FORRESTER®

The Architecture Of Trust: Enabling Modern FRAML Operations With Hybrid And Cloud-Native Approaches

A Strategy For Balancing Innovation And Control In A New Era Of Risks And Regulations

Get started →

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY RED HAT | SEPTEMBER 2025

Architectural Transformation Is Essential For Modernizing FRAML Operations

Banks face a rising volume of coordinated, cross-channel threats that evade detection by existing fraud and anti-money laundering (FRAML) systems. At the same time, regulators expect real-time, integrated, and auditable controls. Traditional environments, often siloed and built on inflexible infrastructure, are no longer sufficient. Modernizing FRAML operations goes beyond adopting advanced detection models or layering on new tools. It requires deeper architectural change, starting with data interoperability, deployment flexibility, and secure, scalable foundations.

Two strategies stand out: Hybrid cloud which helps banks match workloads to the right environment, and cloud-native on-prem which brings agility and scalability to systems that cannot move to the cloud. This study explores how leading banks balance innovation with control and shows that successful modernization hinges on architectural decisions that enable flexibility, resilience, and compliance.

Key Findings

Banks modernize through architectural strategies that balance agility and control; blending cloud innovation with compliance, operational reliability, and strong governance frameworks.

Fragmented data, rigid systems, and slow updates hinder FRAML. These make flexibility, real-time access, and streamlined deployment key to building resilient and future-ready financial defenses.

Hybrid cloud and cloud-native on-prem are complementary strategies that help banks modernize across environments while meeting data residency, regulatory, and integration requirements.

Concealed And Coordinated Threats Demand More Adaptive FRAML Controls

Banks face growing pressure to detect subtle, high-volume threats that exploit gaps in legacy FRAML controls. Respondents cited social engineering and layered small-value transactions as top threats. These tactics mimic regular behavior and overwhelm rules-based systems with volume and complexity, impeding detection.

These risks reflect a broader shift toward more agile and coordinated financial crime. Respondents also flagged cryptocurrency misuse (notably within wealth management), synthetic identities, and bot-driven attacks as major concerns. These threats bypass standard thresholds, exploit cross-channel blind spots, and manipulate detection logic at scale.

They expose the limits of traditional FRAML architecture, which struggle with the subtlety, spread, and scale of modern financial crime. To stay effective, banks must rethink how these systems are architected for an evolving risk environment.

"How have the following trends contributed to an increase in fraud or money laundering risk at your organization? (Select one per row)"

82%	Use of social engineering and scams targeting customers
82%	Use of layered small-value transactions to avoid AML thresholds
76%	Growth of cryptocurrency or virtual asset exposure
76%	Proliferation of synthetic identities and mule accounts
70%	Fraud rings using bots or automation to exploit systems

Note: Showing only top five results for respondents who selected "High contribution" and "Very high contribution".
Base: 222 business and IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

Top Two Trends That Contributed To An Increase In FRAML Risk Across Banking Segments

	Wealth management n=37	Retail banking n=76	Investment banking n=54	Corporate banking n=55
1.	**87%** Growth of cryptocurrency or virtual asset exposure	**82%** Use of layered small-value transactions to avoid AML thresholds	**87%** Proliferation of synthetic identities and mule accounts	**89%** Use of layered small-value transactions to avoid AML thresholds
2.	**87%** Use of social engineering and scams targeting customers	**80%** Use of social engineering and scams targeting customers	**83%** Use of social engineering and scams targeting customers	**78%** Use of social engineering and scams targeting customers

Note: Showing only results for respondents who selected “High contribution” and “Very high contribution”.
Source: Forrester’s Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

Regulatory Pressures Are Reshaping FRAML Operations And Governance

Eighty-one percent of leaders cited that stronger global sanctions have a high degree of impact on their organization's FRAML operations. Financial institutions are increasingly required to enhance screening coverage across jurisdictions, account types, and counterparties, especially where ownership structures and crypto-related exposures complicate compliance.

In parallel, 78% of respondents pointed to a regulatory push for more integrated FRAML risk management, where siloed systems and fragmented investigations are viewed as control gaps. Regulators are also signaling the need for stronger risk governance, coordinated escalation protocols, and cross-institution intelligence sharing to combat financial crime in the ecosystem.

These findings indicate that compliance obligations are expanding beyond traditional FRAML boundaries and require changes across operations, technology, and governance structures.

Expected Extent Of Impact Each Regulatory Development Will Have On Organizations' FRAML Operations

Note: Showing only top five responses for respondents who selected "High contribution" and "Very high contribution".
Base: 222 business and IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

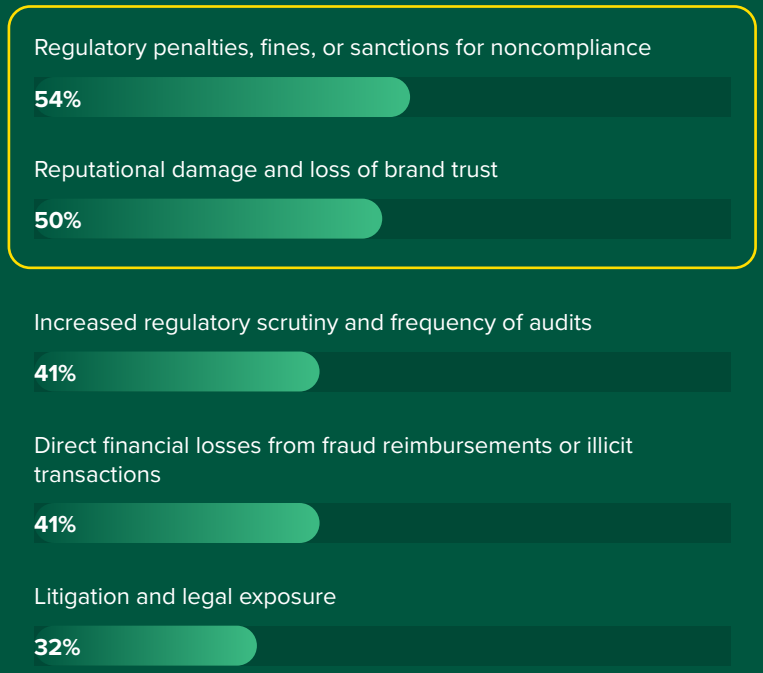
Rising Scrutiny And Harsher Consequences Are Elevating FRAML On The Risk Agenda

As noncompliance increases financial and reputational consequences, FRAML systems are evolving from back-office tools to core financial controls. Over half of respondents cited financial risk from regulatory breaches (54%) and reputational damage (50%) as a top concern. Banks in Singapore are now also financially liable for fraud losses under legislation like the Shared Responsibility Framework.

When reimbursement or restitution is required, demands for system performance increase. Banks must detect incidents in real time, manage cases consistently, and ensure traceable resolution across channels. These needs raise the bar for architectural standards and strengthen the case for event-driven systems built for agility and reliability.

Architecture also shapes how quickly banks can detect, contain, and explain incidents: Integrated and auditable platforms enable faster resolution and more transparent communication with regulators and stakeholders.

Top Three Important Consequences From Failing To Effectively Identify And Address Fraud And Money Laundering Activity



Base: 222 business and IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

Top Two Consequences From Failing To Effectively Identify And Address Fraud And Money Laundering Activity Per Region

	East Asia (Hong Kong, Japan, South Korea, Taiwan) n=88	SEA (Indonesia, Malaysia, Singapore, Thailand) n=71	Australia n=31	India n=32
1.	**52%** Regulatory penalties, fines, or sanctions for noncompliance	**56%** Regulatory penalties, fines, or sanctions for noncompliance	**61%** Reputational damage and loss of brand trust	**59%** Increased regulatory scrutiny and frequency of audits
2.	**52%** Reputational damage and loss of brand trust	**45%** Direct financial losses from fraud reimbursements or illicit transactions	**48%** Regulatory penalties, fines, or sanctions for noncompliance	**56%** Regulatory penalties, fines, or sanctions for noncompliance

Note: Results aggregated from top three consequences selected by respondents in each region.
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

FRAML Teams Must Bridge Fragmented Systems And Teams To Address New Risks

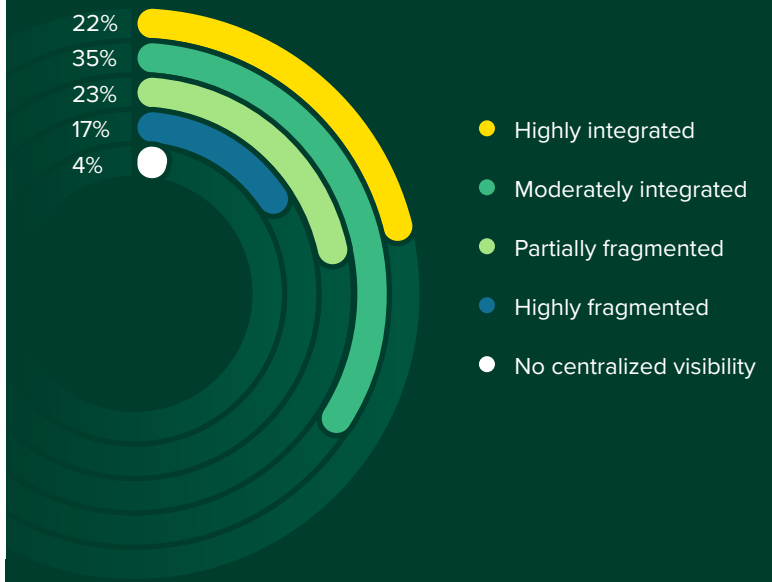
External pressures from evolving threat actors, regulatory scrutiny, and declining public trust are prompting banks to move toward more unified FRAML models.

Yet, only 22% reported that their organization has highly integrated FRAML operations, with most indicating the presence of fragmented teams and limited coordination across risk functions.

This fragmentation reflects both structural constraints and deliberate choices. Few vendors offer end-to-end FRAML capabilities and many banks rely on a patchwork of best-of-breed tools for needs like transaction monitoring or adverse media screening. In-house development, regional autonomy, and legacy systems add to the complexity.

Still, integration should not be pursued for its own sake. Banks should focus on strengthening the connective tissue that links detection logic, streamlines investigations, and enables a consistent view of customer risk across functions.

"How well-architected are your organization's FRAML systems and teams in terms of sharing data and maintaining a unified view of customer risk across products and channels? (Select one)"



Base: 222 business and IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

FRAML Integration Requires Structure-Agnostic Architecture

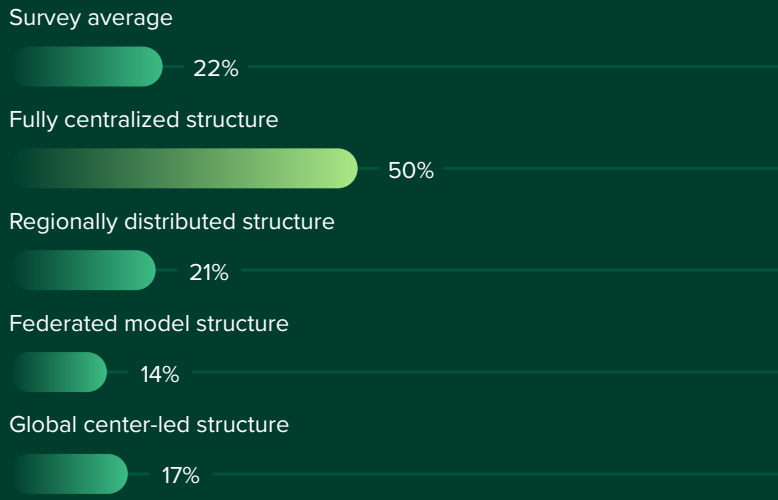
Respondents from fully centralized FRAML teams were far more likely to report highly integrated FRAML systems (50%) compared to those in regional or federated models (21% and 14% respectively), where inconsistent policies, fragmented governance, and disconnected systems remain common barriers.

However, fully-centralized structures are rare. Policy and business functions often remain regional, while data engineering is usually coordinated centrally. Modeling teams may also need local flexibility to reflect jurisdiction-specific risks. This mix reflects the institutional complexity of large banks.

The key to effective integration lies in architectural design: Banks need shared data layers, consistent detection logic, and interoperable case management systems to support coordinated risk management across functions and regions, even within distributed organizational structures.

“How well-architected are your organization’s fraud and AML systems and teams in terms of sharing data and maintaining a unified view of customer risk across products and channels? (Select one)”

Highly integrated FRAML systems and teams



Note: Showing responses of respondents from varied FRAML organizational models who reported that they operate in highly integrated FRAML teams.
Base: 222 business and IT decision-makers with responsibility over their organization’s implementation of FRAML solutions
Source: Forrester’s Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

A Disjointed Data Layer Undermines FRAML Transformation

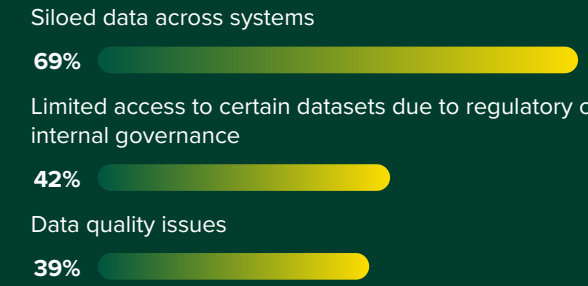
Sixty-nine percent of respondents cited siloed data as the top barrier to FRAML detection at their organization, with a further 42% stating that critical FRAML data is still delivered in batches.

These issues persist even after core modernisation: 53% cited limits to how core systems exchange data with detection platforms for real-time scoring.

Addressing this requires re-architecting the data layer to make risk data accessible in real-time, interoperable, and consistently tied to customer identities to meet the needs of modern FRAML platforms and reduce latency between transaction and detection.

Firstly, data products and curated, reusable datasets with built-in definitions, controls, and identity matching can deliver consistent, ready-to-use risk data. Secondly, bridging strategies that decouple detection platforms from core system constraints can enable faster event flows and adaptive risk operations without reworking the core.

Top Three Challenges When Integrating Different Types Of Data Sources To Support FRAML Detection



Typical Delivery Method For Critical FRAML Detection Data

Base: 67 IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

Top Three Barriers To Consistently Scale Real-Time FRAML Detection Across Customer Channels

53%

Limitations with real-time capabilities of core banking or transaction systems in supporting real-time scoring

> Of these, 50% reported that critical FRAML data was delivered via batch processing, compared to the survey average of 42%.

48%

Lack of unified cross-channel risk view to correlate activity or build a shared risk profile across multiple channels in real time

43%

Channel-specific infrastructure that makes it hard to deploy shared detection logic

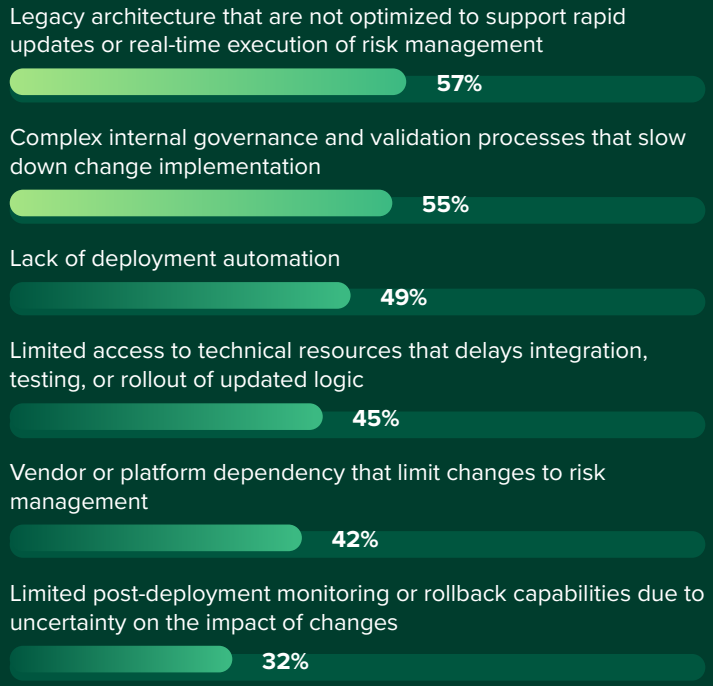
Base: 222 business and IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

Architectural Limitations Delay FRAML Detection Logic Updates

Over half of respondents indicated that legacy architecture (57%) and complex governance processes (55%) slow their organization's ability to update detection logic in response to emerging threats. These constraints create structural delays, especially when updates require manual rule changes, extended testing, or vendor intervention. Governance processes add further lag with multilayered reviews that were originally designed for slower-moving risk environments.

To respond more effectively to evolving fraud and money laundering typologies, banks need architectural foundations that support rapid iteration and modular updates to scoring logic. These foundations should enable auditable change processes within sandboxed testing environments and support continuous integration without compromising control. Re-architecting for flexibility — not just to upgrade platforms — is key to enabling faster, more adaptive risk detection.

Factors That Impede The Effective Management Of Emerging FRAML Risks



Base: 222 business and IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

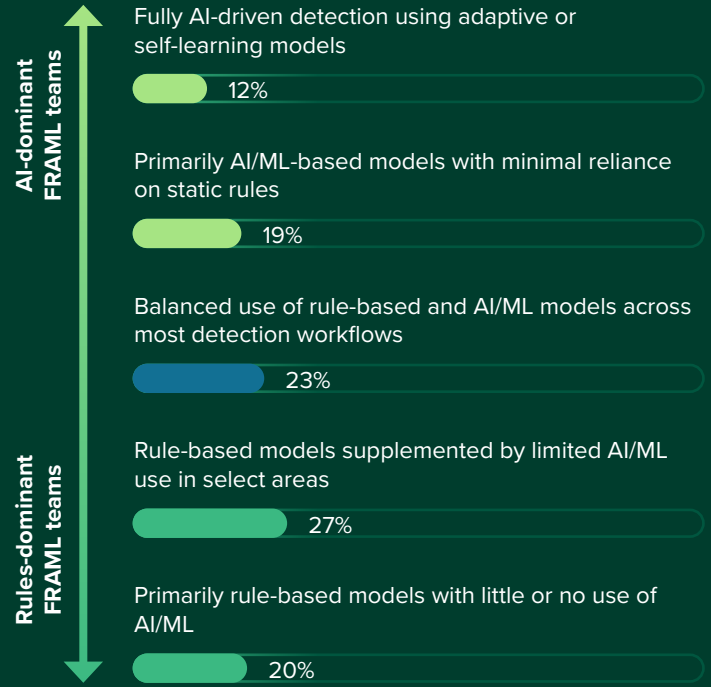
AI Is No Panacea: Adaptive FRAML Rests On Broader Architectural Foundations

AI models are essential for improving detection as threats grow more dynamic and data volumes rise — yet adoption remains uneven. Sixty-nine percent of respondents said their organization still relies on rule-based approaches or applies AI narrowly within workflows. Furthermore, a third require legal or compliance review before deploying AI, and 16% noted their organization has delayed or scaled back due to compliance risks.

Even among AI adopters, legacy architecture is a major constraint: 68% cited it as a barrier to updating detection models versus 53% of rules-dominant peers. Without timely and compliant access to the right data and flexibility to iterate quickly, AI models are harder to test, deploy, and refine within regulatory boundaries.

Realizing AI's potential in FRAML requires real-time data pipelines, privacy-aware data exchange, modular integration, and flexible deployments that support continuous adaptation in compliance-heavy settings.

"Which of the following best describes your organization's current approach to fraud and AML risk scoring? (Select one)"



Base: 222 business and IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

"How have data privacy, residency, or regulatory constraints impacted your organization's ability to adopt AI/ML in FRAML operations? (Select one)"

We require legal or compliance review before deploying AI/ML models.
34%

We adopted privacy-preserving techniques (e.g., synthetic data, federated learning).
18%

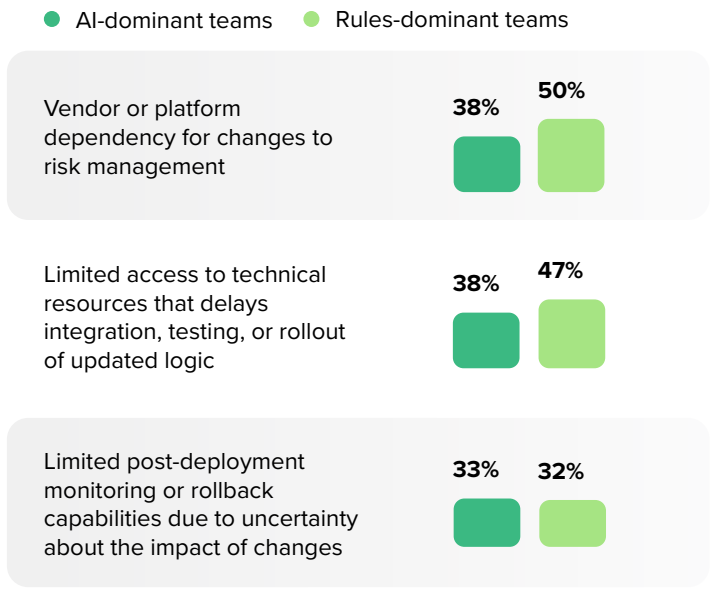
We have delayed or scaled back planned AI/ML initiatives due to compliance risks.
16%

We anonymize or tokenize data before using it for model development.
15%

We have implemented additional access controls or data segregation for model training.
13%

We have restricted the use of AI/ML to on-premises environments only.
3%

Base: 67 IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]



Base: 222 business and IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

Factors That Impede The Effective Management Of Emerging FRAML Risks Across AI Orientation

Transforming FRAML Requires Balancing Innovation With Control

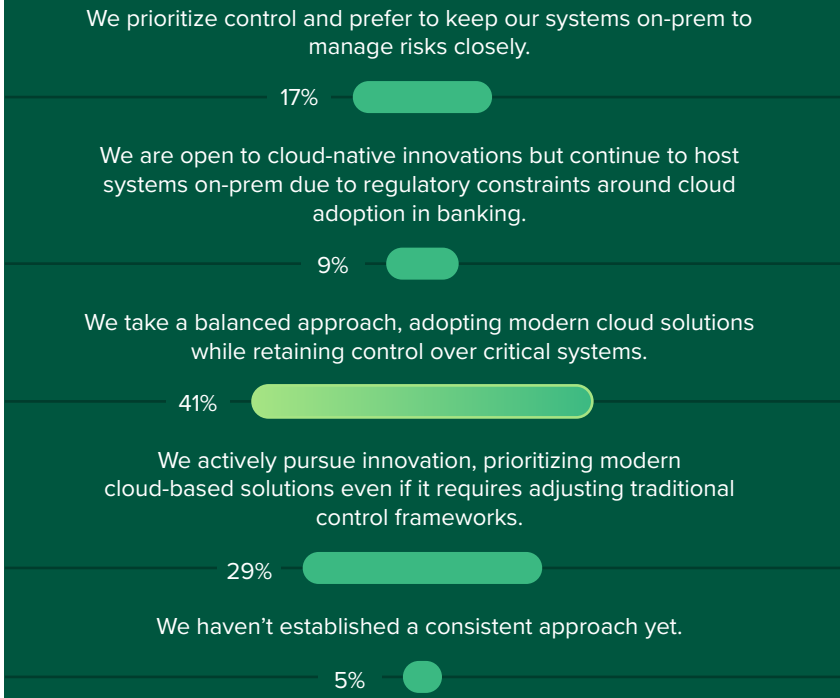
The challenges faced by banks highlight a fundamental trade-off: Upgrading FRAML capabilities while preserving control and compliance.

This trade-off is reflected in how most banking leaders (41%) are approaching modernization by adopting cloud-based solutions while retaining control over critical systems. Only some lean heavily toward either innovation or strict control.

Rather than treating innovation and control as opposing ends of a spectrum, banks should design FRAML architectures that enable both. The future is not about choosing between transformation and risk avoidance — it's about delivering smarter, faster, and more adaptive detection while meeting regulatory expectations.

Modular, interoperable, and secure architectures are key to achieving this balance.

"Which of the following best describes your organization's approach to balancing innovation and control in FRAML systems? (Select one)"



Base: 155 business decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

Hybrid Cloud Is Emerging As A Key Enabler Of FRAML Modernization

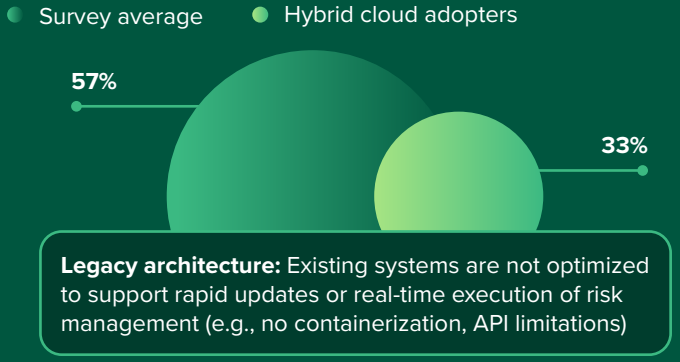
Nearly half of leaders (49%) use a hybrid cloud approach for FRAML systems at their organizations, selectively deploying workloads to cloud or on-prem environments based on data sensitivity and compliance requirements.

Banks that embrace hybrid cloud reported fewer architecture-related challenges. The share of hybrid cloud adopters who cited legacy architecture as a barrier to effective FRAML risk management is lower than the survey average (33% vs. 57%), suggesting that the flexibility and modularity of hybrid cloud help banks overcome many of the aforementioned architectural barriers.

What makes hybrid cloud effective is its flexibility in deployment. Banks can process sensitive data on-prem while using cloud for scalable analytics or agile development. This allows banks to modernize incrementally without exposing critical systems or requiring full-scale replacement, thus offering a balanced path to accelerating change.

"Which of the following best describes your organization's approach to cloud adoption for FRAML systems? (Select one)"

Legacy Architecture As A Factor That Delays The Tuning Of FRAML Risk Management With The Emergence Of New Fraud And Money Laundering Typologies



Base: 67 IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

Cloud-Native On-Prem Extends Hybrid Cloud Benefits To Regulated Environments

Hybrid cloud offers deployment flexibility but does not eliminate the need for on-prem systems. Even in cloud-mature banks, certain workloads must remain on premises due to regulatory, operational, or security constraints. For these workloads, banks need a complementary path to modernization that brings cloud-like agility to regulated, on-prem environments.

Inflexible on-prem systems limit the value of cloud innovation in the stack. These bottlenecks slow down detection logic updates, hinder integration with AI models, and reduce the overall responsiveness of FRAML systems.

Cloud-native on-prem architecture bridges this gap by applying cloud design principles such as containerization, microservices, automated deployment, and scalable analytics within controlled on-prem environments. It lets banks modernize on-prem systems without needing to migrate sensitive workloads that cannot be moved to the cloud due to data residency, or regulatory and operational constraints.

Together, a hybrid and cloud-native on-prem approach delivers agility across cloud and on-prem environments.

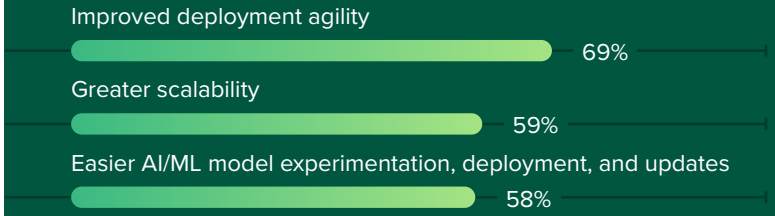
Cloud-Native On-Prem Reconciles Agility With Regulatory And Operational Constraints

Leaders who are at least considering implementing cloud-native architecture cited improved deployment agility (69%), greater scalability (59%), and easier AI/ML experimentation (58%) as top motivations to re-architect their organization's on-prem environment. This underscores the role of cloud-native architecture in enabling faster tuning, adaptive responses, and more intelligent risk management.

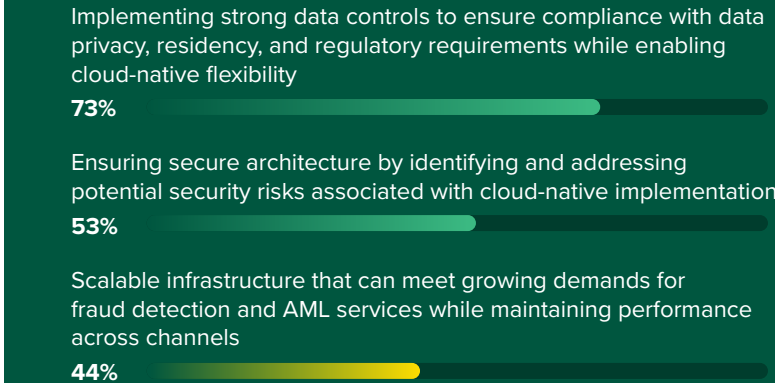
While these motivations center on agility and speed, their implementation priorities reveal a strong focus on assurance. Seventy-three of these respondents identified strong data controls and compliance as a top priority, followed by secure architectural design (53%), and scalable infrastructure (44%).

The combined emphasis on agility and control reinforces cloud-native on-prem as a key enabler of FRAML modernization.

Main Benefits Organizations Expect From Adopting A Cloud-Native Architecture For On-Prem FRAML Detection



Key Priorities When Implementing An On-Prem Cloud-Native Architecture For FRAML Systems



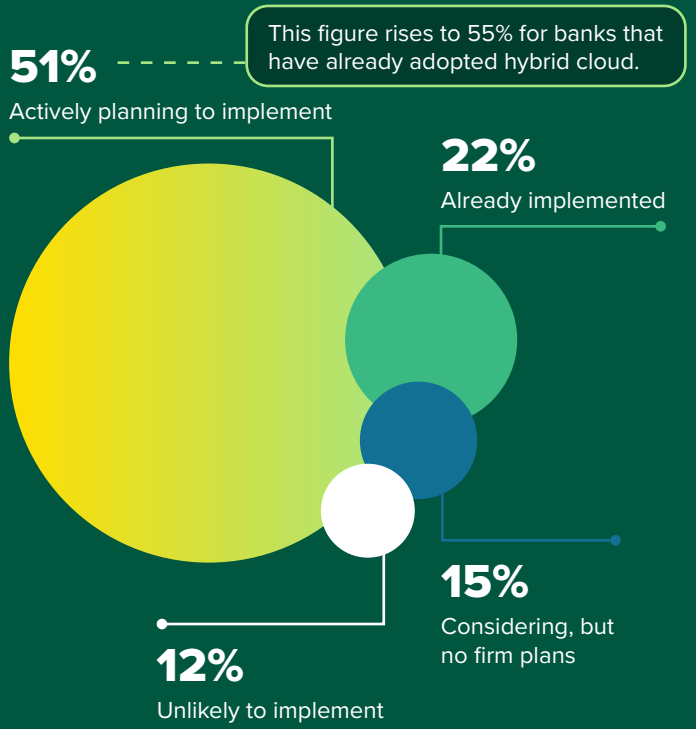
Base: 67 IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

Adoption of Cloud-Native On-Prem Is Accelerating, Led By Hybrid Cloud Adopters

The cloud-native on-prem approach is gaining traction among banks: 51% of banking tech stakeholders shared that their institution is actively planning to implement cloud-native architecture on-prem, 22% have already done so, and another 15% are considering it. Uptake is also stronger among banks that have already adopted hybrid cloud, reinforcing how these two approaches work together to support modernization.

Rather than treat on-prem systems as fixed, leading banks are re-architecting them to operate with the same agility and adaptability as their cloud-based components. In this way, cloud-native on-prem design is fast becoming a natural extension of hybrid cloud approaches.

"How likely is your organization to implement, or has it already implemented, cloud-native architecture on-prem for FRAML systems?"



Base: 67 IT decision-makers with responsibility over their organization's implementation of FRAML solutions
Source: Forrester's Q2 2025 Fraud & AML in APAC Banks Survey [E-63585]

Conclusion

As threats evolve and oversight tightens, banks must modernize FRAML operations without sacrificing control. This research underscores three imperatives:

- **Align architecture and data.** Real-time detection and advanced models require eliminating blind spots from silos, batch pipelines, and inconsistent access through unified, interoperable data layers.
- **Build AI on strong architectural foundations.** AI's impact depends on timely, compliant data access and flexibility to iterate. Legacy systems, fragmented workflows, and governance bottlenecks slow testing, deployment, and refinement.
- **Leverage hybrid cloud with cloud-native on-prem.** Hybrid cloud enables phased change, while cloud-native on-prem brings agility to regulated workloads. Together, they form a secure, flexible platform for adaptive risk management.

Endnotes

[1] Source: Top Trends Shaping Fraud Management In Asia Pacific, 2024, Forrester Research, Inc., August 28, 2024.

[2] Source: The Top Trends In Enterprise Fraud Management In 2024, Forrester Research, Inc., July 15, 2024.

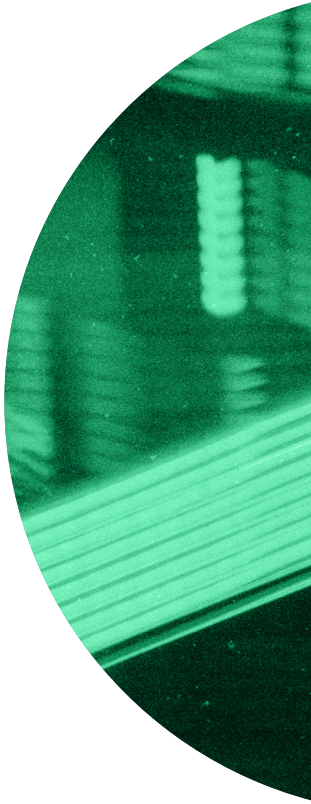
[3] Source: Tang See Kit, Banks, telcos and scam victims to share liability for losses under new framework to kick in on Dec 16, Channel News Asia, October 24, 2024.

Project Team:

Amelia Lau,
Market Impact Consultant

Contributing Research:

Forrester's Technology Architecture & Delivery research group



Methodology

This Opportunity Snapshot was commissioned by Red Hat. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 222 business and IT decision-makers from banks in APAC with influence over their organization's implementation of FRAML solutions. The custom survey began and was completed in May 2025.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Demographics

REGION	
East Asia	40%
Southeast Asia	32%
India	14%
Australia	14%

BANKING SEGMENT	
Retail banking	34%
Corporate banking	25%
Investment banking	24%
Wealth management	17%

ANNUAL REVENUE OF APAC OPERATIONS	
$500M to $999M	19%
$1B to $5B	48%
More than $5B	33%

LEVEL OF RESPONSIBILITY OVER IMPLEMENTING FRAML SOLUTIONS	
Final decision-maker	17%
Part of a team making decisions	41%
Influence decisions	46%

Note: Percentages may not total 100% due to rounding.


FORRESTER®