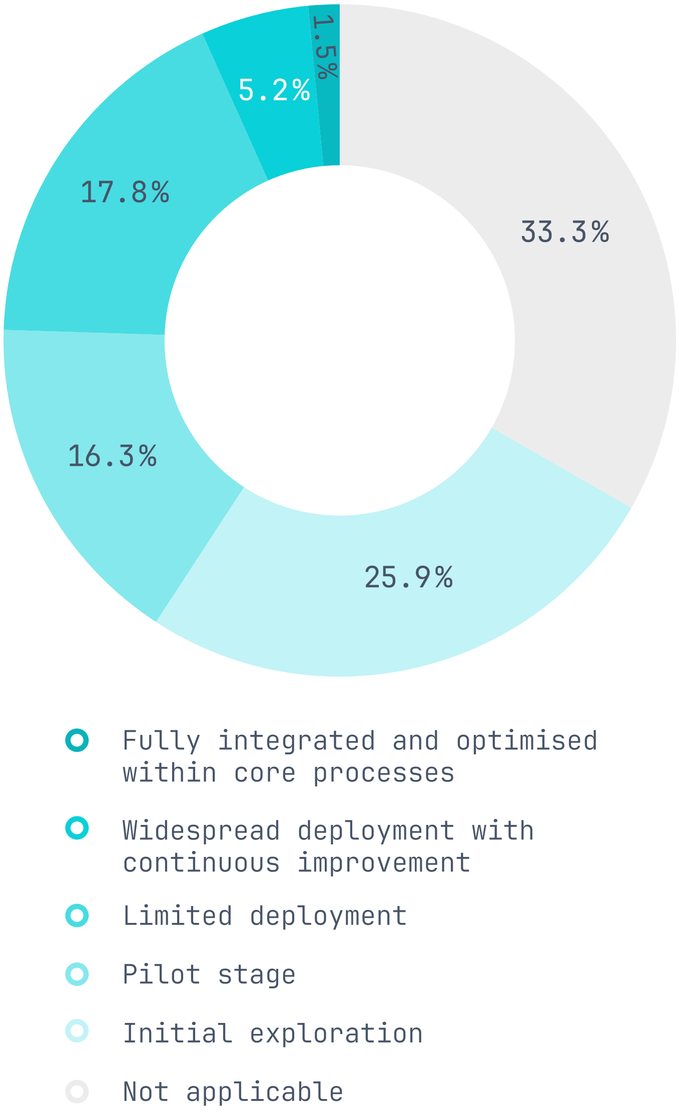
5.2.1 Current state of AI maturity

The maturity of AI implementation in suptech remains limited. In 2025, 33% of agencies report that AI is not yet applicable to their work, and a further 26% are still in initial exploration (Figure 117). Active deployment is concentrated in early stages: 16% report pilots, 18% limited deployment, and 5% widespread deployment. Only 2% of authorities describe AI as fully integrated into core supervisory processes. This distribution confirms a significant gap between recognised potential and operational reality.

Economic classification reveals a pronounced divide (Figure 118). Advanced economies report higher deployment levels: 40% indicate limited deployment, 24% widespread deployment with continuous improvement, and 4% full integration. Emerging markets and developing economies (EMDEs) are earlier in the adoption curve, with 38% describing AI as not applicable, 30% in exploration, and 17% in pilot stages; only 13% report limited deployment, and widespread or fully integrated use is extremely rare. This gap reflects differences in digital infrastructure, resourcing, and access to specialised talent, and raises concerns about potential regulatory divergence.

FIGURE 117.

Maturity Level Of AI Implementation Within The Agency's SupTech Applications



Regional patterns reinforce this picture (Figure 119). North America and parts of East Asia & Pacific and Europe are moving towards more embedded AI, supported by established data infrastructures and targeted innovation programmes. Regions such as South Asia, Sub-Saharan Africa, Latin America & the Caribbean, and MENA remain largely in exploration or pilot phases, although pilot activity is expanding and laying the groundwork for more mature AI use.

FIGURE 118.

Maturity Level Of AI Implementation Within Your Agency's SupTech Applications By Economic Classification

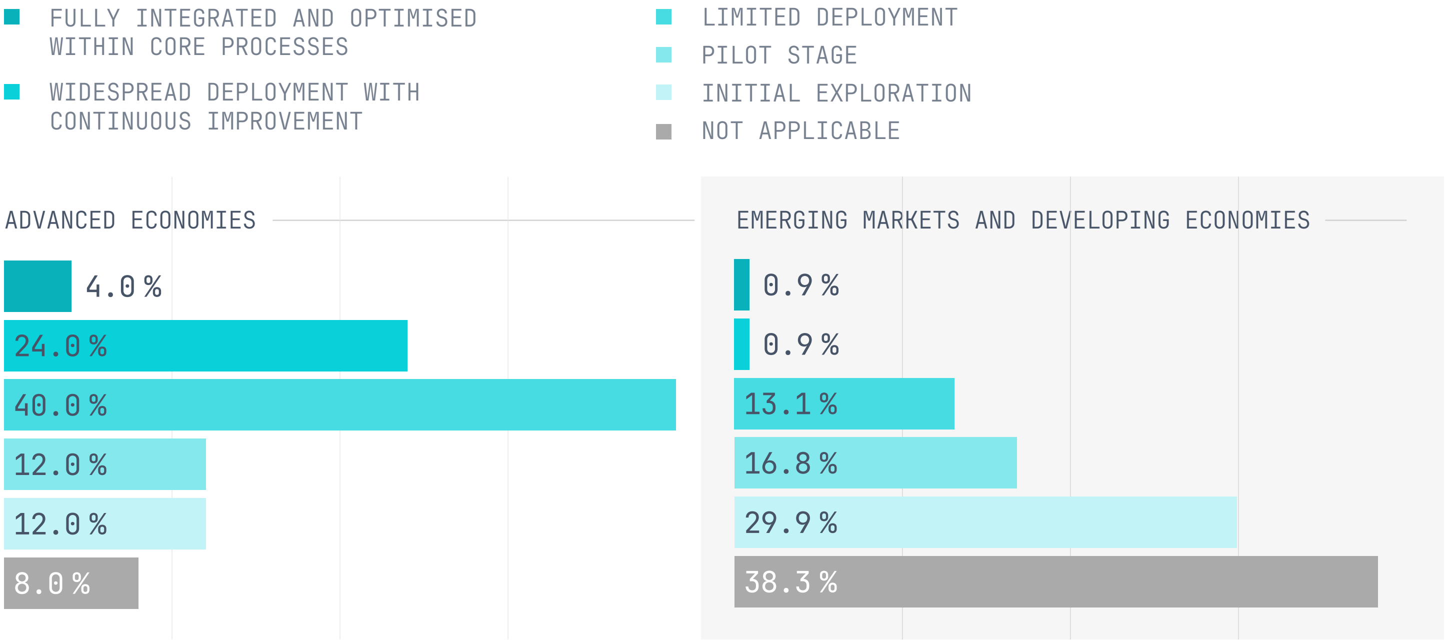
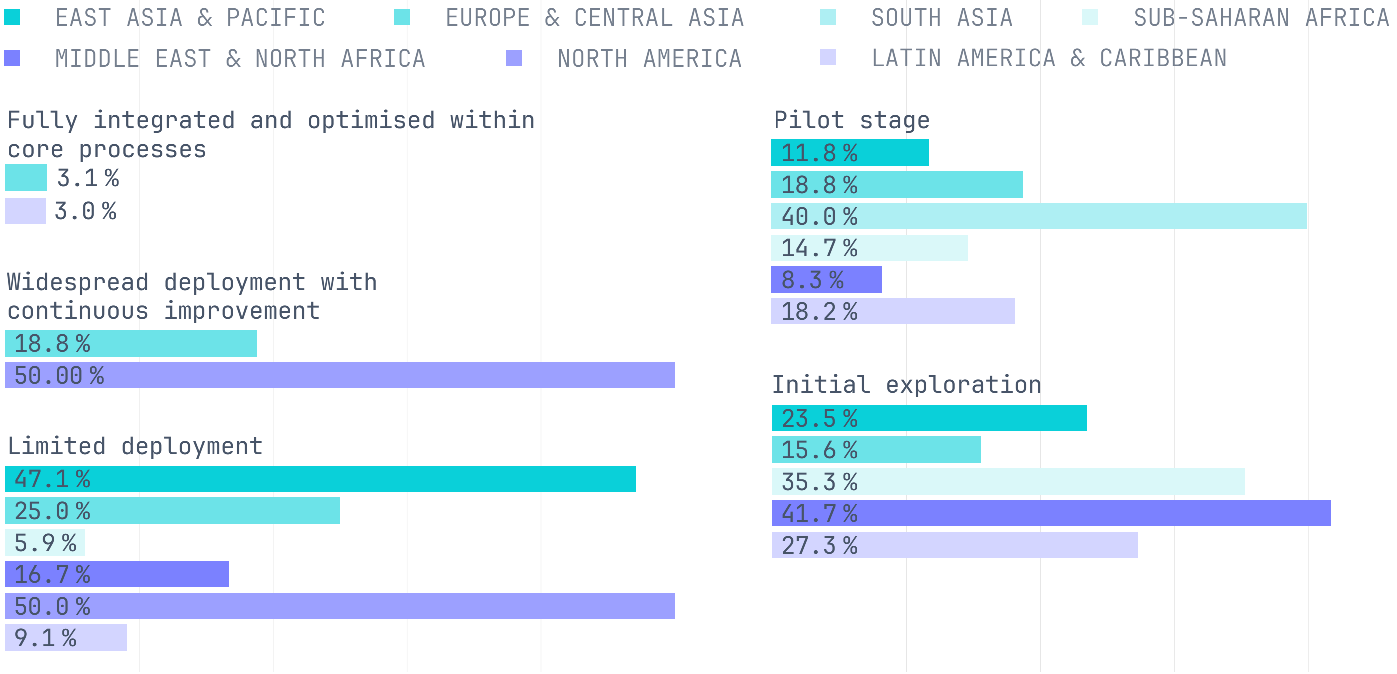


FIGURE 119.

Maturity Level Of AI Implementation Within Your Agency's SupTech Applications By Region



5.2.2 Development approaches and data sources

Development strategies for AI in suptech are predominantly internal. Around 26% of agencies rely on in-house data-science or analytics teams, and 17% combine internal development with external support from consultants or secondees (Figure 120). Foundation models and large language models are adapted to supervisory use by 18% of agencies, while 14% use vendor-provided proprietary models and 12% adapt open-source models. Collaborations with academia, research institutions, or cross-agency partnerships each account for about 2%, indicating that structured external collaboration remains limited.

Data sources for AI and genAI models are largely traditional supervisory datasets. Regulatory and supervisory returns are used by 31% of agencies, and internal supervisory case files by 22% (Figure 121). Web-scraped or open-web data (18%) and transactional data (17%) supplement these core sources. Third-party commercial datasets (7%), open-data portals (5%), synthetic data (2%), and alternative sources such as sensor or geospatial data (2%) are far less common. This reliance on conventional data streams underscores how closely AI adoption is tied to existing data-governance and reporting frameworks.

5.2.3 AI applications and regional priorities

Text analysis and predictive analytics are currently the leading AI applications in suptech, each reported by 23% of agencies (Figure 122). Other common use cases include automated regulatory reporting (17%), AI-enabled customer service (14%), and risk profiling or scoring (12%). Less prevalent but growing applications include real-time decision support (11%), transaction monitoring (10%), reasoning and knowledge-

FIGURE 120.

Primary Approach To AI/ML Model Development And Maintenance

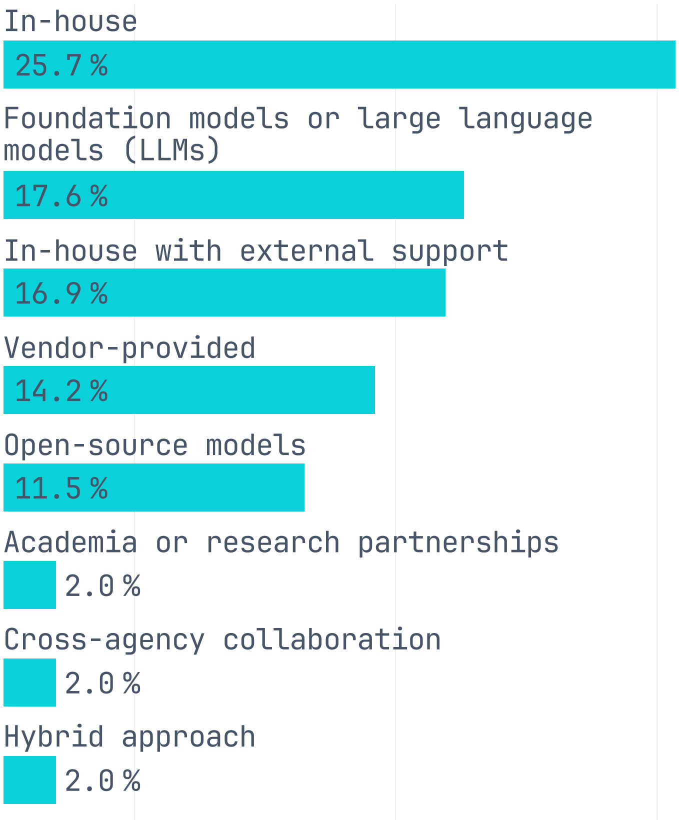


FIGURE 121.

Primary Data Sources For AI/GENAI Models In SupTech Applications

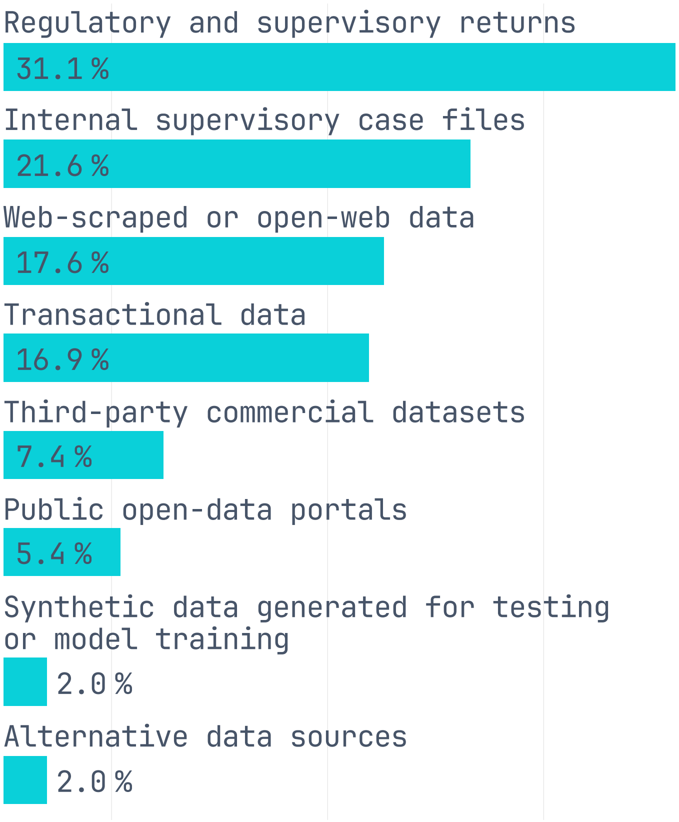
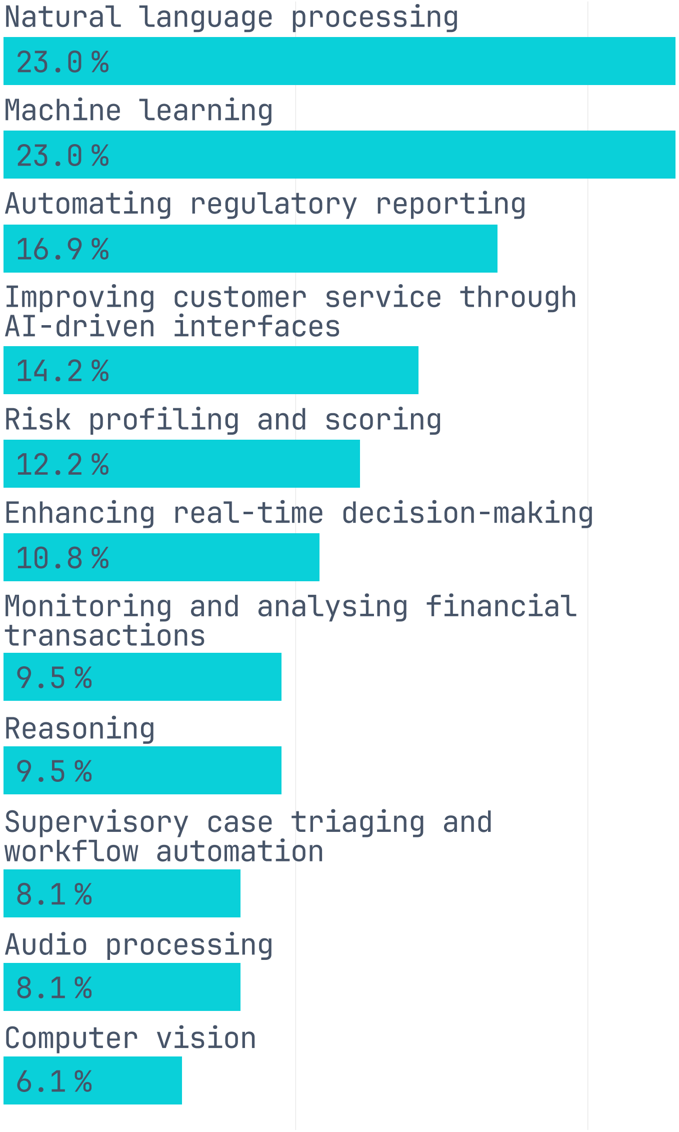


FIGURE 122.

Primary Applications Of AI In SupTech Activities



retrieval tasks (10%), supervisory case triaging and workflow automation (8%), audio processing (8%), and computer vision (6%). Compared with 2024, the centre of gravity has shifted towards operational and consumer-facing functions, while core NLP and ML capabilities remain important but less dominant.

Regional priorities differ. Sub-Saharan Africa places greater emphasis on AI for customer service, text analysis, and predictive analytics. Latin America and North America report stronger use of machine learning and audio processing; East Asia & Pacific prioritises reporting automation and customer service; Europe & Central Asia and South Asia concentrate on NLP, ML, and regulatory reporting automation, with South Asia at an earlier stage; and MENA primarily targets NLP and reporting automation (Figure 123). These patterns reflect differing supervisory mandates, data infrastructures, and market structures.

5.2.4 Challenges to AI deployment

Across regions, the leading barriers to AI deployment relate to governance and human factors rather than pure technology. Data protection, privacy, and security concerns are cited by 30% of agencies (Figure 124). Employment and skills implications follow at 22%, and system-integration challenges at 20%. Explainability and “black-box” concerns (18%) and governance and accountability issues (17%) also feature prominently. Between 2023 and 2025, the relative importance of basic data-quality and model-training challenges has declined, while concerns over integration, external vendor relationships, and regulatory alignment have grown (Figure 125). This shift suggests that many authorities are moving beyond initial experimentation to confronting the organisational and ecosystem implications of AI.

Advanced economies report higher levels of concern across most categories, reflecting their more intensive AI use (Figure 126). Around 61% of AEs cite data-protection and privacy as major constraints, compared with 23% of EMDEs. AEs also report more challenges around skills, explainability, and governance, consistent with their more advanced deployment stages. EMDEs report lower levels of concern but also lower levels of actual use, indicating that foundational capacity building, not regulation, remains the primary constraint.

FIGURE 123.

Primary Applications Of AI In SupTech Activities By Region

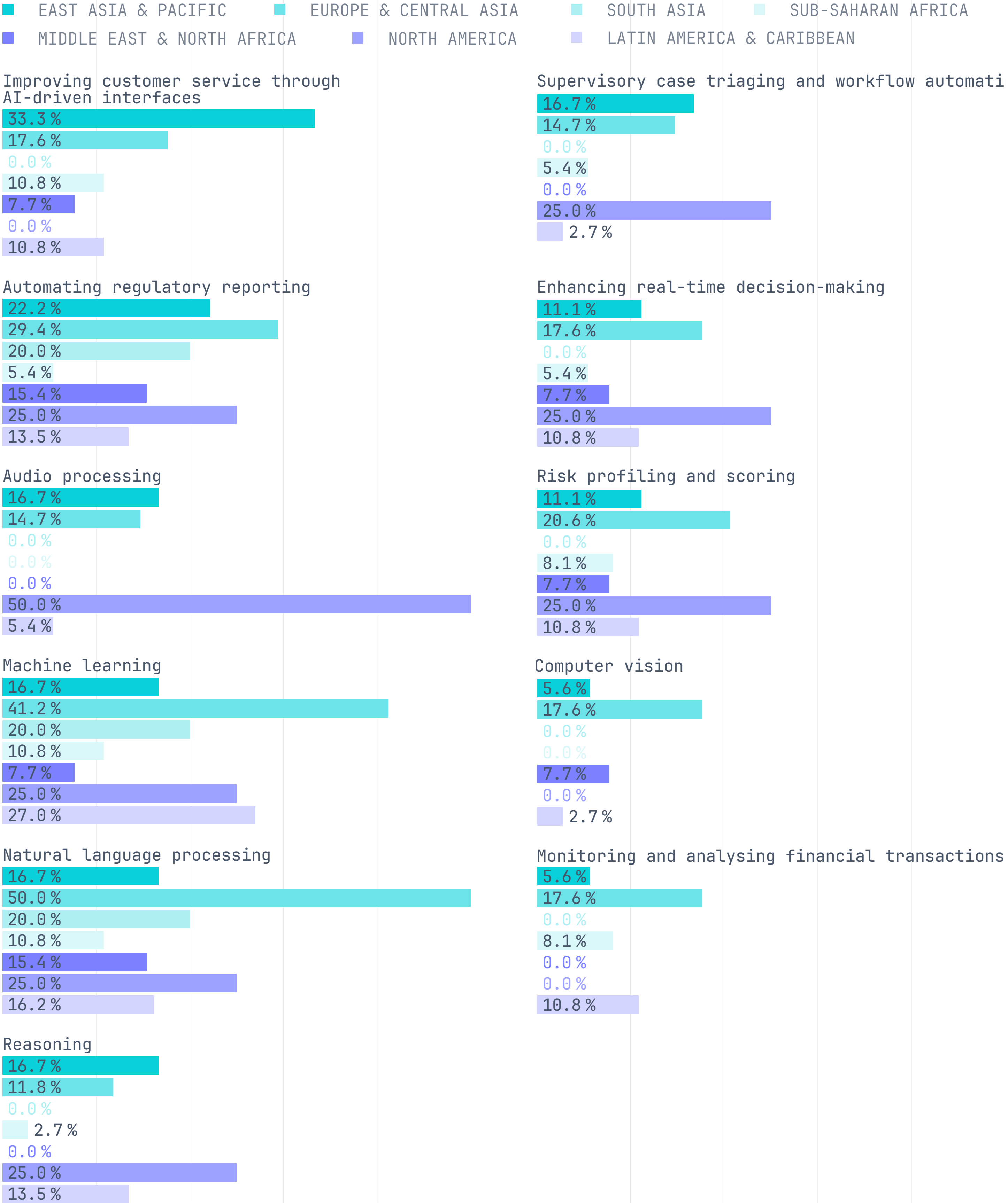


FIGURE 124.

Challenges In The Deployment Of AI

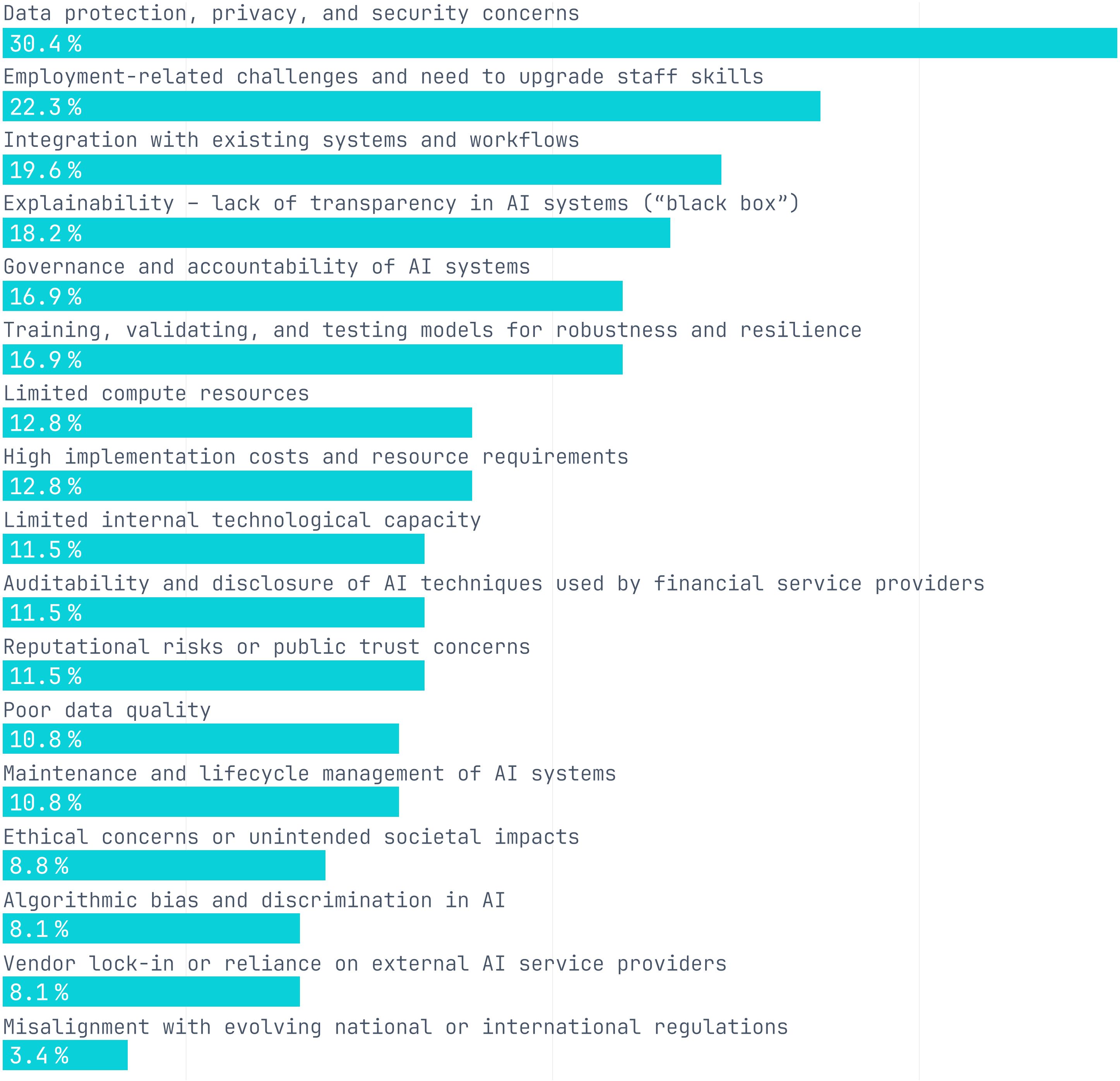


FIGURE 125.

Challenges In The Deployment Of AI 2023–2025

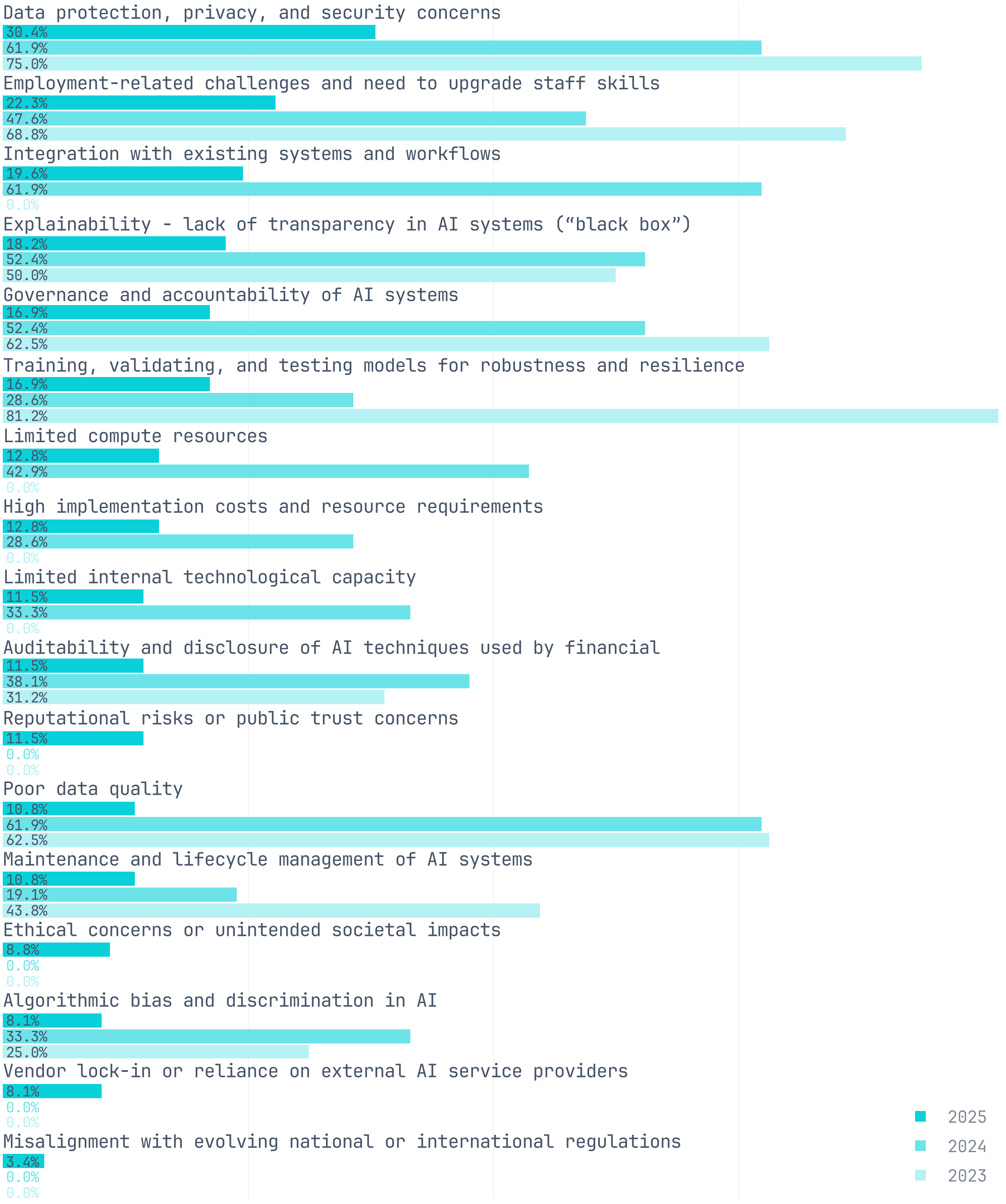
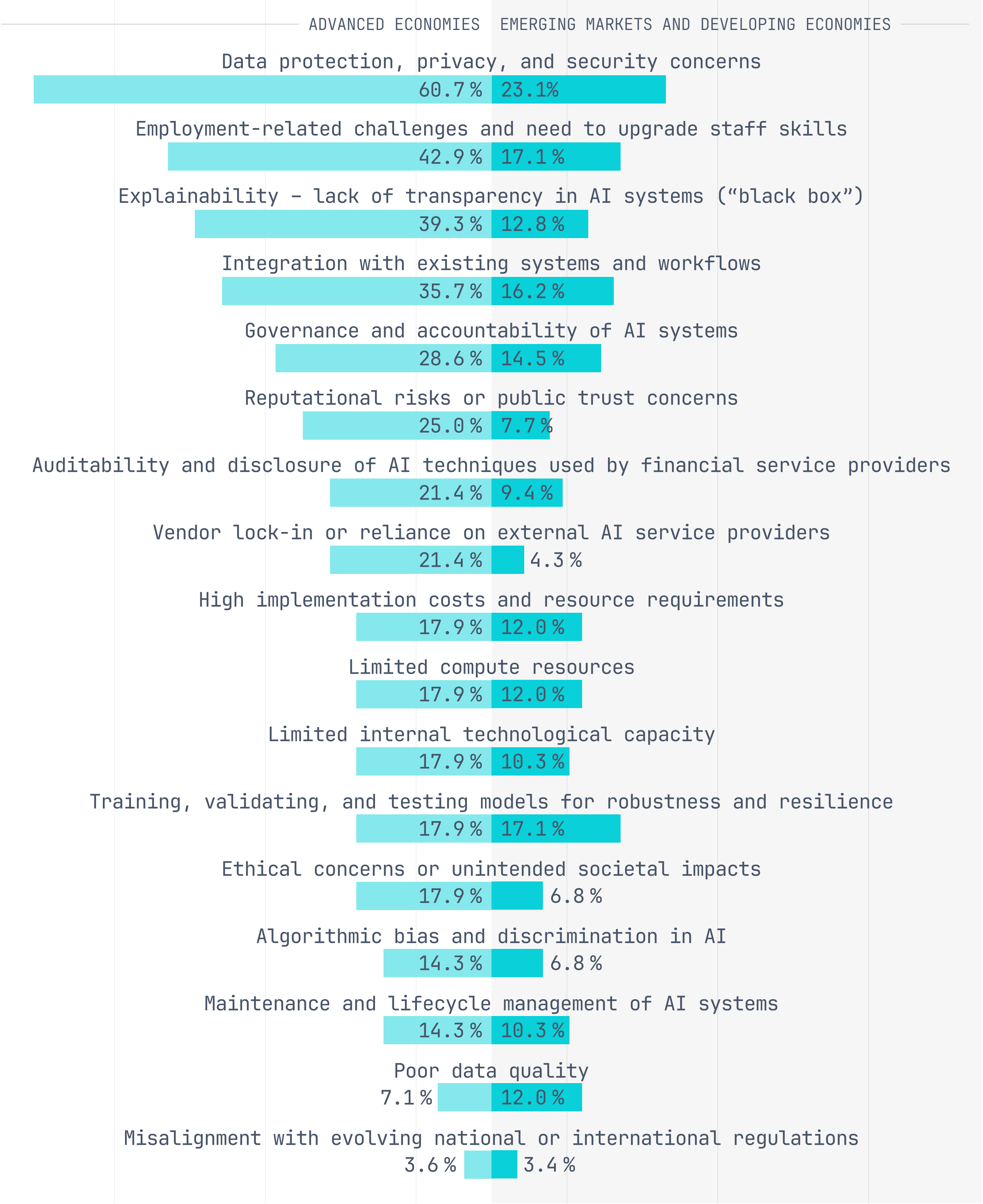


FIGURE 126.

Challenges In The Deployment Of AI By Economic Classification



5.3 GenAI in financial supervision

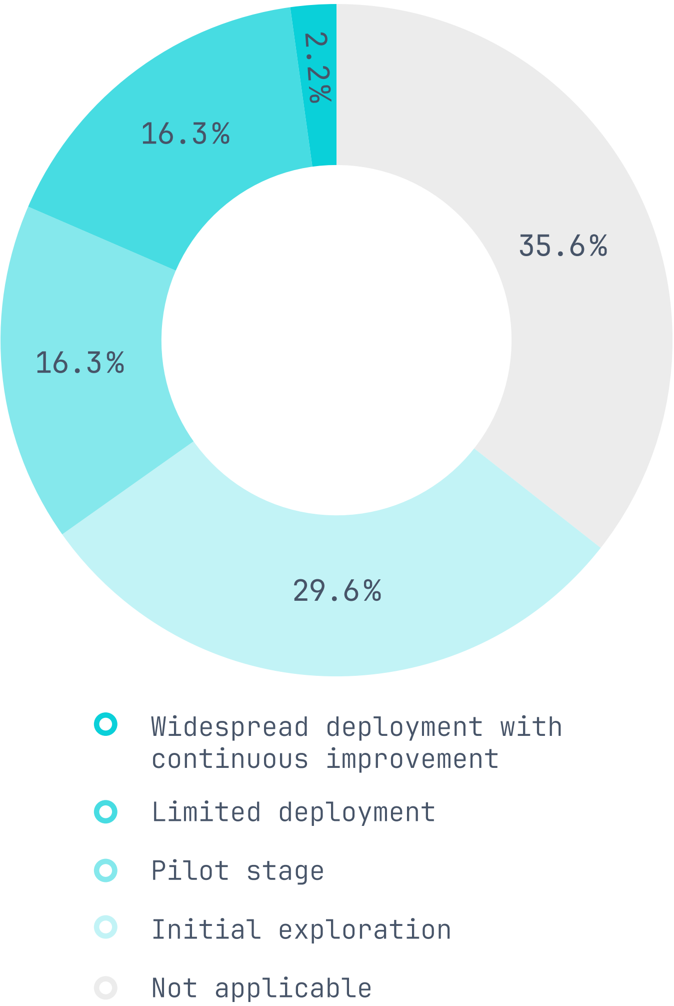
Generative AI is beginning to move from concept to targeted pilots in financial supervision, mainly in document analysis, compliance review, and internal knowledge support. Adoption remains cautious and uneven, with advanced economies leading deployments and most authorities treating genAI as an augmentative tool rather than a replacement for supervisory judgement.

GenAI represents the frontier of AI use in supervision, particularly suited to processing and synthesising large volumes of unstructured text. Unlike traditional AI, which primarily classifies or predicts, GenAI can draft summaries, generate guidance, support scenario analysis, and operate as a conversational interface to complex datasets and rulebooks. These capabilities have attracted significant regulatory interest, given their potential to reduce manual workload and broaden access to specialist knowledge within supervisory agencies.

Despite this potential, the maturity of GenAI in suptech remains low. In 2025, 36% of surveyed authorities consider GenAI not yet applicable to their work, and 30% are still in initial exploration (Figure 127). Active implementation is limited: 16% of agencies report pilots and another 16% limited deployment, while only 2% describe widespread deployment with continuous improvement. No authority reports full integration into core processes. Compared with 2024, the share in initial exploration has fallen (from around half to 30%) and the combined share in pilot or limited deployment has increased modestly, indicating gradual but measured progression towards operational use rather than rapid scaling.

FIGURE 127.

Assessing Maturity Levels In GenAI Implementation For SupTech Applications

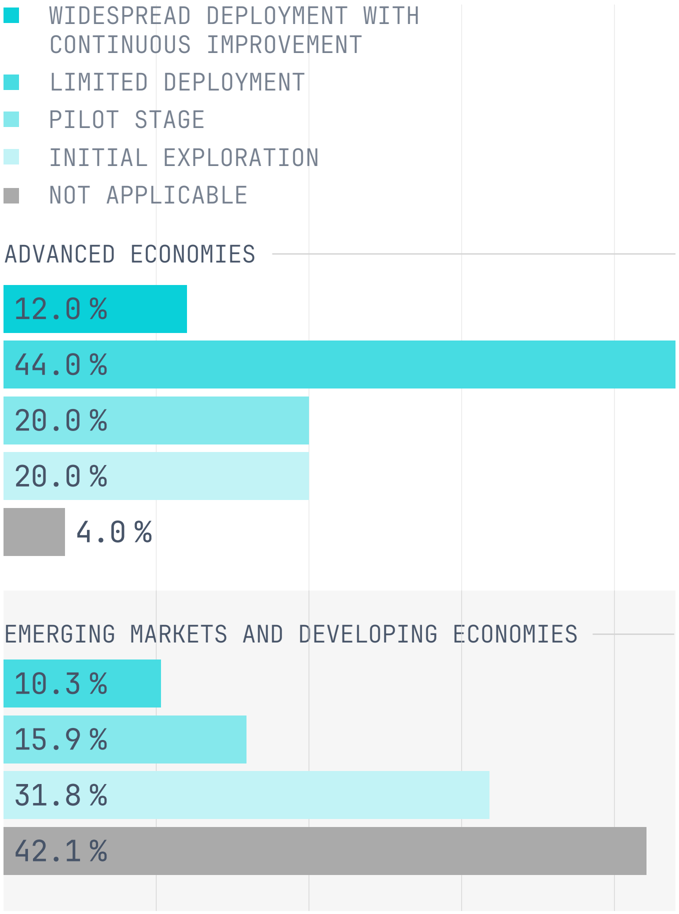


Economic classification again reveals a clear divide (Figure 128). Advanced economies report 44% in limited deployment and 12% in widespread deployment, while only 4% consider genAI not applicable. EMDEs, by contrast, show 42% non-applicability and are concentrated in exploration (32%) and pilot stages (16%), with very limited deployment. This pattern reflects underlying differences in infrastructure, resourcing, and regulatory priorities.

Authorities' public communications and annual reports indicate a growing portfolio of GenAI experiments. The Bank of Thailand's data co-pilot enables supervisors to query credit databases in natural language; Belgium's FSMA has tested LLM-based tools for ESG disclosure analysis; Bank Negara Malaysia and the Bank of Latvia use GenAI to assist in reviewing compliance reports and securities prospectuses; the HKMA, De

FIGURE 128.

Assessing Maturity Levels In GenAI Implementation For SupTech Applications By Economy



Nederlandsche Bank, the Bank of Namibia, and Austria's FMA are all exploring or deploying LLM-based assistants for document analysis, model review, and supervisory data exploration. Across these cases, GenAI is used to augment human analysis, with staff retaining responsibility for decisions and outputs.

Stock-taking work by the BIS and others highlights that GenAI tools are typically discretionary aids rather than embedded decision engines. User acceptance, quality control, and occasional inaccuracies limit the scope of automation, while privacy, security, and integration issues require robust safeguards. As a result, authorities are prioritising use cases where benefits are clear, data are well-controlled, and outputs can be systematically checked.

Overall, GenAI in financial supervision is progressing, but at a cautious pace. Authorities are focusing on targeted, high-value applications and building governance, skills, and infrastructure in parallel. The trajectory suggests that GenAI will become an increasingly important component of the supervisory toolkit, but only where it can be aligned with transparency, accountability, and human-in-the-loop principles.

5.4 AI regulations and suptech

AI regulations are beginning to shape suptech strategies, but their influence is uneven and often indirect. A small group of authorities is actively using AI governance debates to steer their own technology choices, while many others see limited impact or remain unsure how evolving frameworks will affect their adoption plans.

The regulatory landscape for AI in financial services is evolving rapidly. Supervisory authorities must design frameworks that govern AI use by regulated entities while also determining how those same frameworks apply to their internal adoption of AI-enabled suptech. CGAP estimates that, as of early 2025, at least 116 jurisdictions have adopted national AI strategies, but only around 50 have issued AI-specific guidance for financial institutions. Horizontal regimes such as the EU AI Act, sectoral guidelines from central banks and conduct regulators, and cross-cutting principles from bodies such as the OECD are beginning to influence how authorities think about AI safety, fairness, and accountability.

Survey results suggest that the direct impact of AI regulations on suptech strategies is still modest and fragmented (Figure 129). Only 10% of authorities report that AI regulations are accelerating their adoption by providing a clear, enabling framework. Around 7% say regulations hinder adoption, citing overly strict provisions, ambiguity, or underdeveloped guidance. The largest single group (16%) reports minimal impact because they currently make limited use of AI; for these agencies, basic capability building and data-governance challenges dominate. Another 16% are unsure about the regulatory impact, underscoring the novelty of many AI frameworks and the difficulty of mapping them onto internal supervisory use.

More proactive approaches are emerging. Fourteen percent of authorities report shaping AI principles or guidelines that directly influence their suptech strategies, and 10% collaborate with national or international bodies to align AI and suptech approaches. These agencies are not only responding to external regulation but also acting as co-designers of governance frameworks, aiming to ensure that supervisory AI use is consistent with, and sometimes helps define, broader market rules.

Advanced economies display higher levels of engagement and more complex regulatory effects (Figure 130). Around 32% of AEs are directly shaping AI principles relevant to their

FIGURE 129.

Influence Of AI Regulations On Agency Strategies For SupTech Adoption

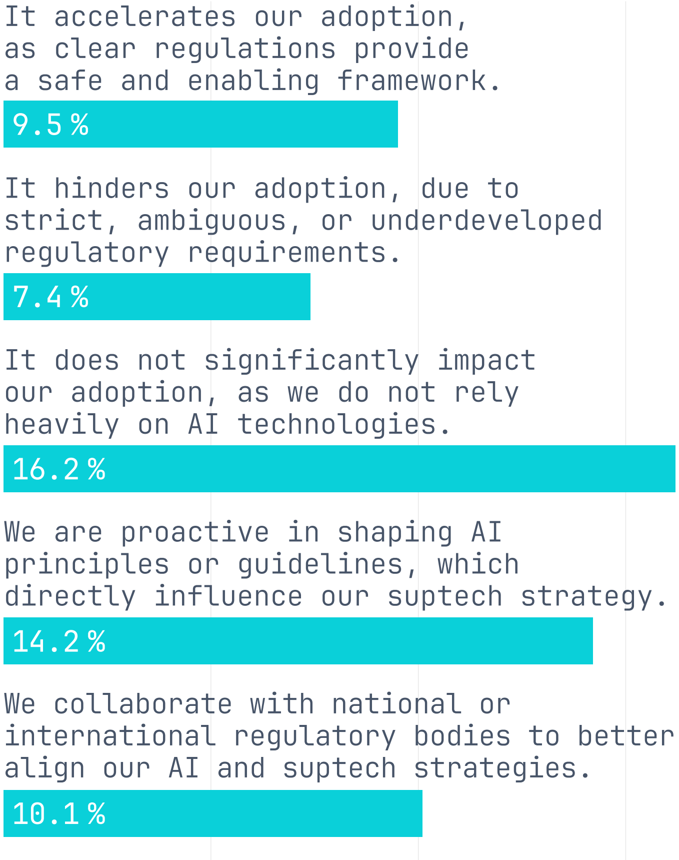
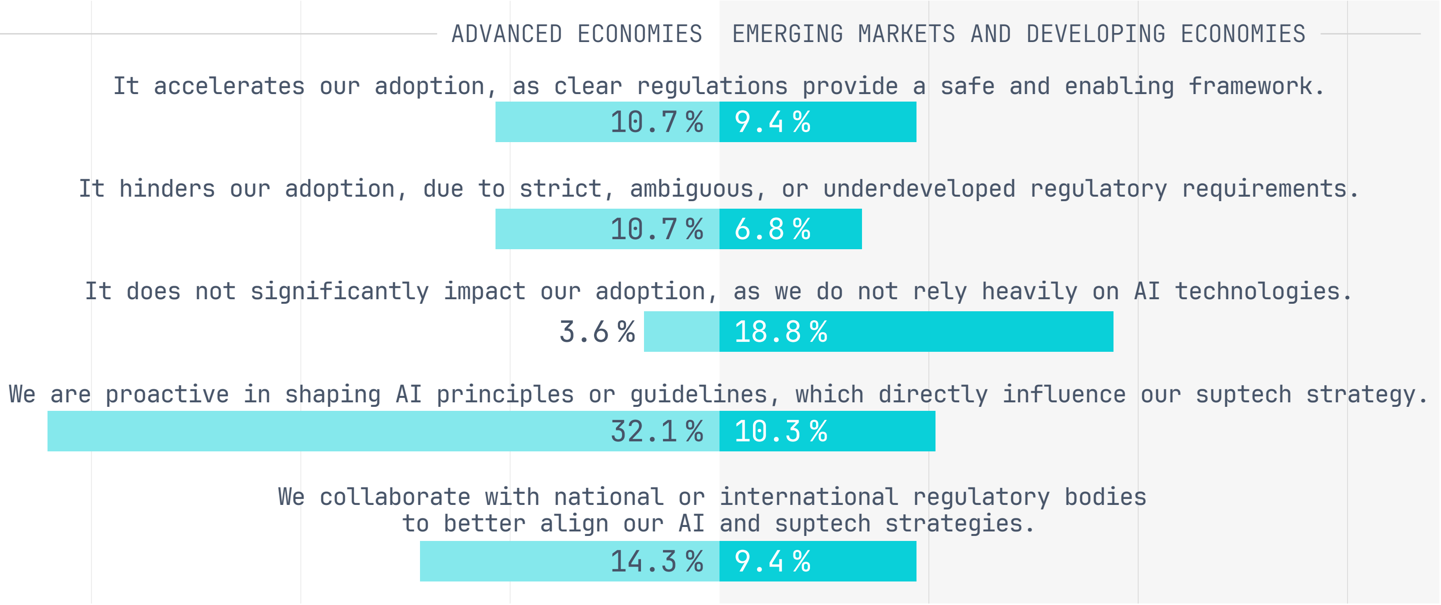


FIGURE 130.

Influence Of AI Regulations On Agency Strategies For SupTech Adoption By Economic Classification



suptech strategies, compared with 10% of EMDEs. Collaborative efforts with other regulatory bodies are reported by 14% of AEs and 9% of EMDEs. AEs are also more likely to report both acceleration and hindrance effects (11% each), reflecting sophisticated but demanding regulatory contexts. EMDEs, by contrast, report lower levels of both enablement (9%) and hindrance (7%), consistent with less developed AI governance frameworks. Nineteen percent of EMDEs say AI regulations have little impact because they make limited use of AI, compared with only 4% of AEs.

These patterns suggest that AI regulation is not yet the main determinant of suptech adoption, but its influence is rising. Authorities are gradually moving from passive compliance to active participation in AI-governance debates, seeking to balance innovation with accountability and financial stability. As global frameworks mature, supervisors will need to align their internal AI use with evolving standards, develop expertise to oversee AI in the financial sector, and contribute to regulatory models that are flexible enough to support innovation yet robust enough to protect consumers and markets.

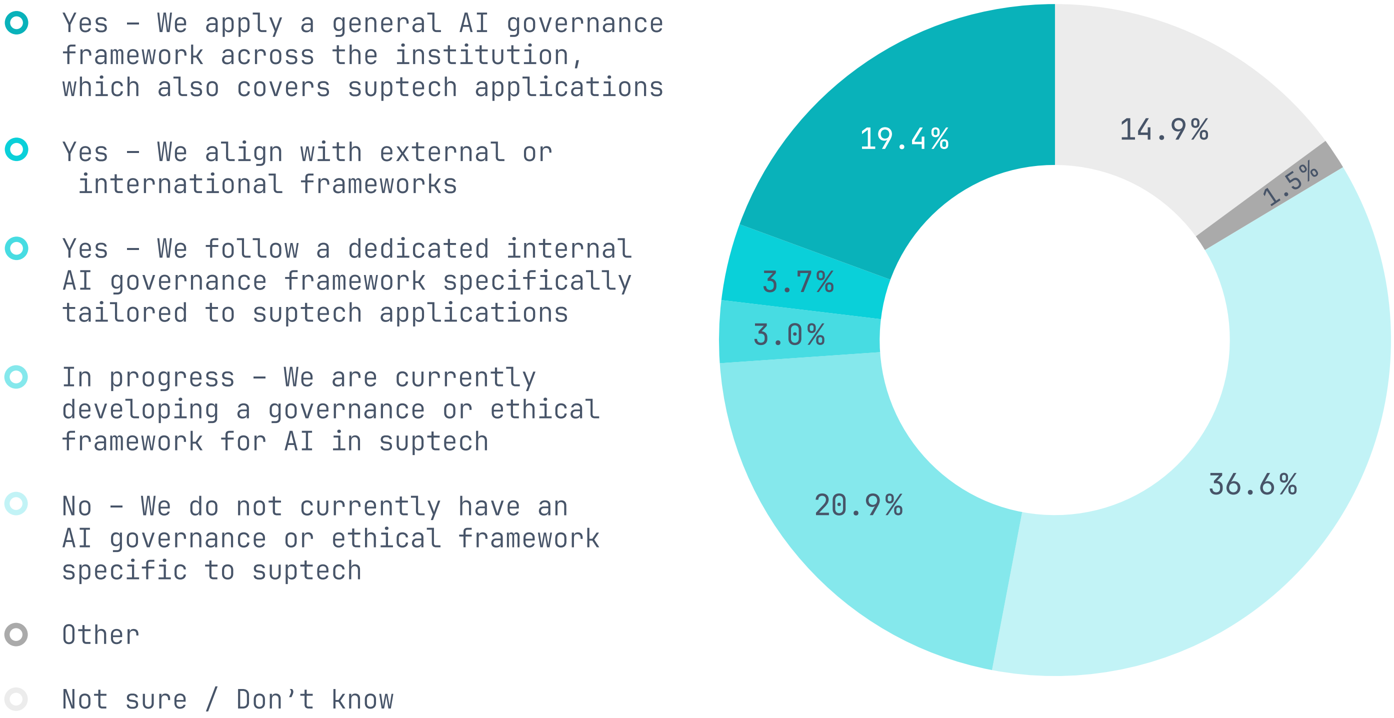
5.5 Ethical considerations in the use of AI

Ethical and governance frameworks for AI in supervision remain underdeveloped. While a small group of authorities has started to institutionalise responsible-AI practices, most operate without formal structures, and transparency mechanisms are rare. The gap between AI deployment and ethical oversight is particularly wide in EMDEs, raising concerns about uneven standards and potential risks to public trust.

The adoption of formal AI-governance and ethics frameworks for suptech applications is still the exception rather than the rule (Figure 131).

FIGURE 131.

Adoption Of Formal AI Governance Or Ethical Frameworks For SupTech Applications



Only 3% of agencies report having a dedicated internal framework specifically tailored to suptech, and 4% align explicitly with international frameworks such as the OECD AI Principles or the EU AI Act. A larger group, 19%, applies general organisational AI-governance arrangements to supervisory applications, indicating that many authorities treat supervisory AI as part of broader technology governance rather than recognising its distinct regulatory implications.

The predominant pattern is absence or uncertainty. Thirty-seven percent of agencies report no current framework for AI in supervision, and a further 15% are unsure whether one exists. Together, this means that over half of surveyed authorities lack clear governance structures for AI-enabled suptech. Some of this gap is offset by 21% of agencies that are actively developing frameworks, signalling growing awareness even if implementation is still in progress. The low uptake of international frameworks suggests that many authorities are still working out how to translate high-level principles into operational guidance for supervisory teams.

Economic disparities are marked (Figure 132). Advanced economies show greater governance maturity: 36% apply general AI frameworks, 28% are developing new ones, and only 12% report having no framework. In EMDEs, 43% of agencies operate without any governance structure, and only 15% have general frameworks in place. Engagement with international standards and dedicated suptech frameworks is also higher in AEs. Uncertainty about governance status is almost twice as high in EMDEs (17% versus 8% in AEs), highlighting knowledge and capacity gaps. The case study from the UK FCA illustrates one emerging model of responsible-AI governance in a supervisory context, integrating ethical principles and governance into the full lifecycle of AI-enabled suptech (see below).

Beyond frameworks, concrete ethical safeguards remain limited (Figure 133). Thirty-two percent of authorities report no specific ethical measures for AI in supervision. Ethical guidelines specific to AI are in place at 15% of agencies, and 12% require training on ethical AI principles. More robust mechanisms are rare: only 6% have ethics boards or external advisory

FIGURE 132.

Adoption Of Formal AI Governance Or Ethical Frameworks For SupTech Applications By Economic Classification

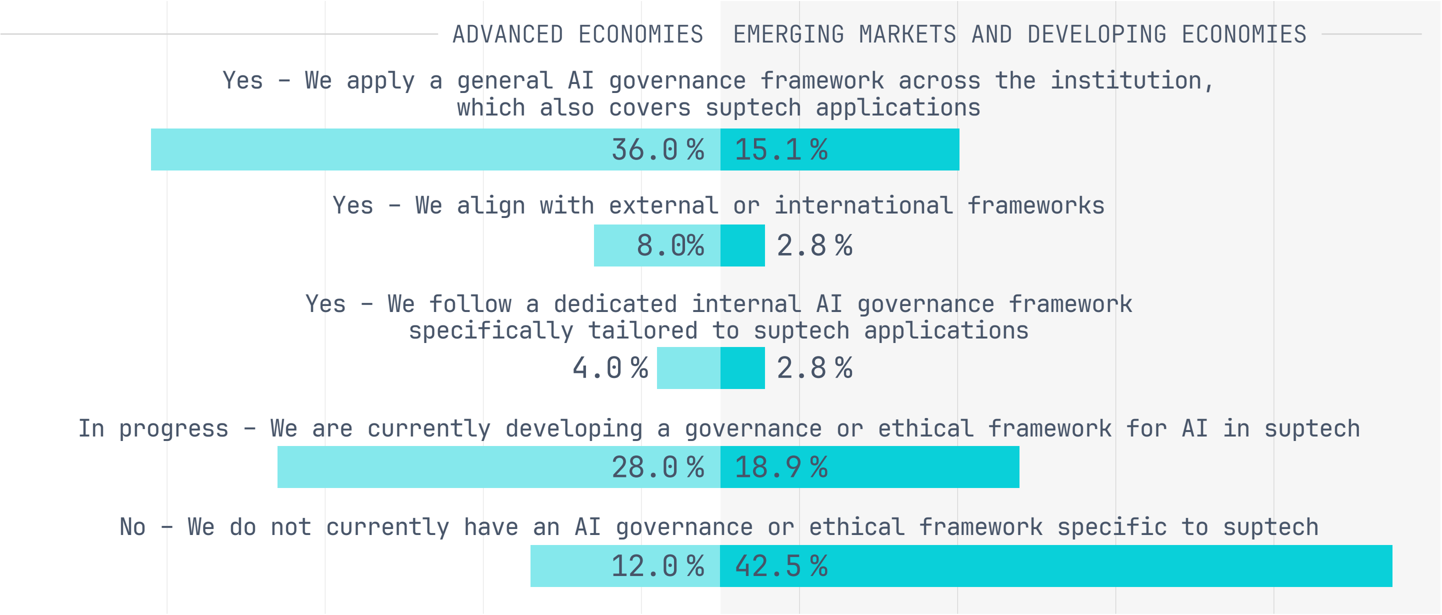
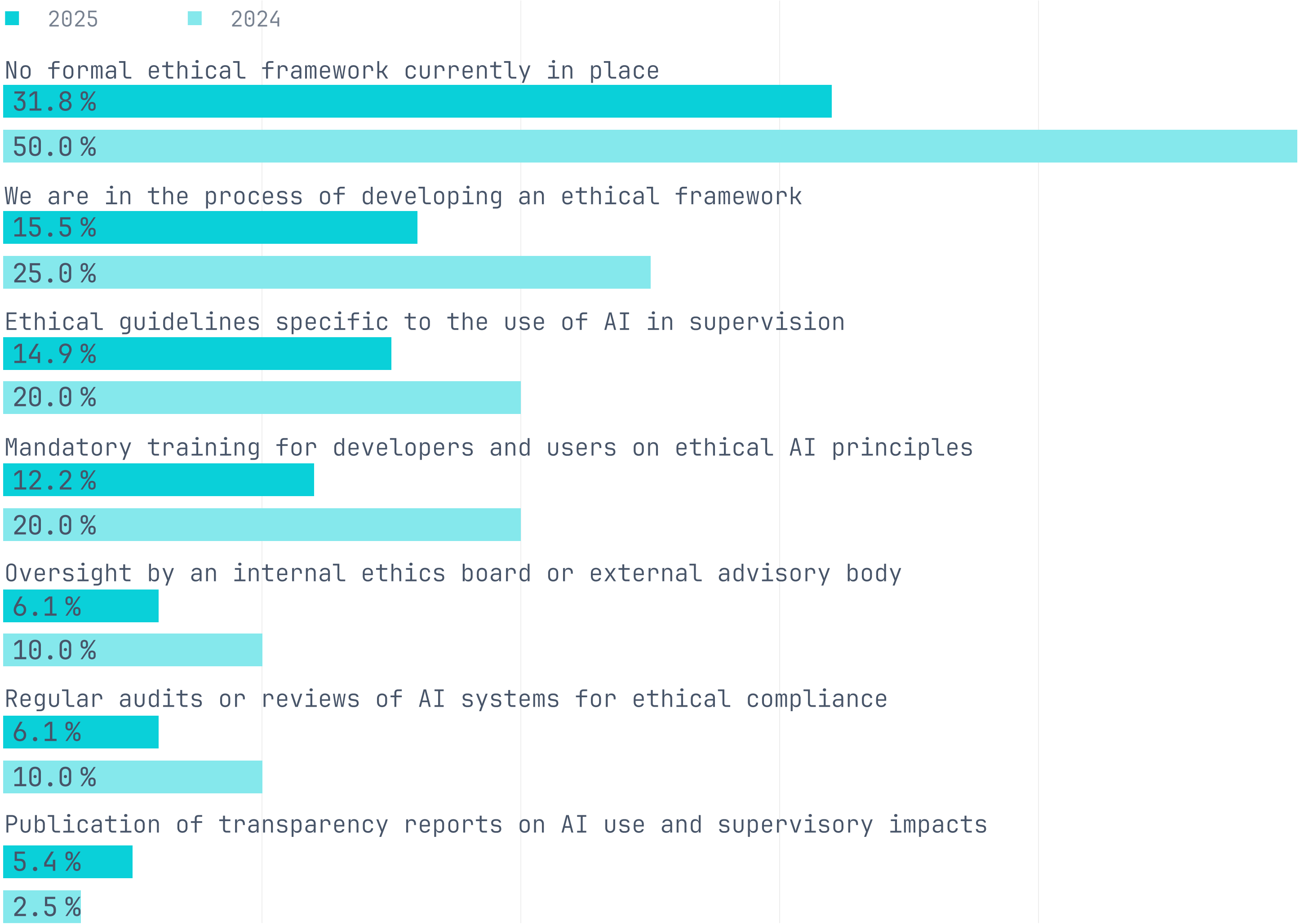


FIGURE 133.

Measures In Place To Ensure The Ethical Use Of AI Technologies In SupTech



bodies, 6% conduct regular ethical audits, and 5% publish transparency reports on AI use and its supervisory impacts. AUSTRAC's efforts to pair AI-driven financial-crime analytics with transparency and governance controls are an example of how agencies are beginning to operationalise these safeguards.

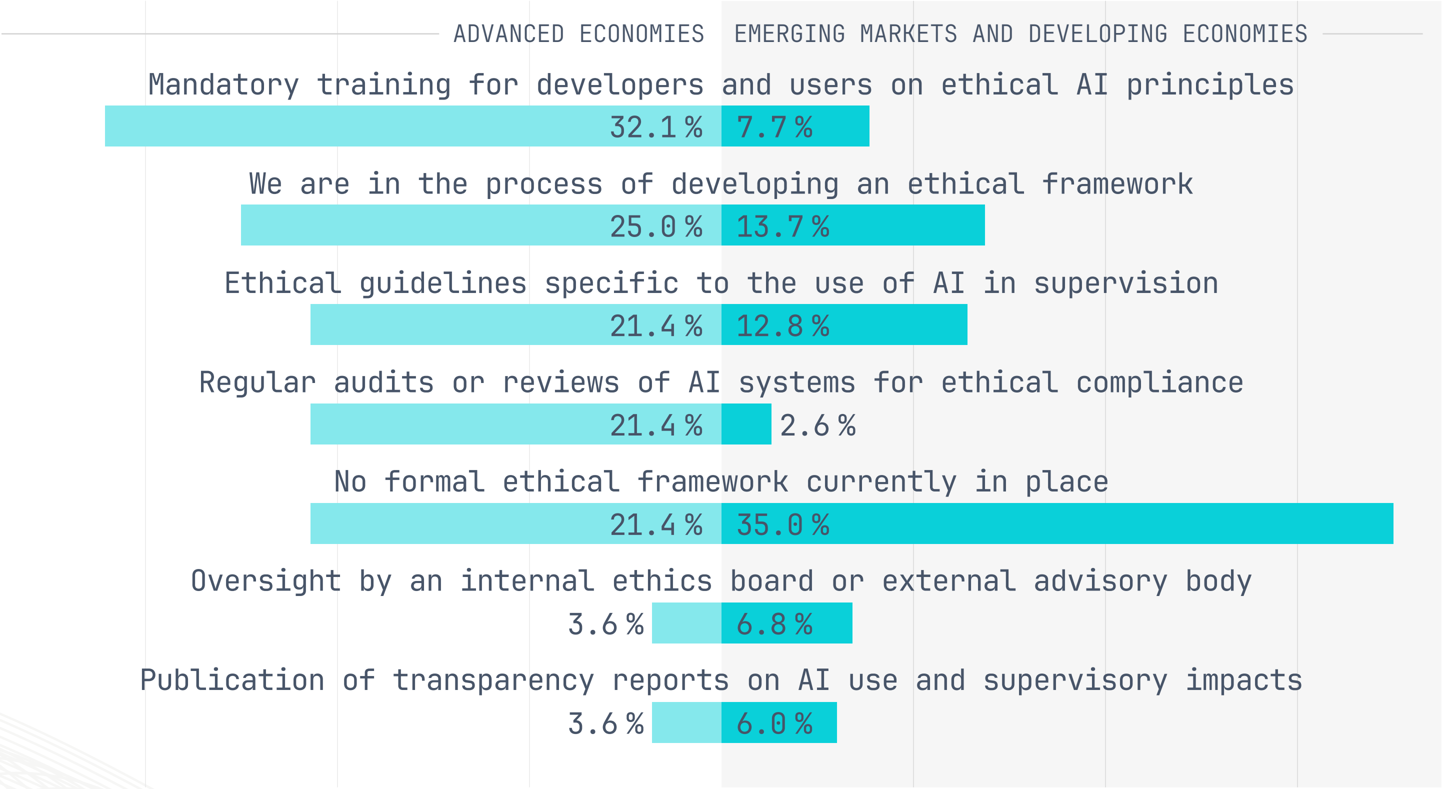
Advanced economies again outperform EMDEs on most measures (Figure 134). Around 32% of AEs mandate ethics training, compared with 8% of EMDEs, and 21% of AEs conduct regular ethical audits versus 3% in EMDEs. AEs are also more likely to be developing or maintaining formal ethical frameworks. However, even among AEs, external transparency – in the form of public reporting on AI impacts – remains uncommon.

Overall, the state of AI governance and ethics in suptech reveals a significant implementation gap. Many authorities are deploying or piloting AI tools without comprehensive frameworks to manage ethical risks, accountability, and public expectations. As AI and GenAI become more central to supervisory practice, this gap could undermine both operational integrity and trust in financial oversight. Closing it will require accelerated development of governance frameworks, adaptation of international principles to supervisory realities, systematic investment in training and audits, and stronger transparency practices. Without these measures, the benefits of AI-enabled supervision will be harder to realise and easier to contest.

FIGURE 134.

Measures In Place To Ensure The Ethical Use Of AI Technologies In SupTech

By Economic Classification



The UK Financial Conduct Authority's thought leadership on Responsible AI & Data

By Fatima Abukar (Principal Advisor, Responsible AI & Data), Steve Hall (Manager, Supervision Hub), Zac Lovell (Data & AI Risk, Senior Associate), Sid Samant (Principal Data Scientist)

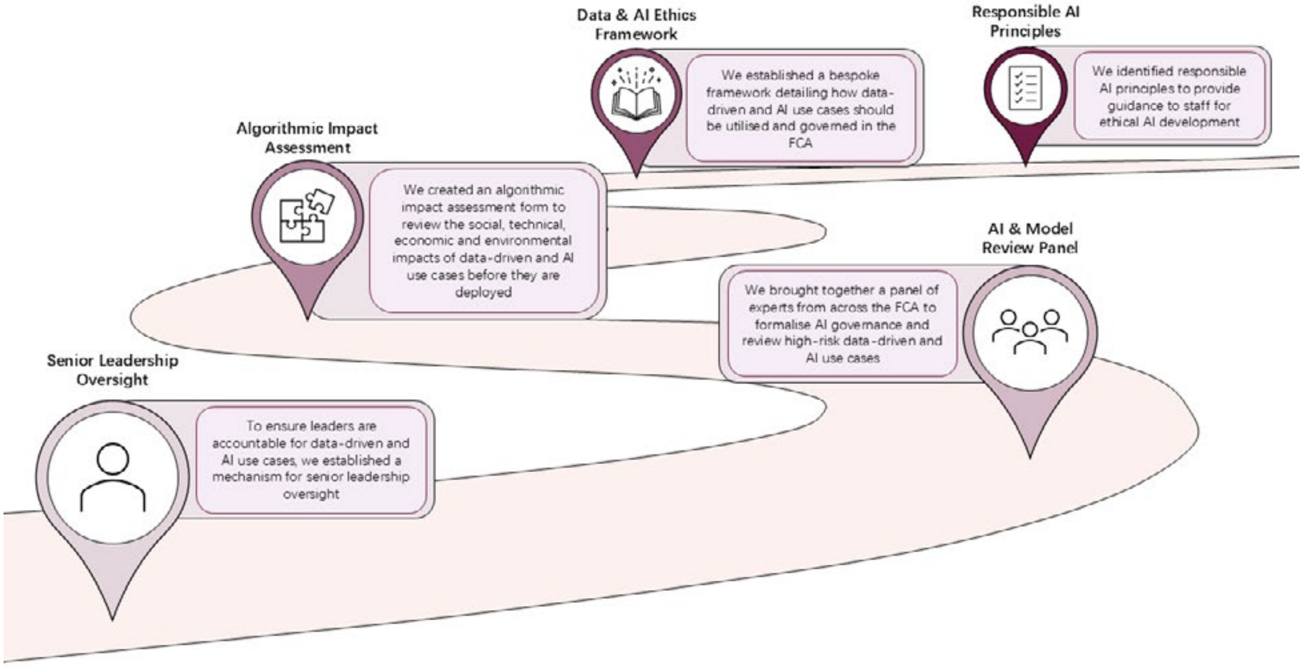
AI capabilities are growing at a rapid pace, which has prompted the UK government to develop the AI Opportunities Action Plan to encourage public sector bodies to harness AI and boost growth. The FCA's five-year strategy describes plans to become a smarter and more technology-focused regulator. It details the FCA's aim to explore data-driven technologies and AI in order to improve regulatory processes. In preparation, an independent and specialist first-line function, the Data & AI Risk Hub, has been set up to establish AI governance and best practices, aiming to support supervisors in adopting safe and trustworthy SupTech solutions. Our vision is supported through a multi-disciplinary and collaborative process that integrates expertise across legal and compliance functions.

Our Journey to Responsible AI & Data

To develop our framework, we began by looking inward to understand the work our colleagues do and the problems they face. We learnt from front-line staff where they believed AI could help, evaluated existing data and technology solutions, and mapped the internal governance that enables their use. To understand external trends and an emerging practice, we engaged with approximately 40 public sector, academic and industry organisations. An additional focus included public sentiment towards AI and its potential to impact society. A key challenge across this work was aligning definitions and risk appetites which continue to change rapidly. As a result, our framework is designed to offer staff coherent guidance that balances opportunity and risk. Built to adapt over time, the framework interoperates with existing governance and standards, while providing practical steps for assurance and accountability.

CONTINUED ON NEXT PAGE

THE FCA'S RESPONSIBLE AI & DATA JOURNEY



Senior Leadership Oversight

To ensure leaders are accountable for data-driven and AI use cases, we established a mechanism for senior leadership oversight

Algorithmic Impact Assessment

We created an algorithmic impact assessment form to review the social, technical, economic and environmental impacts of data-driven and AI use cases before they are deployed

AI & Model Review Panel

We brought together a panel of experts from across the FCA to formalise AI governance and review high-risk data-driven and AI use cases

Data & AI Ethics Framework

We established a bespoke framework detailing how data-driven and AI use cases should be utilised and governed in the FCA

Responsible AI Principles

We identified responsible AI principles to provide guidance to staff for ethical AI development

Innovating Responsibly: SupTech in the Supervision Hub

The FCA Authorisations Division's Supervision Hub oversees firms and individuals across the financial sector. Supervisors interact with consumers daily, addressing queries and complaints, and assisting authorised and regulated firms with system processes and regulatory matters.

A real-time transcription capability has been introduced to support our supervisors. This tool transcribes calls, promoting consistent record keeping and assisting staff with note taking. As a result, supervisors can engage more effectively in conversations focusing more on the discussion rather than logging system updates.

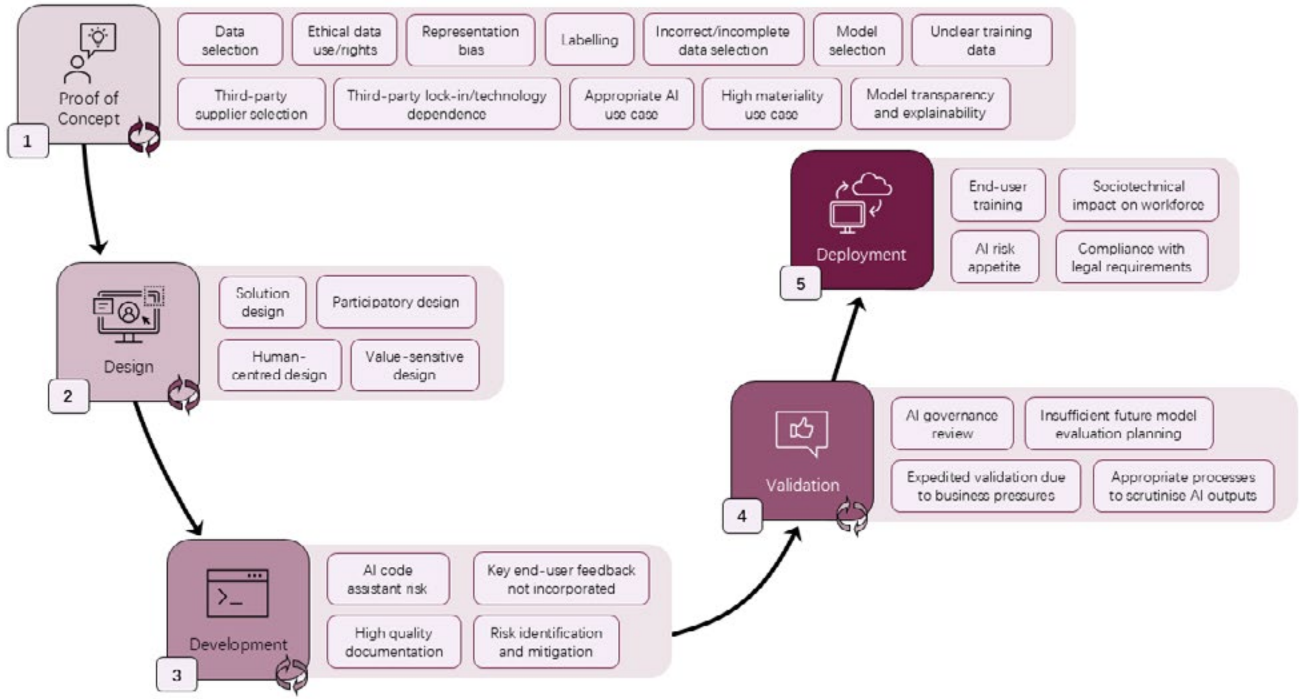
Supervisors can review call transcripts and search for keywords within our central data repository. The current setup addresses operational needs whilst enabling effective oversight to manage any third-party risk and maintain data storage protocols.

Supervisors are aware that transcription tools may not accurately capture all accents or speech patterns. Basic safeguards in place include manual notetaking and requiring supervisors to verify the accuracy of AI-generated outputs.

Another SupTech the Supervision Hub uses, is a conversation bot with automated speech recognition to handle consumer enquiries. The bot determines the enquiry

CONTINUED ON NEXT PAGE

ETHICAL RISKS AND PRACTICES IDENTIFIED THROUGHOUT THE SOFTWARE DEVELOPMENT LIFECYCLE


1
Proof of Concept
Data selection
Ethical data use/rights
Representation bias
Labelling
Incorrect/incomplete data selection
Model selection
Unclear training data
Third-party supplier selection
Third-party lock-in/technology dependence
Appropriate AI use case
High materiality use case
Model transparency and explainability
2
Design
Solution design
Participatory design
Human-centred design
Value-sensitive design
3
Development
AI code assistant risk
Key end-user feedback not incorporated
High quality documentation
Risk identification and mitigation
4
Validation
AI governance review
Insufficient future model evaluation planning
Expedited validation due to business pressures
Appropriate processes to scrutinise AI outputs
5
Deployment
End-user training
Sociotechnical impact on workforce
AI risk appetite
Compliance with legal requirements

type and directs callers to the relevant regulatory body, such as the Financial Ombudsman Service, Action Fraud, or the Financial Services Compensation Scheme. This technology helps to direct the consumer to the right place first time, reducing the number of call transfers and enables consumers to obtain resolutions more efficiently.

This service supports the FCA's commitment to improving regulatory engagement through responsible innovation. The integration of speech recognition and transcription streamlines contact procedures and improves accessibility for consumers. Supervisors can monitor the bot's performance and review routing decisions to ensure continuous improvement and compliance with FCA standards.

Transparency and Agency are key principles within the FCA's Data & AI Ethics Framework. Our first-line function conducts independent evaluations of data-driven and AI use cases, ensuring that teams like the Supervision Hub receive clear and actionable recommendations prior to deploying a SupTech solution. Supervisors retain responsibility for all records and decisions, whilst the implementation of these solutions must be substantiated by operational needs to upholding our commitment to responsible innovation.

CONTINUED ON NEXT PAGE

Looking ahead

Data-driven and AI interventions typically interact with complex social systems risk amplifying existing disparities or creating unintended consequences. As AI becomes increasingly accessible, we find many colleagues have operational knowledge; they know how to run prompts, tools or other integrations. An ongoing challenge is establishing the importance of underlying knowledge of the right behaviours, assumptions, limitations, and risks. Our framework aids colleagues in justifying the necessity for AI from the outset to prevent the adoption of technology as a “shiny new tool”. The goal is to foster an assurance mindset, so that even as the technology evolves, staff are equipped to develop high quality and trustworthy solutions.

Conclusions

The final section of the survey asked three open-ended questions and one multiple-choice question to supervisory authorities, seeking insights into planned technologies and projects, strategic objectives, and expected timelines for implementation. Respondents also described perceived global trends, preparation measures such as strategic planning, training, and cross-agency partnerships, and the main challenges anticipated over the next three years. We analysed these responses using a language-model–assisted classification approach to detect common themes and patterns across the dataset.

Suptech pipeline

Across jurisdictions, the suptech pipeline for the next one to three years indicates a clear global shift toward more advanced, integrated, and data-centric supervisory models. Authorities are moving beyond foundational digitalisation toward the deployment of more sophisticated analytical and AI-enabled applications. Three strategic priorities shape this transition: strengthening risk-based supervision, increasing automation and operational efficiency, and consolidating core data infrastructure.

A central priority for many agencies is the development or expansion of unified data warehouses or supervisory data platforms. These efforts aim to centralise information flows, standardise taxonomies, and enable higher-frequency or near real-time data ingestion. Parallel investments in ICT and cloud infrastructure underscore the recognition that advanced analytics depend on stable, scalable, and secure foundations.

Pipeline plans also reveal accelerated interest in integrating AI and advanced analytics into routine workflows. Authorities cite initiatives to automate key supervisory processes, introduce ML-based predictive analytics and early-warning indicators, and pilot GenAI use cases for tasks such as report summarisation and automated consumer-complaint classification. These use cases are framed as augmenting supervisory judgement, not replacing it.

Finally, agencies are modernising supervisory methodologies themselves, embedding risk-based models directly into new systems, launching dedicated programmes for consumer-protection supervision, and establishing formal suptech strategies or innovation functions. Many note the need for targeted training to ensure supervisors can meaningfully engage with new analytical tools.

Global trends and preparations

Survey responses converge on a set of global trends that define the future trajectory of suptech. AI and advanced data analytics dominate these trends, supporting a shift from retrospective oversight toward more proactive, predictive, and continuous supervision. Authorities highlight growing interest in GenAI for operational efficiency and enhanced analytical capabilities, together with renewed attention to interoperability and shared data ecosystems across sectors.

Emerging risk domains are also shaping priorities. Authorities point to increased supervisory attention to cybersecurity, climate and ESG-related risks, and the monitoring implications of digital currencies. These trends reinforce the need for data standards, cross-border cooperation, and more flexible supervisory architectures.

Preparatory efforts concentrate on three areas: infrastructure, capacity, and governance. Agencies are investing in cloud-enabled platforms and unified data environments to support high-frequency data flows and more complex analytical processes. Pilot initiatives involving LLMs, agentic-AI workflows, and automated risk-scoring systems are becoming more common, though still limited in scale.

Crucially, these technological investments are matched by commitments to staff development. Authorities emphasise the need for data literacy, AI-specific skills, and the practical ability to interpret advanced analytical outputs. In parallel, agencies are strengthening governance frameworks, focusing on data protection, model transparency, validation processes, and ethical AI principles. This mirrors the ethical and governance gaps identified in Section 5.

Partnerships with multilateral bodies, peer agencies, and industry actors are becoming more prominent as authorities seek to reduce duplication, accelerate learning, and align standards.

Challenge

Authorities expect significant and interconnected challenges as they attempt to operationalise their suptech roadmaps. The most pervasive obstacles are financial and human-capital constraints. Advanced tools and data platforms require sustained investment for acquisition, integration, and maintenance, while global competition for data-science and AI talent makes recruitment and retention difficult. These challenges are often compounded by limits on public-sector salary structures and institutional hiring rules.

Beyond resource constraints, agencies anticipate complex technical and organisational barriers. Authorities highlight the difficulty of modernising legacy IT systems, achieving interoperability across disparate datasets, and maintaining cybersecurity and privacy protections while integrating advanced analytics. Many underscore that successful adoption depends on overcoming internal resistance, building user confidence in AI-enabled applications, and establishing governance arrangements that clarify accountability for outputs generated by complex or opaque models.

Quantitatively, limited technical capacity or availability of skilled personnel is the top-ranked barrier, cited by 30% of authorities, followed by budget or funding constraints at 28%. A second tier of challenges — including data availability or quality, cybersecurity, change-management resistance, and legacy-system constraints — are each cited by 8% of respondents. Vendor-related challenges (6%), inter-agency coordination issues (3%), and legal or regulatory uncertainty (2%) round out the list. These proportions reinforce that, for most authorities, talent and funding remain the decisive bottlenecks.

Closing notes

The rapid evolution of financial services is reshaping supervisory expectations, making suptech central to effective, timely, and risk-sensitive oversight. The 2025 State of SupTech Survey shows that while implementation momentum is growing, realising the full value of these technologies requires more than incremental tool deployment. It demands institutional readiness, strategic clarity, and collective action.

Progress remains uneven. Authorities with formal suptech strategies — particularly those integrating data governance, AI readiness, and workforce development — are significantly more likely to deploy multiple applications and to scale pilots successfully. Yet persistent gaps in infrastructure, skills, and coordination continue to impede broader system-level transformation. Even where advanced applications exist, many agencies have not yet established the foundational governance structures needed for safe and accountable AI use.

A critical structural barrier is the absence of regional or thematic scale-up mechanisms. Innovation often remains confined to individual agencies, raising costs and limiting diffusion. Shared testbeds, standards-development groups, and collaborative prototyping environments could materially reduce duplication and accelerate the adoption of high-value technologies. Although models such as tech sprints and innovation labs exist, they remain underused relative to the scale of global demand.

Taken together, the findings suggest a supervisory sector moving steadily — but unevenly — toward a more intelligent, data-driven, and collaborative future. Realising this vision will require sustained investment in capacity, stronger coordination across jurisdictions, and the development of shared platforms and standards. Building these enablers is essential not only for operational efficiency but also for safeguarding public trust and ensuring that all financial authorities can participate in and shape the next generation of digital supervision.

Appendix

APPENDIX 1.

List of respondents

AGENCY	COUNTRY
Agência Angolana de Regulação e Supervisão de Seguros	Angola
Anguilla Financial Services Commission	Anguilla
Banco Central Republica Argentina	Argentina
Comisión Nacional de Valores	Argentina
Central Bank of Armenia	Armenia
Australian Securities and Investments Commission	Australia
Austrian Financial Market Authority	Austria
Bangladesh Bank	Bangladesh
Bangladesh Securities and Exchange Commission	Bangladesh
Financial Services Commission	Barbados
National Bank of Belgium	Belgium
Financial Services and Markets Authority	Belgium
Central Bank of Belize	Belize
Autoridad de Fiscalización y Control de Pensiones y Seguros	Bolivia
Banking Agency of the Federation of Bosnia and Herzegovina	Bosnia and Herzegovina
Banking Agency of Republika Srpska	Bosnia and Herzegovina
Non-Bank Financial Institutions Regulatory Authority	Botswana
Central Bank of Brazil	Brazil
Securities and Exchange Commission of Brazil	Brazil
Securities and Exchange Regulator of Cambodia	Cambodia
Securities and Exchange Regulator of Cambodia	Cambodia
British Columbia Securities Commission	Canada
Office of the Superintendent of Financial Institutions of Canada	Canada

AGENCY	COUNTRY
Financial Consumer Agency of Canada	Canada
Cayman Islands Monetary Authority	Cayman Islands
Financial Market Commission	Chile
Financial Superintendency of Colombia	Colombia
Superintendencia de la Economía Solidaria de Colombia	Colombia
Financial Supervisory Commission	Cook Islands
Costa Rican Securities Superintendency	Costa Rica
Superintendencia General de Entidades Financieras	Costa Rica
Superintendencia de Pensiones de Costa Rica	Costa Rica
Superintendencia General de Seguros de Costa Rica	Costa Rica
Croatian national bank	Croatia
Central Bank of Curacao & Sint Maarten	Curaçao
Central Bank of Cyprus	Cyprus
Cyprus Securities and Exchange Commission	Cyprus
Central Bank of West African's States	Côte d'Ivoire
Superintendencia del Mercado de Valores	Dominican Republic
Superintendencia de Bancos de Republica Dominicana	Dominican Republic
Instituto de Garantía de Depósitos	El Salvador
Central Bank of Eswatini	Eswatini
Financial Services Regulatory Authority of eSwatini	Eswatini
Ethiopian Capital Market Authority	Ethiopia
National Bank of Ethiopia	Ethiopia
Bankf of Finland and Financial Supervisory Authority	Finland
Central Bank of The Gambia	Gambia, The
Federal Financial Supervisory Authority	Germany

AGENCY	COUNTRY
European Central Bank	Germany
National Pensions Regulatory Authority	Ghana
Securities and Exchange Commission	Ghana
Bank of Ghana	Ghana
Bank of Greece	Greece
Grenada Authority for the Regulation of Financial Institutions	Grenada
Superintendencia de Bancos	Guatemala
Banque Centrale de la République de Guinée	Guinea
Bank of Guyana	Guyana
National Commission Of Banks and Insurance	Honduras
Hong Kong Monetary Authority	Hong Kong SAR, China
RESERVE BANK OF INDIA	India
Otoritas Jasa Keuangan	Indonesia
Bank Indonesia	Indonesia
Central bank of Iraq	Iraq
Central bank of Ireland	Ireland
Bank of Italy	Italy
Bank of Jamaica	Jamaica
Jersey Financial Services Commission	Jersey
The Agency of the Republic of Kazakhstan for Regulation and Development of Financial Market	Kazakhstan
Central Bank of Kenya	Kenya
Insurance Regulatory Authority	Kenya
The Sacco Societies Regulatory Authority of Kenya	Kenya
Communications Authority of Kenya	Kenya
Central Bank of the Republic of Kosovo	Kosovo

AGENCY	COUNTRY
Capital Markets Authority	Kuwait
National bank	Kyrgyz Republic
Lao Securities Commission Office	Lao PDR
Lietuvos bankas	Lithuania
Reserve Bank of Malawi	Malawi
Securities Commission Malaysia	Malaysia
Malta Financial Services Authority, Data Management & Business Intelligence	Malta
Bank of Mauritius	Mauritius
Comisión Nacional Bancaria y de Valores	Mexico
Banco de México	Mexico
National Bank of Moldova	Moldova
Financial Regulatory Commission	Mongolia
Central Bank of Montenegro	Montenegro
Moroccan Capital Market Authority	Morocco
Supervisory Authority of Insurance and Social Welfare	Morocco
Banco de Moçambique	Mozambique
Bank of Namibia	Namibia
Nepal Insurance Authority	Nepal
De Nederlandsche Bank	Netherlands
Financial Markets Authority	New Zealand
Superintendencia de Bancos y de Otras Instituciones Financieras	Nicaragua
Central Bank of Nigeria	Nigeria
Nigerian Financial Intelligence Unit	Nigeria
Securities and Exchange Commission	Nigeria
National Bank of the Republic of North Macedonia	North Macedonia

AGENCY	COUNTRY
Central Bank of Oman	Oman
The Financial Services Authority	Oman
Securities and Exchange Commission of Pakistan	Pakistan
Superintendencia de Bancos	Panama
Superintendencia del Mercado de Valores	Panama
Banco Central del Paraguay	Paraguay
Superintendencia de Banca, Seguros y AFP	Peru
Philippine Competition Commission	Philippines
Bangko Sentral ng Pilipinas	Philippines
Securities and Exchange Commission	Philippines
Polish Financial Supervision Authority	Poland
Qatar Financial Centre Regulatory Authority	Qatar
National Bank de Romania	Romania
National Bank of Rwanda	Rwanda
National bank of Serbia	Serbia
Central Bank of Seychelles	Seychelles
Agencija za zavarovalni nadzor	Slovenia
Central Bank of Solomon Islands	Solomon Islands
Financial Intelligence Centre of South Africa	South Africa
National Credit Regulator	South Africa
South African Reserve Bank	South Africa
Financial Sector Conduct Authority	South Africa
Eastern Caribbean Central Bank	St. Kitts and Nevis
Centrale Bank van Suriname	Suriname
FInansinspektionen	Sweden

AGENCY	COUNTRY
Swiss Financial Market Supervisory Authority	Switzerland
Bank of Tanzania	Tanzania
Securities and Exchange Commission Thailand	Thailand
Bank of Thailand	Thailand
Trinidad and Tobago Securities and Exchange Commission	Trinidad and Tobago
Conseil du Marche	Tunisia
Bank of Uganda	Uganda
National Bank of Ukraine	Ukraine
Central Bank of The United Arab Emirates	United Arab Emirates
Dubai Financial Services Authority	United Arab Emirates
Financial Conduct Authority	United Kingdom
Bank of England	United Kingdom
Federal Reserve	United States
Superintendencia de Servicios Financieros - Banco Central del Uruguay	Uruguay
The Central Bank of the Republic of Uzbekistan	Uzbekistan
State Securities Commission	Vietnam
Palestine Capital Market Authority	West Bank and Gaza
Palestine Monetary Authority	West Bank and Gaza
Competition and Consumer Protection Commission	Zambia
Securities & Exchange Commission, Zambia	Zambia
Bank of Zambia	Zambia
Insurance and Pensions Commission	Zimbabwe
The Securities and Exchange Commission of Zimbabwe	Zimbabwe
Reserve Bank of Zimbabwe	Zimbabwe

APPENDIX 2.

Definitions

Application programming interfaces (APIs) — allow software programmes to interact by exchanging data which can prompt certain actions, such as making a transaction. This includes payment APIs, data APIs, 'ecosystem expansion' APIs and 'consent and identity' APIs. (World Bank 2020b)

Artificial intelligence (AI) — defined as IT systems that perform functions requiring human capabilities. AI can ask questions, discover and test hypotheses, and make decisions automatically based on advanced analytics operating on extensive data sets. Machine learning (ML) is one subcategory of AI. (World Bank 2020a)

Big data — high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation. (Gartner 2022)

Business intelligence (BI) — software and services to transform data into actionable insights that inform an organisation's strategic and tactical business decisions. BI tools access and analyse data sets and present analytical findings in reports, summaries, dashboards, graphs, charts and maps to provide users with detailed intelligence about the state of the business. The term business intelligence often also refers to a range of tools that provide quick, easy-to-digest access to insights about an organisation's current state based on available data. (CIO 2019)

Central Bank Digital Currencies (CBDCs) — an electronic form of central bank money with potential wide use by households and businesses to store value and make payments. It is central bank digital money in the national unit (e.g., the US dollar) representing legal tender with the liability of the central bank, like physical currency in circulation. (Deloitte 2022)

Chatbot — a computer programme that simulates and processes human conversation (either written or spoken), allowing humans to interact with digital devices as if they were communicating with a real person. (Oracle 2022)

Climate-related risks - financial risks posed by the exposure of financial institutions to physical or transition risks caused by or related to climate change, for example, damage caused by extreme weather events or a decline in asset value in carbon-intensive sectors. (NGFS 2020)

Cloud computing — an innovation in computing that allows for the use of an online network ('cloud') to host processors, leading to an increase in the scale and flexibility of computing capacity. (FSB 2020)

Computer vision (CV) — a field of AI that enables computers and systems to derive meaningful information from digital images, videos and other visual inputs — and take actions or make recommendations based on that information. Subcategories include image segmentation (where items are in an image) and image classification (what the items are). (R²A 2017)

Consumer protection — the framework of laws, regulations, and institutional arrangements that safeguard consumers by ensuring fair and responsible treatment for them in the financial marketplace. (World Bank 2022)

Cybersecurity — preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability, can also be involved. (FSB 2018)

Data lakes — centralised repositories designed to store, process, and secure large amounts of structured, semi-structured, and unstructured data. It can store any type of data in its native format and process it, ignoring size limits. (Google 2022)

Data processing — the collective set of data actions (the complete data life cycle, including, but not limited to, collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission and disposal). (NIST 2020)

Data validation — an activity aimed at verifying whether the value of a data item comes from the given (finite or infinite) set of acceptable values. For example, this ensures a postal code is valid or that a numeric value does not include letters or symbols. These rules can be enforced in either a manual or automatic fashion. (OECD 2008)

Data visualisation — the graphical representation of data for understanding and communication. This typically takes the form of exploratory (trying to explore and understand patterns and trends within your data) or explanatory (surfacing something in your data you would like to communicate to your audience) forms. (Johns Hopkins 2022)

Data warehouse — a data management system designed to enable and support business intelligence (BI) activities, especially analytics. Data warehouses are solely intended to perform queries and analysis and often contain large amounts of historical data. The data within a data warehouse is usually derived from various sources, such as application log files and transaction applications. (Oracle 2022)

Descriptive analytics tools — interactive applications used to search and summarise historical data to identify patterns or meaning, including dashboards, data visualisation tools and automated statistical summaries. (TechTarget 2022)

Digital assets — digital instruments issued or represented by using distributed ledger or similar technology. This does not include digital representations of fiat currencies, such as e-money. (FSB 2022)

Digital financial services — refers to services such as payments, transfers, savings, credit, insurance, securities, financial planning and account statements that are delivered via digital/electronic technology, such as e-money, payment cards and a regular bank account. (World Bank 2020b)

Digital twins - virtual replicas or copies of physical systems that can be used for simulation and analysis of how such system evolve over a long period of time. (IMF 2024)

Distributed Ledger Technology (DLT) — refers to technology such as blockchain that records information through a distributed ledger (a repeated digital copy of data at multiple locations). These technologies enable nodes in a network to securely propose, validate and record state changes (or updates) to a synchronised ledger distributed across the network's nodes. (World Bank 2020a)

Environmental risks — financial risks posed by the exposure of financial institutions and/or the financial sector to activities that may potentially cause or be affected by environmental degradation (such as land contamination and desertification, biodiversity loss, and deforestation) and the loss of ecosystem services. (NGFS 2020)

Financial inclusion — the uptake and use of a range of appropriate financial products and services by individuals and MSMEs (micro, small, and medium enterprises), provided in a manner that is accessible and safe to the consumer and sustainable to the provider. (World Bank 2020b)

Financial stability — a stable financial system can efficiently allocate resources, assess and manage financial risks, maintain employment levels close to the economy's natural rate, and eliminate relative price movements of real or financial assets that will affect monetary stability or employment levels. Financial stability is paramount for economic growth, as most transactions in the real economy are made through the financial system. (World Bank 2016)

Fintech — an acronym for 'financial technology'. It refers to the advances in technology that have the potential to transform the provision of financial services spurring the development of new business models, applications, processes, and products. (World Bank 2020a)

Generative Artificial Intelligence (GenAI) — a form of AI that can generate text, images, or other types of media all in response to a simple 'prompt'. These systems learn from patterns and structure of their training data, finally presenting an inspiring piece of new data. Notable examples include chatbots like ChatGPT by OpenAI and Bard by Google, along with AI systems like Stable Diffusion, Midjourney and DALL-E. (Cambridge SupTech Lab 2023)

Generative Pre-trained Transformers (GPT) — a type of LLM and a prominent framework for generative artificial intelligence.

Geographic information systems (GIS) — a computerised system for capturing, storing, checking and displaying data related to positions on the Earth's surface, enabling analysis and visualisation based on spatial relationships between this data. (NatGeo 2022)

Image processing — the general process of digitising and formatting visual information (for example, photographs and video) so useful information can be automatically extracted via technologies such as optical character recognition (OCR), facial recognition and other computer vision techniques. (R^{2}A 2017)

Innovation accelerator — supports early-stage, growth-driven companies through education, mentorship, and financing. Startups enter accelerators for a fixed period and as part of a cohort of companies. The accelerator experience is a process of intense, rapid, and immersive education aimed at accelerating the life cycle of young innovative companies, compressing years' worth of learning by doing into just a few months. (HBR 2016)

Innovaion hub/office — an Innovation facilitator set up by a supervisory agency that provides support, advice or guidance to regulated or unregulated firms in navigating the regulatory framework or identifying supervisory policy or legal issues and concerns. Unregulated entities can engage with regulators to discuss fintech-related issues (for example, sharing information and views) and seek clarity on complying with the regulatory framework and/or licensing requirements. (World Bank 2020a)

InsurTech — the insurance-specific branch of fintech that refers to the variety of emerging technologies and innovative business models that have the potential to transform the insurance business. (IAIS 2017)

Large Language Model (LLM) — a computational model notable for its ability to achieve general-purpose language generation and other natural language processing tasks such as classification.

Liability risks — Risks stemming from legal action taken against financial institutions that finance companies whose activities have negative environmental impacts.

Machine Learning (ML) — A field of study in artificial intelligence concerned with the development and study of statistical algorithms that can learn from data and generalize to unseen data, and thus perform tasks without explicit instructions.

Macroprudential supervision — supervision that considers the interactions among individual financial institutions, as well as the feedback loops of the financial sector with the real economy, including the costs that systemic risk entails in terms of output losses. (ECB 2014)

Market Development — The act of increasing the total market served by a company by finding new customers and markets or providing new products to existing customers and markets. (Cambridge 2022)

Market integrity — concerned with the capacity to pursue the 'dirty money' that flows through the global financial system, imposing a significant cost on national security, economic opportunity, and the rule of law. It is also connected with regulators' ability to uncover, prosecute, and prevent such movements in the future, as well as to restore official funds stolen in corruption to public coffers. (World Bank 2022)

Microprudential supervision — supervision that focuses on safeguarding individual financial institutions from idiosyncratic risks and preventing them from taking too much risk. (ECB 2014)

Natural language processing (NLP) — an interdisciplinary field of computer science, AI, and computation linguistics that focuses on programming computers and algorithms to parse, process, and understand human language. NLP is a form of AI. (FSB 2020)

Network analysis — the use of quantitative and qualitative data to model and draw insights regarding the formal and less-formal interconnections between a set of related entities, for example, a measure of the degree to which a financial system will be weakened by the cascading transmission of financial distress across institutions. (IMF 2010)

Open Banking — Refers to the way in which banks can make data and services available via interfaces (generally APIs) to authorised service providers or third parties who act on behalf of the customer who owns the account. (Open Banking Europe 2022)

Open Finance — A financial innovation that enables customer-permissioned access to and use of financial data held by institutions to provide new and enhanced services and develop innovative business models. It expands on open banking by including a broader range of financial products, such as investments, insurance and pensions. (FSI 2025)

Optical character recognition (OCR) — a specific form of computer vision that focuses on transcribing image data into textual data. Examples include license plate readers, OCR-enabled scanners and mobile apps, passport and other identification card readers, and file conversion tools. (R²A 2017)

Physical risks — The economic costs and financial losses resulting from the increasing severity events (such as heat waves, droughts, landslides, floods, wildfires and storms), as well as longer-term progressive shifts in the climate (such as ocean acidification, rising sea levels and average temperatures). (NGFS 2020)

Predictive analytics tools — the advanced analysis of historical data to create statistical models to predict future events, values, facts or characteristics. This process may include recommendation engines (tools where the prediction is an optimal value or action) and employ ML (computerised, iterative optimisation of the aforementioned statistical models). (TechTarget 2022)

Production Application — a fully deployed (production) application means that any unnecessary limitation of access during prototype stage have been removed. For example: access to all relevant supervisors across all relevant departments, integration with all relevant supervised entities, or access across all relevant channels for the public. (Cambridge SupTech Lab 2024)

Proof of concept (POC) — a Proof of Concept (POC) is a limited exercise (in both scale and scope) and resulting documentation aimed at demonstrating the feasibility and practicability of a technological solution to a problem; it is therefore often the first level of engagement between vendor/developer and user. Proof of Value (POV) exercises might build on a POC to demonstrate measurable business benefits, such as cost savings or improved performance relative to a baseline. A POC is built based on technical specifications, using dummy data, bare-bones architecture, and mock-up dashboards and visualizations. The POC serves to (i) establish consensus on the features that a final product would possess in an ideal world, (ii) draft specs that are intelligible to the technologists who will develop the eventual product; (iii) resolve ambiguities before decisions become hard to reverse; (iv) and determine the feasibility of the solution. (Cambridge SupTech Lab 2024)

Prototype (Working Prototype) — A working prototype is a live technology solution that demonstrates the end-to-end feasibility and tangible data product deliverables that can be tested and validated by the financial authority. (Cambridge SupTech Lab 2024)

Regulatory technology (regtech) — an acronym for 'regulatory technology'. It involves new technologies to help regulated financial service providers streamline audit, compliance and risk management and other back-office functions to enhance productivity and overcome regulatory challenges, such as the risks and costs related to regulatory reporting and compliance obligations. This can also refer to firms that offer such applications. (World Bank 2020a)

Robotic process automation (RPA) — the automation of the basic tasks defined by a user; these tasks can include filling forms and checking forms for completeness. (TechTarget 2022)

Sentiment analysis — a specific form of Natural Language Processing (NLP) that focuses on inferring the emotional content expressed in each corpus of text or transcribed speech. Examples include social media data mining to understand public sentiment surrounding a given topic or entity and analysing customer service requests/complaints to inform escalation. (R²A 2017)

Structured data — Data that are produced to a template and thus have consistent, predictable properties that are usually optimised for data processing by design; examples might be, e.g., a downloadable bank statement, a time series of share prices, or the readings from a seismograph. Structured data are typically numerical. Unstructured data, on the other hand, are typically qualitative / nominative in nature and require greater effort to process because they must first be forced into a template. Examples of unstructured data might include, e.g. work emails, meeting minutes, comments on online forums, social media content (e.g., tweets) or voice recordings. (Cambridge SupTech Lab 2022)

Suptech — an acronym for 'supervisory technology'. It is the application of technology and data analysis solutions to complement and enhance a financial authority's financial market oversight capabilities. Suptech applications are used by financial authorities to access more granular, diverse, timely and trustworthy data to improve operational efficiency and generate previously unattainable insights, thus improving decision-making. (Cambridge SupTech Lab 2022)

Text mining — the process of discovering interesting and useful patterns and relationships in large volumes of text. This process uses tools from statistics and AI. (IBM 2022)

Topic modeling - A method of unsupervised learning that uses natural language processing to let the data define key themes in a text. Topic modelling can efficiently identify hidden trends in large amounts of unstructured financial information. (BIS 2018)

Transition risks - Financial risks which can result from the process of adjustment towards a lower-carbon and more circular economy, prompted, for example, by changes in climate and environmental policy, technology or market sentiment. (NGFS 2020)

Web scraping — the process of using software to extract data from websites. (Cambridge SupTech Lab 2022)

APPENDIX 3.

Abbreviations

2G - 3G - 4G	Second - Third - Fourth Suptech Generation
A2A	Account-to-account
ABA	American Bankers Association
ADGM	Abu Dhabi Global Market
ACPR	Autorité de Contrôle Prudentiel et de Résolution
AE	Advanced Economy
AFA	Andorran Financial Authority
AI	Artificial Intelligence
AIDF	Asian Institute of Digital Finance
AMLA	Anti-Money Laundering Authority
AML/CFT	Anti-Money Laundering
API	Application Programming Interface
APP	Authorised Push Payment
APRA	Australian Prudential Regulation Authority
ASSAL	Association of Insurance Supervisors of Latin America
ASBA	Association of Supervisors of Banks of the Americas
ASIC	Australian Securities and Investments Commission
ADB	Asian Development Bank
AUSTRAC	Australian Transaction Reports and Analysis Centre
BCP	Business Continuity Plan
BCBS	Basel Committee on Banking Supervision
BI	Business Intelligence
BIS	Bank for International Settlements
BOE	Bank of England

BOJ	Bank of Japan
BMA	Bermuda Monetary Authority
BSP	Bangko Sentral ng Pilipinas
CASC	Canadian Anti-Scam Coalition
CBDC	Central Bank Digital Currency
CDD	Customer Due Diligence
CDO	Chief Data Officer
CFT	Counter-Terrorism Financing
CFPB	Consumer Financial Protection Bureau of the United States
CFTC	Commodity Futures Trading Commission of the United States
CGAP	Consultative Group to Assist the Poor
CHAPS	Clearing House Automated Payment System
COBIT	Control Objectives for Information and Related Technologies
CONSOB	National Commission for Companies &the Stock Exchange of Italy
CPF	Counter Proliferation Financing
CPMI	Committee on Payments and Market Infrastructures
CTO	Chief Technology Officer
CTR	Cash Transaction Report
DeFi	Decentralised Finance
DG	Data Governance
DLT	Distributed Ledger Technology
DNB	De Nederlandsche Bank
DORA	European Union Digital Operational Resilience Act
DPI	Digital Public Infrastructure
DTS	Digital Transformation Solutions
DX	Digital Transformation

EAP	East Asia and the Pacific
EBA	European Banking Authority
ECA	Europe and Central Asia
ECB	European Central Bank
e-KYC	Electronic Know Your Customer
EIOPA	European Insurance and Occupational Pensions Authority
EMDE	Emerging Market and Developing Economy
ESA	European Supervisory Authority
ESG	Environmental, Social, and Governance
ETL	Extract, Transform, Load
EU	European Union
EU-SDFA	European Union Supervisory Digital Finance Academy
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
Fintech	Financial Technology
FIRE	Format for Incident Reporting Exchange
FMA	Financial Market Authority
FNA	Financial Network Analytics
FSA	Japan's Financial Services Agency
FSB	Financial Stability Board
FSC	Jersey Financial Services Commission
FSS	South Korea Financial Supervisory Service
FSDU	Financial Sector Deepening Uganda
FSMA	Financial Services and Markets Authority
FSRA	Abu Dhabi Financial Services Regulatory Authority
FX	Foreign Exchange

GDPR	General Data Protection Regulation
GE	Gender Equality
GenAI	Generative Artificial Intelligence
GENIUS	Guiding and Establishing National Innovation for U.S. Stablecoins
GRC	Governance, Risk, and Compliance
G20	Group of 20
HFT	High-frequency trading
HIC	High-Income Country
HKMA	Hong Kong Monetary Authority
HTTPS	Hypertext transfer protocol secure
HR	Human Resources
IA	Insurance Authority
IAIS	International Association of Insurance Supervisors
ICT	Information and Communication Technology
IDB	Inter-American Development Bank
IFRS	International Financial Reporting Standards
IFSB	Brazilian Financial Health Indicator
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISSM	Mozambique Insurance Supervision Institute
IT	Information Technology
IReF	Integrated Reporting Framework
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
KYC	Know your customer
LAC	Latin America and the Caribbean

LIC	Low-Income Country
LfRA	Labeling for Retrieval Augmentation
LLM	Large Language Model
MAS	Monetary Authority of Singapore
MENA	Middle East and North Africa
MFI	Microfinance Institution
MSME	Micro, Small and Medium Enterprises
MiCAR	Markets in Crypto-Assets Regulation
MVP	Minimum Viable Product
ML	Machine Learning
MSME	Micro, Small, and Medium Enterprise
NBFIs	Non-bank financial institutions
NA	North America
NBR	National Bank of Rwanda
NCA	National Competent Authority
NGFS	Network for Greening the Financial System
NIST	U.S. National Institute of Standards and Technology
NLP	Natural Language Processing
NYDFS	New York Department of Financial Services
OAIC	Australian Office of the Australian Information Commissioner
OCR	Optical Character Recognition
OECD	Organisation for Economic Co-operation and Development
OeKB	Oesterreichische Kontrollbank
OeNB	Central Bank of the Republic of Austria
OJK	Financial Services Authority of Indonesia
ORSA	Own Risk and Solvency Assessment

PAPPS	Pan-African Payment and Settlement System
PDF	Portable Document Format
PEP	Politically Exposed Persons
PET	Privacy Enhancing Technology
PF	Proliferation Financing
POC	Proof of Concept
PSX	Pakistan Stock Exchange
RAG	Retrieval-Augmented Generation
RBA	Reserve Bank of Australia
RBI	Reserve Bank of India
Regtech	Regulatory Technology
RFP	Request for Proposals
RPA	Robotic Process Automation
RTGS	Real-Time Gross Settlement
SA	South Asia
SSA	Sub-Saharan Africa
SBP	State Bank of Pakistan
sDQI	Supervisory Data Quality Index
SACCO	Savings and Credit Cooperative Organization
SEC	Securities and Exchange Commission
SECP	Securities and Exchange Commission of Pakistan
SEBI	Securities and Exchange Board of India
SERC	Cambodian Securities Regulator
SFC	Hong Kong's Securities and Futures Commission
SFC	Financial Superintendency of Colombia
SFTP	Secure File Transfer Protocol

SQL	Structured Query Language
SSA	Sub-Saharan Africa
SSC	State Securities Commission of Vietnam
SSM	Single Supervisory Mechanism
ST	Suptech
STR	Suspicious Transaction Report
Suptech	Supervisory Technology
UI	User Interface
UK	United Kingdom
UAE	United Arab Emirates
US	United States
USD	United States Dollar
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNDP	United Nations Development Programme
UPI	Unified Payments Interface
UX	User Experience
VA	Virtual Asset
VASP	Virtual Asset Service Provider
WEF	World Economic Forum
XAI	Explainable Artificial Intelligence
XBRL	eXtensible Business Reporting Language
YOY	Year-on-year

www.cambridgesuptechlab.org

UNIVERSITY OF CAMBRIDGE
Judge Business School

Cambridge
Centre
for Alternative
Finance

CAMBRIDGE SUPTECH LAB

IN COLLABORATION WITH

DIGITAL
TRANSFORMATION
SOLUTIONS