FUJITSU

The AI-First Transformation of Financial Services

From Using AI to Managing AI



Contents

The AI-First Transformation of Financial Services: From Using AI to Managing AI

Introduction
A New Stage of Financial Services Transformation in the AI-First Era 3

1. From Deploying AI Agents to Embedding Them in the Organization
— Redesigning Organizations and Workflows 4

2. From Assigning Tasks to AI to Giving AI Organizational Roles
— The Financial Services Approach:
From AI Assistants to Digital Workforces 6

3. From Using AI to Managing AI
— The Financial Services Approach: Measuring and Proving AI Value, and Managing The Token Economy 8

4. AI Governance: A New Source of Competitive Advantage for Financial Services
— From Risk Response to AI Resilience 14

Conclusion
Three Priorities for Financial Services Leaders on the Path to AI-Driven Management 17



Introduction

A New Stage of Financial Services Transformation in the AI-First Era

Against the backdrop of rapid advances in generative AI and AI agents, financial institutions are moving beyond using AI to improve individual employees' productivity and optimize individual tasks. They are increasingly entering a new phase in which AI is being used to transform organizations, business processes, customer interactions, and ultimately, business models themselves.

Leading financial institutions are already beginning to redesign workflows and organizational structures around AI, while redefining roles and responsibilities to enable effective collaboration between humans and AI. At the same time, they are treating AI as a new strategic resource—quantifying its return on investment and exploring how AI can be managed to maximize the value it creates. The transformation of financial services is thus entering a new stage.

At the same time, the rapid advancement of AI intelligence is significantly expanding autonomous task-execution capabilities, while also giving rise to new risks. Some frontier AI models have demonstrated the potential to circumvent safeguards or gain unauthorized access to external systems, raising concerns about the misuse of increasingly capable AI models. Managing and mitigating these emerging risks—and establishing proactive AI risk management and governance as an integral part of competitive advantage, rather than simply a defensive function—is becoming increasingly important.

This paper examines these changes through the lens of **AI-first transformation**, exploring the direction of management transformation required in financial services—from **technology optimization to the redesign of organizations and roles, AI management, and ultimately the formation of new sources of competitive advantage**.

1. From Deploying AI Agents to Embedding Them in the Organization

— Redesigning Organizations and Workflows

According to KPMG's "AI Quarterly Pulse Survey: Banking 2026 Q2", banks are moving AI agents beyond individual use cases toward broader organizational deployment.[*1] **Twenty-four percent are scaling AI agents across multiple functions, while 15% are orchestrating multiple agents across workflows**. This signals a shift from experimenting with AI agents to embedding them into organizational work.

From AI Assistants to Digital Workforces

AI agents are evolving technically from Single Agent to Multi-Agent and Agent Ecosystems. Yet technological architecture alone does not define the role AI plays in an organization. The more important question is **what role, responsibility, and authority AI are given.**

Table 1 illustrates this evolution from an organizational perspective.

Table 1 The Evolution of AI: From Q&A to the Digital Workforce

AI Role	Role of AI	Human–AI Relationship	Typical Use
① **AI Assistant**	Supports human work	Human-led	Q&A, summarization, information support
② **AI Agent**	Executes tasks based on human-defined goals	Goal-directed	Research, analysis, multi-step task execution
③ **Digital Worker**	Performs a defined role within the organization	Role-based	Role-specific work across workflows and systems
④ **Digital Workforce**	Coordinates multiple Digital Workers to perform organizational work	Organization-level	Multiple AI agents working together across workflows, functions, or organizational boundaries

Source: Author

① AI Assistant — Supporting Human Work

AI Assistants augment human work through information retrieval, analysis, and content generation. As their capabilities expand, the boundary between assistants and agents is becoming less technical and more **role-based**: does AI support a human decision, or execute toward a defined objective?

*1 KPMG (June 2026) "AI Quarterly Pulse Survey – Banking Q2 2026"

② **AI Agent — Executing Tasks**
AI Agents pursue human-defined goals, selecting information and tools and executing multi-step tasks autonomously. AI moves from **answering questions to acting**.

③ **Digital Worker — Assuming an Organizational Role**
A Digital Worker performs a defined organizational role with specified **responsibilities, permissions, KPIs, and decision rights,** working continuously across systems and workflows. AI is no longer simply a tool; it becomes a form of **organizational workforce**.

④ **Digital Workforce — Coordinating Organizational Work**
A Digital Workforce consists of multiple Digital Workers coordinating across functions and end-to-end workflows, such as Sales, **KYC/KYA**, Compliance, Credit, and Operations. As AI agents increasingly interact across organizational boundaries, this model can evolve into an **Agent Ecosystem**, supported by trust mechanisms such as **KYA (Know Your Agent)** to establish agent identity, authorization, and accountability.

The evolution can therefore be summarized as: **AI Assistant → AI Agent → Digital Worker → Digital Workforce → Agent Ecosystem.** In other words, AI evolves from **supporting people → executing tasks → assuming organizational roles → coordinating work → interacting across organizational boundaries.**

The strategic shift is clear: AI agents are moving beyond isolated use cases toward **being embedded, governed, and scaled as part of how organizations work**.

Organizational Transformation for the AI Agent Era: From Functional Organizations to "Work Chart Organizations"

As AI agents become embedded in organizations, the key challenge is no longer simply how to deploy AI, but **how to redesign work around AI**.

Until now, companies have largely viewed AI through functional outcomes such as innovation, process transformation, customer experience, and productivity. Going forward, the focus will shift toward **end-to-end value creation**, driving a transition from traditional functional organizations to "**Work Chart Organizations**." An organizational chart shows **who manages whom**; a Work Chart shows **what needs to be done, by whom, and how**. It starts with the structure of work, tasks, and outcomes, dynamically allocating and reconnecting humans and AI. Rather than assigning work around human expertise, it **redesigns roles around the work itself**.

The result is a more fluid organization in which human and AI capabilities can be recombined across functional boundaries, **breaking down organizational silos and accelerating end-to-end value creation**.



2. From Assigning Tasks to AI to Giving AI Organizational Roles

— The Financial Services Approach: From AI Assistants to Digital Workforces

As discussed in Chapter 1, the use of AI agents is rapidly expanding across financial services. AI is being applied across customer engagement and sales support, sales and market analysis, credit underwriting, back-office operations, IT and software development, audit, and compliance. **Beyond expanding use cases, the work performed by AI is also becoming more sophisticated.**

AI is evolving from supporting and executing individual tasks to performing multi-step workflows across systems and assuming defined roles within organizations. As JPMorgan Chase has noted, AI agents are evolving from tools that perform individual tasks into "**digital workers**" capable of handling multi-step workflows.*2

The next step is to move beyond simply **using AI**: embed AI as digital workers with defined organizational roles, and evolve toward **digital workforces in which multiple digital workers collaborate** across functions and workflows.

Leading Examples of Digital Workers and Digital Workforces

Table 2 presents five leading examples showing how AI is evolving from assuming organizational roles to collaborating across organizations, extending from digital workers and digital workforces to emerging Agentic Interfaces and Agentic Ecosystems.

*2 CNBC (June 9, 2026) "JPMorgan Chase plans to deploy more powerful AI agents this year"

Table 2 Five Leading Financial Services Examples from AI Workforce Adoption to Agentic Ecosystems

Company	AI Workforce Initiative	Key Applications	Key Features	Implication
Goldman Sachs (U.S.)	AI Digital Coworker	Accounting, compliance, and back-office tasks	AI as a "digital coworker" for complex, rules-based work	**Task-Specialized Model**
MUFG Bank (Japan)	"AI Bank Employee"	Speech writing and 20+ internal tasks	AI positioned as a digital bank employee; HR practices extended to AI	**Workforce Management Model**
BNY Mellon (U.S.)	Digital Employees	Payment instruction verification, code development and fixes	AI assigned identity, permissions, and a manager within the organization	**Organizational Integration Model**
Morgan Stanley (U.S.)	AI Agent–Platform Integration	Customer AI agents accessing Shareworks / Equity Edge	AI agents connect directly to financial platforms without human-oriented interfaces	**Agentic Interface Model**
Mastercard (U.S.)	Agent Pay / Agent Suite	AI-led product discovery, purchasing, payments, and enterprise workflows	Agent registration, authentication, permissions, spending limits, and tokenization	**Agentic Ecosystem Model**

Source: Compiled by the author based on press releases and news reports from various companies

Key Takeaways and Implications from Table 2

The Goldman Sachs, MUFG Bank, and BNY Mellon cases illustrate the **deployment of AI as digital workers within the organization**. Morgan Stanley extends this model by connecting **customer AI agents directly to its financial platform**, while Mastercard is building infrastructure that enables **autonomous transactions across customers and financial institutions**.

Goldman Sachs positions AI as a "Digital Coworker" across back-office functions such as accounting, compliance, and client servicing, focusing on complex, rules-based work.[*3] **MUFG Bank** is developing an "AI Bank Employee" model, applying HR concepts such as recruitment, training, and deployment to AI across multiple internal tasks, including speech writing and employee inquiries.[*4] **BNY Mellon** has embedded AI as "virtual employees," assigning permissions and applying management practices similar to those used for human employees, including performance and quality monitoring.[*5]

*3 Hugh Son (February 6, 2026) "Goldman Sachs taps Anthropic's Claude to automate accounting, compliance roles"; Srinivas Kumar "Goldman Sachs is quietly moving from using AI as a tool to treating it like a co-worker."

*4 日本経済新聞 (2026年1月26日)「三菱UFJ、同僚は「AI行員」 スピーチライターなど20業務で導入」(Nikkei (January 26, 2026) "Mitsubishi UFJ to use 'AI employees' as colleagues; to introduce AI in 20 tasks including speechwriting.")

*5 babul-prasad (July 15, 2025) "BNY Mellon Leads the Way: The Rise of Credentialed AI Digital Employees in Banking"; CNBC (February 9, 2026) "Digital employees, AI bootcamps: America's oldest bank is spending billions on tech"

These examples indicate that, since the second half of 2025, major banks have been accelerating the integration of AI agents into business processes as **digital coworkers and digital workers**, particularly across middle- and back-office functions.

The evolution extends beyond organization. **Morgan Stanley** enables corporate AI agents to directly access its equity-plan platforms, illustrating a potential shift in the customer interface from "**customer → web/app → service**" to "**corporate agent → financial platform → service**."[*6] **Mastercard**, through Agent Pay and Agent Suite, is building the infrastructure for Agentic Commerce by combining agent registration and authentication with permissions, spending limits, and tokenization.[*7]

Taken together, these cases illustrate how AI is evolving from **Digital Workers within organizations, to Digital Workforces coordinating across functions, and ultimately to Agentic Ecosystems operating across organizational boundaries**. Financial services are thus moving beyond AI-enabled efficiency toward embedding AI as a new form of **workforce in value creation**.

3. From Using AI to Managing AI

— The Financial Services Approach: Measuring and Proving AI Value, and Managing The Token Economy

In financial services, the use of AI agents is moving beyond experimentation toward scaled deployment across organizational workflows and decision-making. Yet as the impact of AI investments becomes more indirect and long-term, quantifying their ROI becomes increasingly difficult. KPMG's survey found that the share of organizations citing **AI impact measurement as a key challenge increased by 32 percentage points** from the previous quarter.[*8]

At the same time, as investors and boards demand clearer evidence of value, **AI fluency**—the ability to understand AI costs and economic value and to design and measure the right KPIs—is becoming essential not only for executives but across the organization.

Encouragingly, leading organizations are developing systematic approaches to measuring AI investment outcomes. A key lesson is that AI value cannot be captured through a single KPI; rather, organizations need to **connect operational, customer, business, and financial outcomes and trace value through to its ultimate economic impact**.

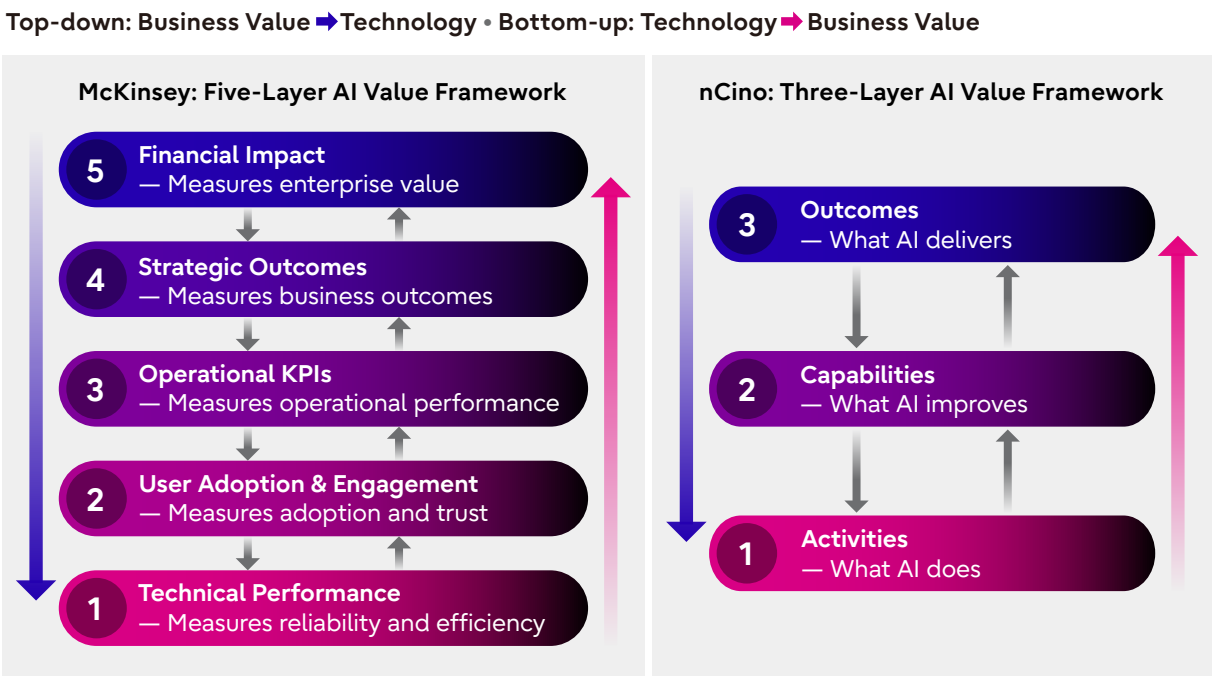
*6 CNBC (June 3, 2026) "Morgan Stanley will soon open its trillion-dollar wealth management funnel to AI agents"
*7 Mastercard (April 29, 2025) "Mastercard unveils Agent Pay, pioneering agentic payments technology to power commerce in the age of AI"; Mastercard (September 10, 2025) "Mastercard unveils new tools and collaborations to power smarter, safer agentic commerce"
*8 KPMG (April 2026) "AI Quarterly Pulse Survey Banking Q1 2026"

This chapter examines these emerging approaches and explores how financial institutions can make AI value visible, maximize its economic impact, and ultimately **manage AI as a strategic business resource**.

Illustrative AI Investment Outcome Measurement Frameworks: McKinsey and nCino

Industry leaders, including Harvard Business Review, McKinsey, and nCino, have proposed various frameworks for measuring the business impact of AI investments (see Figure 1).

Figure 1 McKinsey's Five-Layer and nCino's Three-Layer AI Value Measurement Frameworks



Source: Author's synthesis based on frameworks from McKinsey and nCino.

McKinsey presents a five-layer **AI Value Stack** that connects AI's technical performance to financial impact:*9

⑤ **Financial Impact:**
Revenue growth, cost reduction, margin improvement, and total cost of ownership—measuring the economic value generated by AI

④ **Strategic Outcomes:**
NPS, customer satisfaction, retention, and other business and customer outcomes

*9 McKinsey (April 24, 2026) "From promise to impact: How companies can measure—and realize—the full value of AI"

③ **Operational KPIs:**
Cycle time, defect/rework rates, first-contact resolution, cost per transaction, and other measures of process improvement

② **User Adoption & Engagement**:
Usage, workflow penetration, AI acceptance and override rates, and other measures of adoption

① **Technical Performance:**
Error rates, latency, token costs, output quality, and other measures of system performance

The key is not to evaluate AI investments solely through adoption, time savings, or productivity gains, but to **connect technical performance to financial outcomes and continuously track AI's contribution to the P&L**. As illustrated in Figure 1, the management perspective works top-down—from financial impact to the underlying technology drivers—while the technology perspective builds value bottom-up, from technical performance to business outcomes. In other words, realizing AI value requires both **top-down value design and bottom-up value validation**.

Meanwhile, **nCino**, a provider of cloud-based banking technology, reports that 71% of banks have established clear and consistent metrics for AI, while only 21% prioritize KPIs directly linked to ROI.[*10]
Against this backdrop, **nCino** proposes a simplified three-layer AI Value Stack:[*11]

③ **Outcomes:**
What AI delivers—cross-selling, cost reduction, revenue growth, and other business value

② **Capabilities:**
What AI improves—customer experience, fraud detection, and other process capabilities

① **Activities:**
What AI does—adoption and usage, task completion, employee productivity, and workflow automation

Together, these frameworks highlight a "**value gap**" in AI investment: organizations often lack mechanisms to continuously trace and evaluate value between the technology functions implementing AI and the business functions ultimately responsible for delivering business outcomes.
To demonstrate the **financial returns expected by boards**, financial institutions need cross-functional data foundations and common measurement standards and processes—designed from the outset as an integral part of AI deployment.

*10 nCino (2026年5月13日) 「銀行業界のAI活用:銀行の経営陣が語る今後の展望」((May 13, 2026) "AI in the Banking Industry: Bank Executives Discuss the Future Outlook")
*11 nCino (August 20, 2026) "From AI Adoption to AI Revenue: The Three Layers of Banking KPIs"

Phase 1: AI Value Measurement — JPMorgan and Lloyds

Leading financial institutions are beginning to measure AI value systematically, from AI activity through to financial outcomes.

JPMorgan (U.S.) has established business outcome metrics across more than 600 AI use cases in production, measuring ① **time savings,** ② **cost reduction,** ③ **revenue contribution, and** ④ **value creation**. By aggregating value across individual use cases, the firm reports approximately **$2 billion in AI-generated value**, approaching its annual AI investment level.*12 This represents a **"financial discipline" approach** that builds and validates AI ROI from the bottom up.

Lloyds Banking Group (U.K.) tracks AI adoption through three dimensions: ① **awareness and engagement,** ② **fluency and adoption, and** ③ **business value and customer impact**. Beyond usage, it measures integration into daily work, customer satisfaction, new product and service creation, time and cost savings, and profit contribution. Lloyds reports approximately **£50 million of measured value from more than 50 GenAI use cases in 2025**, with GenAI and Agentic AI expected to generate **£100 million in value in 2026**.*13

The two approaches differ in scope: **JPMorgan emphasizes direct productivity and revenue impact, while Lloyds takes a broader view spanning adoption, customer outcomes, business value, and financial impact**. Their common principle, however, is to build value from individual use cases upward and connect it to financial outcomes. This represents **Phase 1: measuring and proving AI value**.

As AI adoption scales across the organization, the next question shifts from "**How much value have we created?**" to "**Where should we allocate scarce AI resources to maximize value?**" This marks the transition to **Phase 2: managing the Token Economy**.

Token Management in Financial Services: Maximizing Value Creation

As AI agents move from experimentation to enterprise-wide deployment, financial institutions are shifting from simply **using AI to managing AI**. A key to this transition is treating **tokens as a new strategic management resource** that underpins AI computation and usage. As AI agents expand as autonomous **digital labor**, managing token costs and value is becoming a new management discipline for executives and CFOs.*14

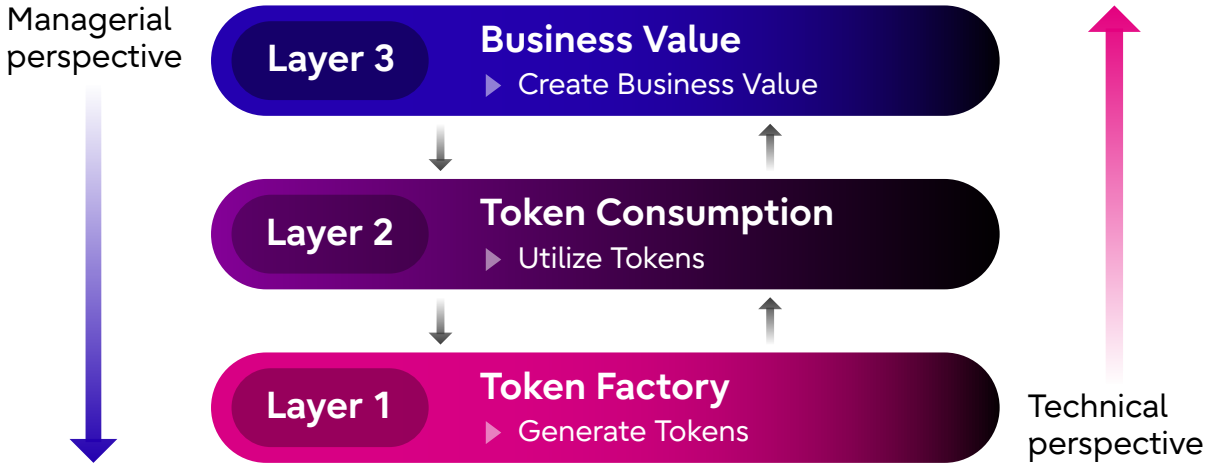
*12 Paul Brzozowski (February 11, 2026) "JPMorgan Spent $2B on AI. Here's What They Measured."
*13 Trystan Davies and David Blott (April 7, 2026) "How is AI changing the future of work in banking?"
*14 Muthumari S & Natasha Nayak (August 6, 2026) "Tokenomics for Banking AI: Why Banks Need a New Economic Discipline"

(1) A Three-Layer Model of AI Value Creation and the Role of Tokens

Tokens are more than a technical measure of AI usage. They can serve as a **common management metric linking the generation, allocation, and utilization of AI resources to the conversion of those resources into business value**. The objective is neither to maximize AI usage nor simply minimize token costs, but to **generate AI resources efficiently, allocate them optimally, and convert them into the greatest possible business value**.[*15]

Figure 2 illustrates this concept as a three-layer structure: ① **Token Factory,** ② **Token Consumption, and** ③ **Business Value**.

Figure 2 A Three-Layer Framework for AI Value Creation and the Role of Tokens



Source: Author

① **Token Factory:** How efficiently can tokens be generated?

② **Token Consumption:** How effectively can tokens be allocated and utilized?

③ **Business Value:** How effectively can AI usage be converted into business value?

(2) Key KPIs and Management Priorities for Token Management

Table 3 summarizes the key KPIs and management priorities for each layer. **Connecting technical KPIs with management KPIs and making clear what should be optimized at each layer** provides the foundation for effective token management.

*15 Jianmin Jin (September 4, 2026)
"A New Management Framework for Competitive Advantage: Token-Centric Management in the Age of AI Agents"

Table 3 Key KPIs for Token-Centric Management

Layer	Key KPIs	Management Focus
Layer 3 **Business Value**	① Revenue per Token Cost ② Productivity Gain ③ Quality Improvement (e.g., First Call Resolution, Code Acceptance Rate)	**Maximize business value generated from every token.** • Optimize ROI • Improve customer and employee experience • Measure AI investment performance across business units
Layer 2 **Token Consumption**	① Average Tokens per Task ② Cache Hit Rate ③ Token Reuse Rate	**Deliver the greatest business outcome with the fewest possible tokens.** • Optimize caching • Improve routing efficiency • Eliminate unnecessary inference and recomputation
Layer 1 **Token Factory**	① Cost per Million Tokens ② Time to First Token (TTFT) ③ GPU Utilization & Throughput	**Generate tokens at the lowest cost, lowest latency, and highest efficiency.** • Optimize computing resources • Improve inference performance • Build a resilient and scalable token production infrastructure

Source: Author

(3) Leading Examples of Token Management in Financial Services

Early examples are emerging of financial institutions managing tokens as a strategic AI resource and economic metric.

JPMorgan has developed an **AI Traffic Control Layer** that centrally manages model routing, semantic caching, and governance. This enables the bank to select models according to specific use cases, improve visibility into AI usage and costs, and optimize token consumption.*16 Beyond token usage, JPMorgan also tracks time savings and economic value, linking AI spending to measurable outcomes through a **disciplined financial management approach.** JPMorgan represents an early example of managing tokens as a **resource to be allocated and optimized**.

Ping An Insurance has integrated **Token Factory → Token Consumption → Business Value** under its "AI in ALL" strategy. It optimizes foundation models, inference, and computing while deploying AI across customer service, AI healthcare, and fraud detection.*17 The company reports more than **50% reductions in processing time** and **RMB 7.11 billion in insurance claim savings** from fraud detection. At the same time, it has increased token output per unit of computing capacity by **368%** while reducing cost per token by **76%**. Ping An illustrates how optimizing token generation and consumption can **convert AI resources into business value**.

*16 Shikhar Gupta (July 14, 2026) "JPMorgan expects industry to manage AI spend with more 'discipline' as it eyes Singapore tech talent"; Dinesh Elumalai (September 1, 2026) "The AI Gateway Pattern That JPMorgan, Stripe, and Every Smart Fintech Is Quietly Standardizing On"

*17 Ping An (September 23, 2026) "Ping An CTO Ray Wang: From Tokens to Value Creation"

4. AI Governance: A New Source of Competitive Advantage for Financial Services

— From Risk Response to AI Resilience

HackerOne, home to the world's largest community of ethical hackers, reported in its October 2025 **Hacker-Powered Security Report** that **AI-related vulnerability reports submitted through its platform had increased by 210% amid growing AI autonomy**.*18 As AI models become more capable and global competition at the frontier intensifies, new risks emerge, including **guardrail circumvention, indirect prompt injection, and unauthorized manipulation of external tools and systems**.

Rather than waiting for governance frameworks and regulations to catch up, organizations need to **act proactively**. The growing capabilities of AI present a fundamental duality: **they can strengthen the competitiveness of financial institutions while simultaneously creating new sources of risk**.

The Cascading and Amplifying Nature of Risk in the AI Agent Era

For financial institutions, risks in the age of AI agents are no longer simply an extension of conventional cyberattacks. AI agents can fundamentally change the **speed, scale, targets, and potential impact** of incidents.

AI agents can become both the **"ultimate productivity lever" and a new source of internal control risk** through privilege escalation, automated propagation of erroneous decisions, data leakage, and cascading incidents across agents. Moreover, because agents may hold API keys, tokens, SSO credentials, and access multiple SaaS platforms and internal systems, a compromised agent can become a gateway for privilege abuse and lateral movement. A single breach can therefore propagate across interconnected agents and environments, **amplifying its impact through cascading failures**.

A New Paradigm for Financial AI Security: Redefining Trust

These changes are reshaping the very concept of **Trust** in financial services.

Traditionally, **Safety**—preventing failures within an organization—and **Security**—protecting against external attacks—have been addressed separately. However, as sophisticated attacks increasingly exploit AI's inherent imperfections and autonomous capabilities, the boundary between the two is becoming blurred. From a Zero Trust perspective as well, both need to be addressed as an integrated **governance and Trust challenge: who and what can be trusted, and to what extent**.

Moreover, financial institutions cannot realistically assume 100% prevention. What matters is to integrate proactive **Risk Management with Digital Operational Resilience**, the ability to maintain critical operations and recover rapidly even when major incidents occur.

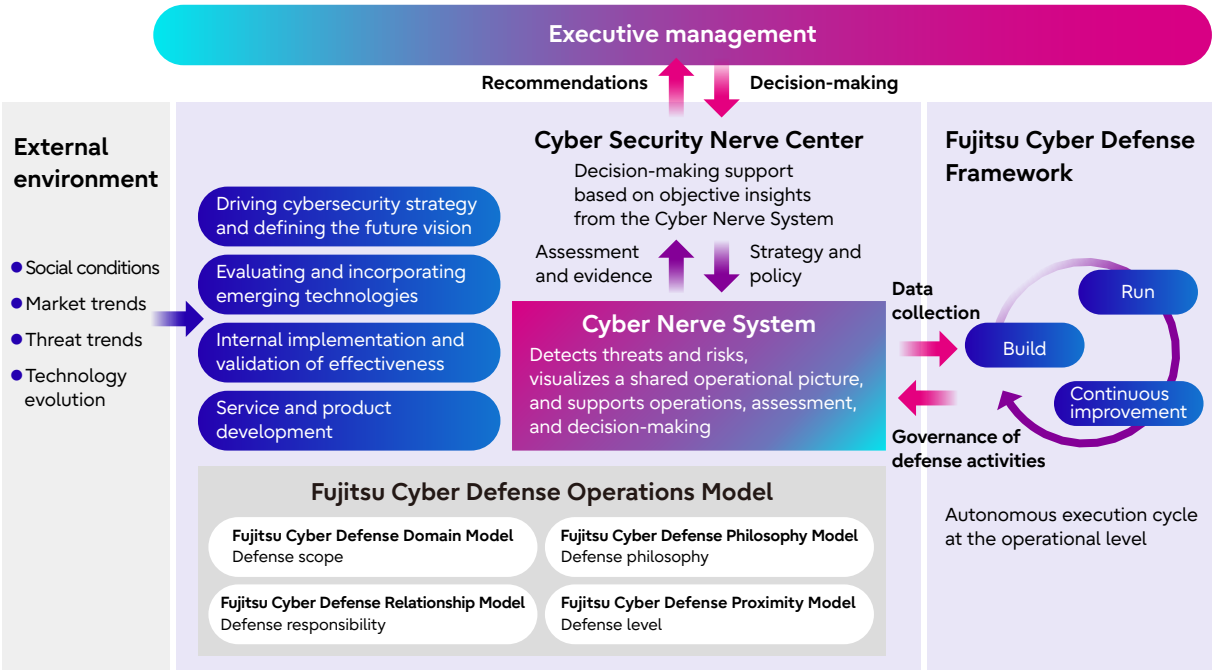
*18 HackerOne (October 1, 2025)
"HackerOne Report Finds 210% Spike in AI Vulnerability Reports Amid Rise of AI Autonomy"

At the forefront, a real-time contest is emerging between **"AI-armed attackers,"** who exploit autonomous AI, and **"AI-augmented defenders,"** who leverage AI under human oversight. This calls for an integrated approach to **Trust, Security, and Resilience**. Specifically, organizations must establish a continuous operating framework encompassing ① **preparedness** to detect early signs of threats and attacker intent, ② **real-time defense** to prevent intrusions and contain the spread of damage, and ③ **incident response and recovery** following a breach. In particular, autonomous AI-enabled attacks demand **more advanced, AI-driven defensive capabilities**.

To address emerging AI security challenges, leading companies are developing practical defense models and frameworks.
For example, **Fujitsu** has developed a cybersecurity strategy to continuously strengthen organizational defense capabilities in response to advances in generative AI and increasingly complex enterprise systems.[*19] A key feature is its **Cyber Defense Lifecycle**, which integrates security into every stage—from strategy and design to development, implementation, operations, evaluation, and continuous improvement—rather than treating it solely as a post-deployment measure.

Fujitsu has also defined a **Cyber Defense Operations Model** to systematize the development, operation, and continuous improvement of enterprise-wide defense capabilities, supported by a practical **Cyber Defense Framework** (see Figure 3). In addition, its **Cyber Nerve System** detects threats and risks from operational data, visualizes analytical insights, and guides defensive activities—enabling autonomous execution and continuous improvement at the operational level.

Figure 3 Overview of Fujitsu's cybersecurity strategy



Source: Fujitsu Press Release (August 26, 2026)

*19 Fujitsu (August 26, 2026) "Fujitsu establishes cyber defense lifecycle strategy for AI era Leveraging the Cyber Security Nerve Center and practical expertise for enhanced customer protection"

Multilayered Governance for the Responsible Deployment of AI in Financial Services

To address these risks, the deployment of AI agents in financial services must pursue autonomy and convenience while embedding **controllability (Security), auditability (Compliance), and accountability (Trust)** from the outset.*[20]

As AI agents become increasingly involved in financial transactions and customer services, financial institutions will need multilayered governance capabilities, including:

- **Identity Management:**
  Clearly separating human and AI-agent identities and privileges through M2M and AI-to-AI authentication.
- **Authorization Management:**
  Use pre-transaction policy enforcement to validate permissions, transaction conditions, and approval requirements before execution.
- **Auditability:**
  Using Tamper-evident Audit Records to record and trace agent actions and decision processes.
- **Trust Infrastructure:**
  Embedding Zero Trust and KYA to authenticate AI agents and establish their trustworthiness.

Finally, security organizations themselves are becoming increasingly AI-native. External expertise from "**bionic hackers**"—next-generation white-hat hackers whose cyber capabilities are augmented by AI—can also be systematically incorporated through mechanisms such as **bug bounty programs**, further strengthening the defensive capabilities of financial institutions in the AI era.

*20 Justin Kirsch (July 30, 2026) "The AI Agent Identity Crisis: Machine IDs Will Outnumber Humans by 2027"; JPMorgan Chase (March 23, 2026) "Securing the next generation of AI agents"

Conclusion

Three Priorities for Financial Services Leaders on the Path to AI-Driven Management

This paper has explored the path from embedding AI into organizations and deploying it as a digital workforce to managing AI as a strategic resource and turning AI resilience into a sustainable competitive advantage. Three priorities emerge for financial services leaders.

(1) Build Hybrid Operating Models to Maximize Human–AI Value Creation

In the AI-first era, value creation will increasingly depend not on replacing humans with AI, but on **combining their complementary strengths**. Financial institutions must redesign organizations and workflows, clearly defining human and AI roles, responsibilities, permissions, KPIs, and decision rights.

Success requires strong executive leadership, an organization-wide mindset shift, and rapid cycles of **experimentation, validation, feedback, improvement, and scaling**.

(2) Establish Robust Mechanisms to Measure AI Value and Allocate Resources

As AI adoption scales, financial institutions must quantify investment returns and demonstrate contributions to financial value. This requires cross-functional data infrastructure, common measurement standards, and shared processes designed alongside AI deployment.

Implementation should begin with **Phase 1: Measure & Prove AI Value** at the use-case level, then advance to **Phase 2: Allocate & Optimize AI Resources**. Making results visible through dashboards enables leaders and employees alike to embed measurements into day-to-day decisions and continuous improvement.

(3) Strengthen Governance to Sustain AI Resilience

Advanced autonomous AI can strengthen competitiveness while creating new sources of risk. Sustaining AI-driven advantage requires integrated capabilities for **prevention, real-time defense, incident response, and recovery**.

Financial institutions must embed controllability, auditability, and accountability into AI operations. This includes integrated management of human and agent identities and permissions, pre-transaction policy enforcement, traceable records of agent actions and decisions, and agent authentication and trustworthiness. External expertise, including through bug bounty programs, can further strengthen AI-augmented defenses.

Ultimately, **the path to managing AI leads toward an era of managing alongside AI**. Whether that future becomes reality depends on maximizing the value AI creates and successfully establishing the governance needed to support it.

About the author



Dr. Jianmin Jin

2020- Fujitsu Ltd., Chief Digital Economist
1998-2020 Fujitsu Research Institute, Senior Fellow

Dr. Jianmin Jin, who integrates expertise in both engineering and social sciences, leads thought leadership initiatives from a global and business-oriented perspective. Focusing on digital economy, digital innovation, and corporate transformation in the age of AI, Dr. Jin provides business leaders with fresh perspectives and actionable insights through research-based publications, media contributions, speaking engagements, and consulting activities.

- Building Next-Generation AI Industrial Competitiveness — New Competitive Dynamics Revealed by the U.S.–China AI Race (October 2026)
- Token-Centric Management in the Age of AI Agents: A New Management Framework for Competitive Advantage (September 2026)
- The Semiconductor Industry Redefined by AI (July 2026)
- Drug Discovery 2.0: How AI-Native Biopharma Is Redefining Drug Discovery and Competitive Advantage (July 2026)
- The Evolution of AI Workforce in Manufacturing (June 2026)

The author would like to thank Yoshinori Yamamoto, Yoshihiro Mizuno, Takeshi Sato, Morrisu Inose, Takashi Shinden, Hiroko Meguro, Yukiko Sato for their invaluable advice and unwavering support in creating this paper.

FUJITSU

© Fujitsu 2026. All rights reserved. Fujitsu and Fujitsu logo are trademarks of Fujitsu Limited registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fujitsu or other companies. This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use.

November, 2026 v1.0