

FSLN SUMMARY OF THEMES

From pilots to production: AI, cyber resilience, and the rise of regulated digital money

September 2026



2

Financial institutions are navigating a period of rapid technological change. Artificial intelligence is moving from experimentation into core business operations, creating new opportunities while raising urgent questions about cost, governance, accountability, and resilience. At the same time, AI is increasing the speed and scale of cyber threats, while stablecoins and tokenization are beginning to reshape financial infrastructure. Together, these developments are prompting boards and senior leaders to reconsider how their institutions create value, manage risk, and prepare for a more digital financial system.

On September 23 in Singapore, board directors and senior executives from leading financial institutions, along with EY leaders, regulators and subject matter experts, gathered for the inaugural meeting of the Financial Services Leadership Network in Asia-Pacific. Participants explored the state of AI deployment and the evolving cybersecurity landscape, and the rise of stablecoins and tokenization.¹

For a list of meeting participants, please see page 9.

[AI leadership depends on reinvention, not efficiency](#)

[AI investment is raising questions about costs, returns, and dependency](#)

[As AI agents gain autonomy, human accountability must keep pace](#)

[AI is accelerating cyber risk, challenging organizational defenses](#)

[Digital money is moving from the fringe to regulated financial infrastructure](#)

AI leadership depends on reinvention, not efficiency

As experimentation with AI gives way to deployment at scale, participants described leaders as those that combine top-down strategic direction with bottoms up experimentation and adoption across the workforce, anchor AI initiatives in the business rather than the technology function, and invest in data quality, permissions, and infrastructure before chasing use cases. Participants identified several markers that distinguish institutions positioned to lead:

- Build ahead of the curve.** Most institutions look at AI's current capabilities and costs and pilot accordingly. Leading institutions are more forward looking, launch different projects and initiatives early in the development of the technology, and position themselves to benefit as models improve and new use cases emerge. As one executive remarked, these institutions *"recognize that the technology will continue to improve and costs will come down. They start the journey early and keep moving. By the time those initiatives are live, the technology has advanced significantly, and they are already months ahead of their competitors."*
- Redesign workflows around AI.** Simply layering AI onto existing processes often yields only incremental improvements because those processes were designed for a workforce operating without AI. Some participants argue that the larger opportunity lies in redesigning workflows around new human-machine capabilities. Drawing on the history of disruptive technologies, an executive recalled how newspapers initially responded to the internet by putting their front pages online, replicating an existing product on a new medium, while others reinvented the product entirely. The same pattern is emerging with AI: *"The risk is that you don't reimagine your business on the basis of this being possibly the most disruptive technology that we've seen in our lifetimes."*
- Align AI with strategic priorities.** Leaders treat AI as a strategic issue, ensuring that AI efforts are mapped to where the organization creates distinctive value for the business. One participant warned that strategies amounting to *"we need to do AI"* without a clear link to business value are a recognizable failure pattern. An executive was blunt: *"If you're just treating it as an individual technical project, it's not going to give you a lot of benefit. It has to be a supporting factor to your business objective, and those have to be owned by business owners."*
- Consider the implications of customers using AI.** AI is putting new capabilities into the hands of customers and counterparties. It's also creating new agent-to-agent interactions, with AI assistants negotiating with institutions' service channels. Some participants believe these developments will reshape customer engagement in ways most firms have not yet planned for. One director described testing a bank's investment recommendation with a public AI model, which came back with a very

different assessment: *"So I'm taking a very different view as a customer from what the bank is selling me. How do we as institutions think about how the outside world is looking at our business using AI and how do we respond?"*

AI investment is raising questions about costs, returns, and dependency

AI investment continues to accelerate. One participant cited a forecast of worldwide AI spending reaching \$2.5 trillion in 2026, with infrastructure accounting for the largest share of investment. Within financial services, much of this spending remains focused on productivity gains in areas such as underwriting, claims, and payment processing. At the same time, institutions are confronting a broader set of questions that extend beyond adoption itself, including rising costs, demonstrating value, cyber resilience, vendor concentration, and technology dependency. Participants identified several practical considerations for navigating these challenges:

- **Control the cost side deliberately.** Although the price of using individual models and processing tokens has declined, institutions' total AI spending continues to rise as usage expands and firms absorb the broader costs of compute, cloud commitments, licensing, integration, data preparation, and deployment. Usage-based pricing also makes expenses difficult to forecast. As one participant noted, *"We've become much more deliberate about controlling costs. If you give everybody access to all the frontier models and tell them to go off and use them, it gets very expensive very fast. We're being deliberate about who gets access to various models, with cost controls, model controls, and closer oversight of usage."*
- **Measuring returns remains a challenge.** One director observed, much of AI's value lies in preventing adverse outcomes, particularly in areas such as cybersecurity, fraud, and operational risk, making its impact difficult to quantify: *"It's very difficult to measure that which you have avoided."* At the same time, participants stressed that organizations face growing pressure to demonstrate value and exercise cost discipline. As one executive observed: *"It's hard to measure the return; it's easy to measure the investment."*
- **Build in the ability to walk away.** Vendor lock-in is a shared concern, particularly as AI infrastructure is increasingly concentrated among a small number of providers with growing influence over pricing, financing, and access. To avoid becoming overly dependent on any single provider, several participants suggested creating an abstraction layer, a technical buffer between the tools employees use and the models behind them, that allows the firm to switch providers as capability and price shift. One noted: *"Anytime you're going to negotiate with an organization, it's*

essential to make sure you have the leverage to be able to walk away if price becomes an issue," particularly in a market where "it is definitely a horse race and different horses have their noses in front at different times."

- **Prepare for AI sovereignty and dependency risks.** Many institutions rely on frontier AI capabilities developed and controlled outside their home jurisdictions, raising questions about who controls access, under what circumstances it could be restricted, and what contingency options exist if critical services become unavailable. As one participant observed, *"The questions are coming now: who controls access? Who can close access? Is AI infrastructure and capability outside our control and our government's control? Who decides it can be restricted or withdrawn? What happens if that happens?"* Participants noted that these concerns are increasingly shaping regulatory discussions and national strategies. *"There were banks in a very large European country talking with their local regulators about whether they should maintain a utility core banking platform for that country. The cost of that is going to be enormous. This isn't just a US-China debate. You're seeing many jurisdictions now trying to come up with a sovereign answer, even if it is not as good as the frontier models."*

As AI agents gain autonomy, human accountability must keep pace

As AI shifts from answering questions to taking actions, governance and guardrails become even more important. Some participants saw a growing role for government intervention, noting, *"Recent research has shown that more than three-quarters of people in Western economies want AI to be regulated. Given that backdrop, I suspect we will see governments stepping in more actively than they have so far, whether that proves beneficial or not."* Others urged caution about what regulation would mean in practice: *"Regulation sounds like a fantastic idea in principle, but just understand what it is that you're asking for,"* one executive warned. This executive noted that existing frameworks, including executive liability for harm, may be sufficient, and that calls to slow down development may mask competitive motives. While views on regulation diverged, participants agreed that organizations cannot wait for regulatory clarity before strengthening their own governance frameworks. Participants identified several disciplines that warrant board attention as AI becomes more autonomous:

- **Demand clear ownership of every agent.** Boards should know that there is an owner of each AI initiative and each deployed agent, that there is a plan for what happens to that ownership when the person leaves, and how delegation works. One executive described the standard he would set as a director: *"I want to know who owns each single one... What is the agent allowed to do? Would we know if it went*

wrong? And can we stop it? Have we tested that?" With clear ownership comes unequivocal accountability: *"A human is accountable for an agent. There's no 'oh, sorry, AI did it and I didn't check it,'"* a participant said.

- **Oversight must extend beyond the model.** One executive cautioned against relying solely on a model's built-in safeguards, noting that outputs can change depending on the context and information provided. For consequential decisions, leading firms place controls around the model, such as through layered review processes: one model performs a task, a second validates the result, and disagreements are escalated to a human decisionmaker.
- **Preserve explainability and fairness through traceability.** In an industry built on trust, every AI-influenced decision, whether a credit determination or a product recommendation, must be traceable after the fact, with the digital equivalent of an audit trail. Participants noted that the technology for this is improving, but the volume of decisions is vastly larger than in human-only processes.

AI is accelerating cyber risk, challenging organizational defenses

AI is transforming the threat landscape. A participant stated that AI *"hasn't fundamentally changed cyber so much; what has changed is scope and speed."* Attackers are able to test for vulnerabilities with incredible speed and efficiency. This asymmetry favors attackers, who operate without governance constraints while defenders navigate budgets, priorities, and committees. As one participant put it, *"We've seen the bad guys move much, much faster than anyone can."* Participants discussed several implications for oversight:

- **Expect the resilience budget to keep rising.** *"Across financial services, the average we are now seeing is that 11% of the technology budget is devoted to cyber resilience, and that has doubled over the last several years."* Participants expected that trajectory to continue as AI amplifies both attack volume and sophistication.
- **Prepare for increasing AI-enabled fraud targeting customers and institutions.** AI-powered impersonation, including synthetic voices and other forms of digital deception, increasingly targets customers. One executive recounted a bank whose customer received a call from a voice that was indistinguishable from a family member claiming to be in financial distress. This participant suggested that such techniques will only become more compelling. However, the same models used for attacks are also beginning to identify fraud patterns that would be difficult for humans to detect. As the executive put it, *"This is an amoral technology. It will definitely be used as a sword. It needs to also be used as a shield."* Institutions may need to

rethink customer authentication, fraud detection, and customer-protection strategies on the assumption that AI-enabled deception will continue to improve.

- **Treat speed of response as the critical capability.** Large financial institutions can never prevent all attacks, making rapid detection and containment essential. But even the most sophisticated technology organizations have struggled to quickly detect and respond to AI-enabled breaches. While AI shows promise as a defensive tool, challenges remain: in one example cited, safety-trained models initially refused to assist defenders because the requests resembled offensive cyber activity.
- **Establish crisis protocols in advance.** The compressed timelines of AI-enabled attacks leave no room for deliberation mid-incident. As one participant advised, *"Make sure you prioritize and are clear on things you can decide on beforehand, because there is no time to decide on things in the middle of a crisis."*

Digital money is moving from the fringe to regulated financial infrastructure

The growing importance of digital money represents a second major technology shift on financial institution boards' agendas. Participants explored the modes of digital money now emerging, and how each serves a different purpose and operates across a different network. Central bank digital currencies are best suited as a trusted settlement layer between institutions, while tokenized bank deposits, digital representations of money held on a bank's balance sheet, are fit for wholesale and institutional use cases. Stablecoins, digital tokens designed to hold a stable value against a reference currency, are currently the most dynamic category. Their value in circulation has grown from less than \$10 billion in 2020 to more than \$300 billion in 2026, with approximately 98% denominated in U.S. dollars.³ As financial institutions weigh where and how to engage with digital forms of money, participants shared observations on how the space is evolving and oversight priorities:

- **Regulatory clarity is increasing stablecoin adoption.** As one participant observed, *"The more you have regulation and clarity stepping in, the faster it's scaling—the exact opposite of what the founders of decentralized finance expected... it comes down to trust."* Clear legal frameworks give users confidence that issuers are licensed, reserves are properly managed, and redemption rights are enforceable. New frameworks across the United States, Europe, and major Asian financial centers, have pulled institutional users decisively toward licensed, fully backed, transparent issuers. *"Banks that weren't so excited to talk before are much more interested in the technology now."*
- **Focus on areas where moving money is still slow, expensive, or operationally**

complex. The strongest opportunities today are in cross-border payments, remittances, and corporate treasury operations. Stablecoins can serve as a faster settlement layer between local currencies, helping move money across borders more efficiently and, in some cases, reducing collateral requirements and improving balance-sheet efficiency. As one participant observed, the greatest value is often found in “*higher cost, higher friction corridors*” where there is “*real value in cost savings.*”

- **Watch the convergence with AI.** Because stablecoins are programmable and divisible to tiny fractions of a dollar, participants argued that they are emerging as a preferred payment mechanism for AI agents acting on behalf of individuals and organizations. Potential use cases include micropayments for access to data, content, software, and other digital services that would be impractical to purchase through traditional payment rails. In this view, stablecoins could enable new forms of machine-to-machine commerce and automated transactions at a scale and granularity that would be difficult for humans to manage directly.
- **Hold the business case to the same standard as any other investment.** A participant suggested that any investment in the business of stablecoins needs to be rooted in the needs of the institution or its clients: “*Whether you think the tech is cool is not really the point. Is there a pain point and value add to your business?*” Without a genuine business case, the institution probably should not proceed.
- **Insist on controls built for always-on rails.** Networks that operate every hour of the day year-round require heavy oversight including compliance and sanctions monitoring that is programmed into the assets and processes themselves; real-time surveillance rather than periodic review; and a clear internal owner. Participants stressed that new digital-money arrangements should be subject to the same scrutiny and safeguards as traditional payment systems, including the ability to quickly suspend participation, halt transaction flows, or intervene if operational, compliance, security, or other issues emerge. To get comfortable, a participant suggested that any financial institutions exploring a new digital money arrangement should ask: “*What additional controls need to be in place? Can we switch it off instantly? How quickly can we shut it down if something goes wrong?*”

Reflection questions for senior financial services leaders

- Have we invested sufficiently in the infrastructure, data, security, and controls required to support AI innovation at scale?
- Where and how much are we investing in cybersecurity capabilities to defend against increasingly sophisticated AI-enabled attacks?
- What AI agents are operating across the organization today, who is responsible for them, and what happens if that individual leaves the firm?
- Would we know if an agent failed or behaved incorrectly, and how quickly would we know?
- How does our business change if customers, competitors, and partners are all using AI agents?
- How are we reimagining the business in response to what may be a foundational technology shift?
- As tokenization expands, which of our products, assets, or transactions could benefit from faster settlement, greater automation, or broader accessibility, and what advantages would that create for customers and the institution?
- How prepared are we for a future in which clients, counterparties, AI agents, and digital marketplaces increasingly transact using digital forms of money rather than traditional payment systems?
- Do we have the governance, compliance, and risk-management capabilities needed to operate in a 24/7 digital-asset environment, including sanctions screening, KYC/AML controls, interoperability risks, and real-time monitoring?

Meeting Participants

The following individuals participated in all or part of the meeting or related conversations:

Participants

James Allworth, Head of Innovation,
Cloudflare

Christine Fellowes, Non-Executive Director,
NAB

Shirish Apte, Remuneration Committee
Chair, Standard Chartered; Lead
Independent Director, Keppel; Audit
Committee Chair, Singlife

Mervyn Fong, Chair of the Board, Mizuho
Securities Asia and Mizuho Securities
(Singapore)

Eric Badger, Head of Southeast Asia and
Singapore Chief Executive, BNY

Kenneth Gay, Chief FinTech Officer,
Monetary Authority of Singapore

Michele Bang, Non-Executive Director,
Reinsurance Group of America

Euleen Goh, Non-Executive Director, HSBC
Bank plc

Arijit Basu, Non-Executive Director,
Prudential plc; Chair of the Board, IndusInd
Bank

Penny Goh, Board Chair, HSBC Bank
(Singapore) Limited; Remuneration
Committee Chair, Keppel

Harpreet Bindra, Chief Executive Officer,
HSBC Life Singapore

David Katz, Chief Executive Officer, Circle
Singapore

Sok Hui Chng, Chief Financial Officer, DBS

Patrick Lee, Chief Executive Officer,
Singapore and Chief Executive Officer,
ASEAN & South Asia, Standard Chartered

Bonghan Cho, Non-Executive Director, DBS

Huey Ru Lin, Non-Executive Director, SGX
Group

Martha Cummings, Nominating and
Corporate Governance Committee Chair,
Marqeta

Joseph Liow, Dean of the Lee Kuan Yew
School of Public Policy, National University
of Singapore

Michael Cutler, Fractional Chief Technology
Officer, AI Operating Lead, SC Ventures,
Standard Chartered

Boon Chye Loh, Chief Executive Officer,
SGX Group; Non-Executive Director, GIC

Karen Fawcett, Non-Executive Director,
LGT Group

Josephine Lok, Chief Executive Officer,
Mizuho Bank Singapore

Albert Ng, Audit and Risk Management
Committee Chair, Ping An Insurance; Audit
and Control Committee Chair, CICC

Winston Ngan, Non-Executive Director,
HSBC Bank (Singapore) Limited and United
Overseas Insurance

Robert Oates, Chief Risk and Compliance
Officer, HSBC Singapore

Ken Wye Saw, Non-Executive Director,
Citibank Singapore

Selwyn Scharnhorst, Executive Director,
Istari

Stanley Sia, Non-Executive Director,
Maybank Singapore

EY

Omar Ali CBE, Global Financial Services
Leader, EY

Nitin Datta, Singapore Technology
Consulting Leader; Partner, Data &
Analytics, EY

Nam Soon Liew, Asia East Deputy Regional
Managing Partner; ASEAN Managing
Partner; Singapore and Brunei Managing
Partner, EY

Joy Tan, Chair of the Board, Income
Insurance

Yen Yen Tan, Non-Executive Director,
Jardine Cycle & Carriage

Thomas Wilson, Country Manager,
President and Chief Executive Officer,
Allianz Ayudhya Assurance

David Wong, Non-Executive Director,
Frasers Property Limited

Chee Keong Yap, Risk Committee Chair,
Singlife

Albert Yip, Head of Technical Success,
APAC, OpenAI

Sumit Narayanan, Asia East Financial
Services Co-Leader; ASEAN Financial
Services Leader; ASEAN Financial Services
Consulting Leader, EY

Li Yun Seah, ASEAN Banking & Capital
Markets Leader; Partner, Assurance, EY

Jonathan Zhao, Global Insurance Leader,
EY

Tapestry Networks

Dennis Andrade, Chief Executive Officer

Tucker Nielsen, Managing Director

Tiffany Luehrs, Senior Associate

About this document

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc., and EY and the associated logos are trademarks of EYGM Ltd.

Endnotes

¹ **Use of Artificial Intelligence: Portions of this document may have been prepared with the assistance of artificial intelligence tools. All content has been reviewed and approved by Tapestry Networks.**

² *Summary of Themes* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from members and guests in connection with the meeting but may be edited for clarity.

³ European Central Bank, Christine Lagarde, "[Stablecoins and the Future of Money: Separating Functions from Instruments](#)," speech at the Banco de España LatAm Economic Forum, May 8, 2026,