CORE SYSTEM PARTNERS

RISK AND COMPLIANCE MARKET INTELLIGENCE REPORT

PREPARED BY CORE SYSTEM PARTNERS

Principal Author: Rick Mavrovich

CEO & Managing Director, Core System Partners

May 2025

212-202-0078 | info@coresystempartners.com | coresystempartners.com

Author's Note

This report was developed by Core System Partners and led by Rick Mavrovich, CEO & Managing Director, in collaboration with the firm's senior research team. The findings are based on interviews with senior leaders at **15 banks across the U.S., Europe, and the MENA region.**

The insights reflect not just data, but lived experience—captured through real-world transformation efforts, regulatory engagements, and modernization initiatives. This report is designed to help bank leaders navigate the shifting intersection of compliance, technology, and operational execution.

Executive Summary

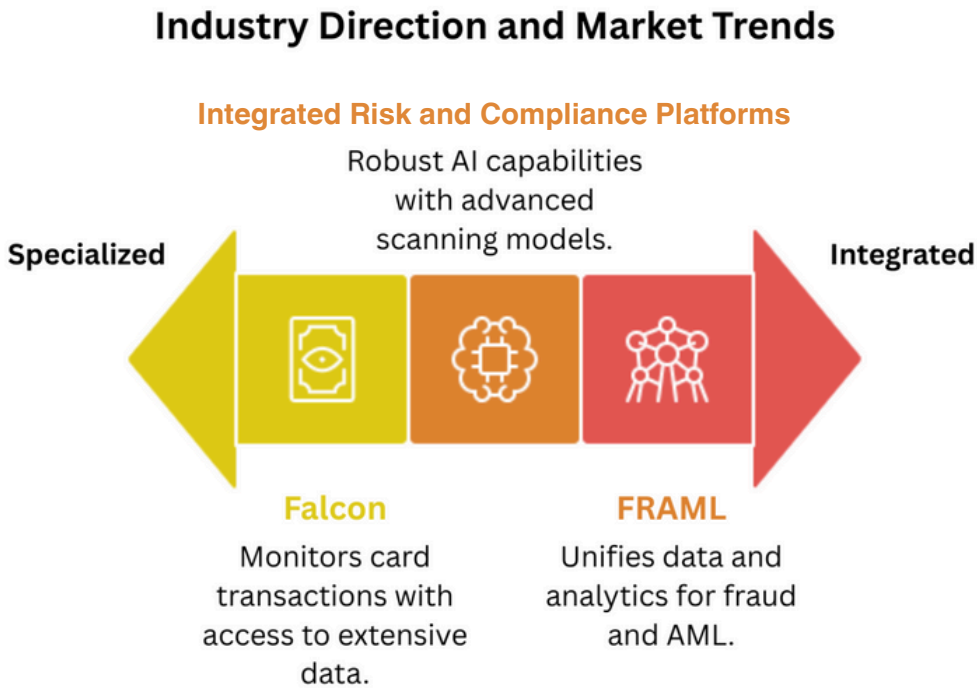
This report provides a market scan of risk and compliance systems for commercial banks, highlighting where the market is headed, who's doing what, and what matters most. The research draws from interviews with eleven senior risk and compliance leaders—spanning 15 global and regional banks, and fintechs—and analysis from industry analysts like Gartner, McKinsey, Aite-Novarica, and others.

Here's the big picture: banks are stuck between specialized tools that do one thing well and broader platforms that promise integration. Meanwhile, the pressure to modernize keeps climbing. Regulators are expecting more. Fraud is evolving. And tech teams are juggling legacy platforms that weren't built for today's pace.

Gartner sums it up well: "By 2025, 50% of global banks will use AI/ML systems for AML monitoring, up from less than 10% today, reducing false positives by more than 35% while improving detection rates."

This report gives banks and decision-makers the market context they need to make informed calls about where to go next.

PART I: INDUSTRY DIRECTION AND MARKET TRENDS



1. Evolution of Risk and Compliance Technology

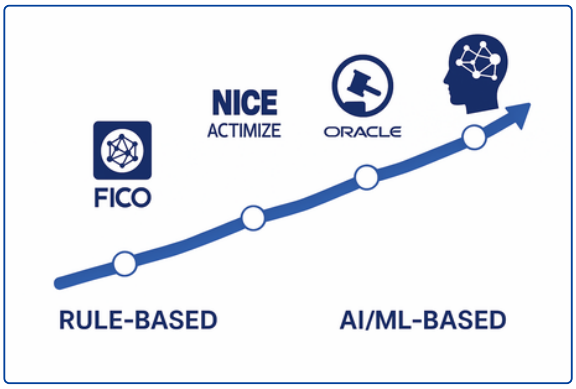
1.1 Risk Management Technology Trends

Risk management systems continue to evolve toward greater automation, analytics capabilities, and integration. Specialized solutions for distinct risk domains remain prevalent, but consolidation is increasingly evident.

"*In the fraud space, Falcon is hands down the best tool in the industry for monitoring card-based transactions. The reason why is about 96% of all debit card and credit card and ATM transactions flow through FICO. So they have access to data that allows them to identify fraud runs and anomalies across the U.S.*" — Head of Operations, Regional Bank

This sentiment is echoed by other experts who affirm that specialized systems continue to dominate in high-volume transaction monitoring domains. However, larger institutions are increasingly exploring enterprise solutions.

"According to McKinsey's Global Banking Annual Review, "Banks spend 5-10% of their operating costs on compliance, with technology representing approximately 20% of compliance spending. Yet only 24% report being satisfied with the effectiveness of their compliance technology infrastructure."



Alongside consolidation, several noteworthy developments are reshaping the risk technology landscape:

- **Advanced Analytics:** Machine learning models demonstrating 25–40% reductions in false positives while maintaining detection rates
- **Behavioral Analytics:** Shift from rules-based detection to behavior-based anomaly detection
- **Network Analysis:** Enhanced capabilities to identify hidden relationships in complex financial crime patterns

The Office of the Comptroller of the Currency (OCC) notes in its Semiannual Risk Perspective that "Banks must understand their compliance technology's detection capabilities, limitations, and ensure appropriate human oversight of automated processes, particularly as AI and machine learning become more prevalent in compliance functions."

1.2 Compliance Technology Trends

The compliance technology market is experiencing significant change, with legacy rule-based systems gradually giving way to more sophisticated approaches:

We're moving everything except for Falcon right now over to the Oracle FCCM suite. Oracle's got a lot more robust capabilities around AI... they're kind of a leader in that space with different scanning models and patterns." — Senior Technology Executive, Global Bank

According to Aite-Novarica Group's "AML Technology Benchmark Study 2023," "The alert-to-SAR ratio remains stubbornly high at many institutions, with the industry average showing approximately 95% of alerts classified as false positives after investigation." This inefficiency is driving institutions toward more advanced solutions.

"*The more state-of-the-art platforms bring in a combination of various methods, including continuous learning. In traditional rule-based systems, if I'm exporting books to Nigeria as my business, every one of my transactions will be triggered, with no way to recognize this is normal activity for me. Newer systems with machine learning can adapt to individual behavior."* — Head of Technology, Global Bank

Key trends in compliance technology include:

- **AML and KYC Platform Modernization:** Solutions expanding beyond rule-based monitoring to include AI and network analysis
- **Regulatory Reporting Automation:** Enhanced capabilities for regulatory filing generation and submission
- Sanctions and Watchlist Screening Innovations: More sophisticated matching algorithms with reduced false positives

FinCEN Director Andrea Gacki noted at the 2023 ACAMS AML Conference that "The use of innovative approaches and technologies in AML compliance is encouraged, provided institutions maintain appropriate governance, oversight, and documentation to demonstrate system effectiveness."

1.3 Convergence and Integration

While specialized solutions remain prevalent, the market is moving toward greater integration across risk and compliance domains:

"The industry is definitely going toward integrating payment solutions with risk and compliance functions. It makes it easier to have the same people handle multiple functions while streamlining the technology stack." — Payment Operations Executive, Regional Bank

Deloitte's Financial Services Risk & Compliance Survey observes that "The convergence of fraud and financial crimes compliance functions (FRAML) represents a significant opportunity for institutions to reduce costs by 15–20% while improving risk management effectiveness through unified data, analytics and investigation processes."

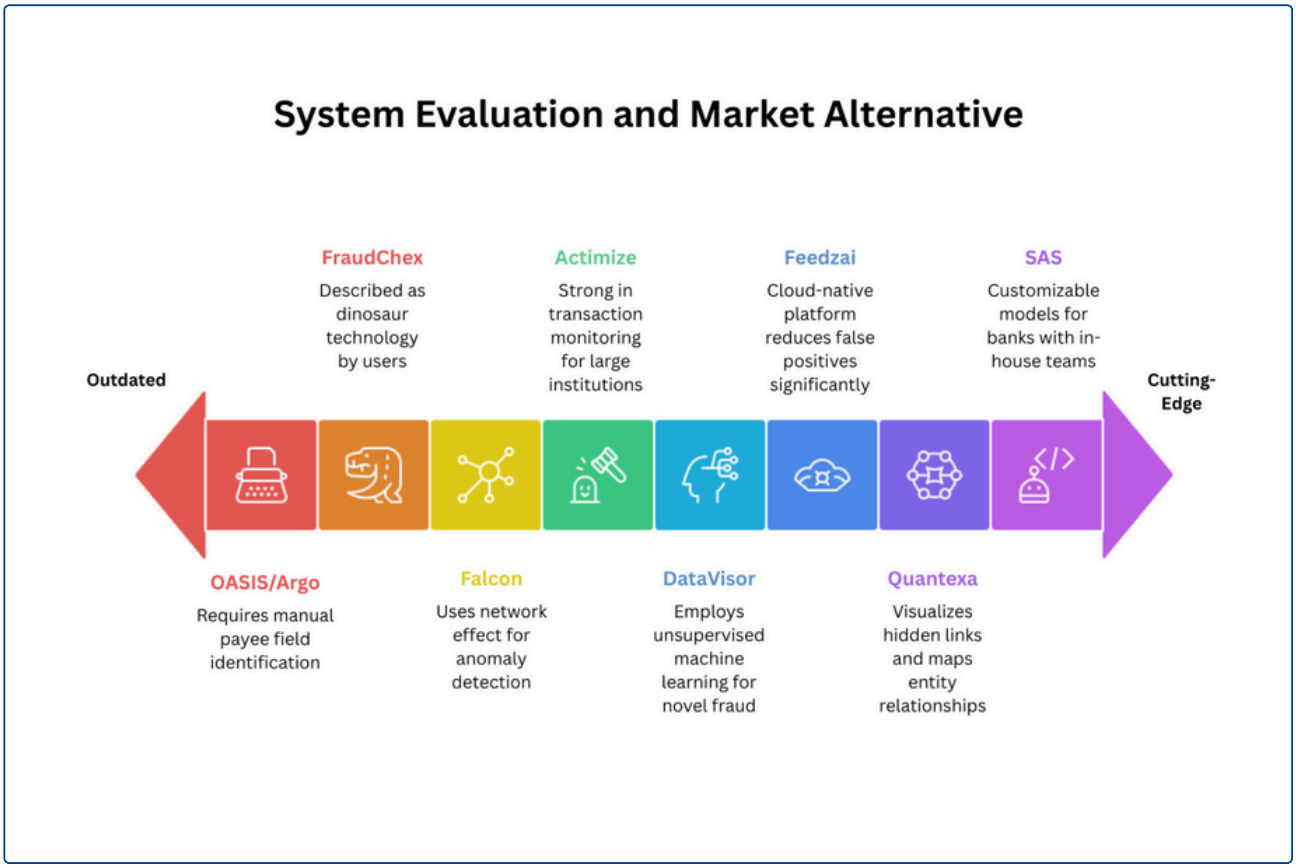
This integration appears mostly in:

- ***FRAML Convergence:*** *The merging of fraud and anti-money laundering functions*
- ***Common Data Architecture:*** *Unified data models supporting multiple risk and compliance domains*
- ***Enterprise Risk Platforms:*** *Solutions encompassing multiple risk types within a consistent framework*

"From an organizational perspective, fraud was always handled by operations because it's front line. AML is handled by compliance. The trend now is to keep those level one reviews separate, but combine the investigation teams at level two, using the same tools and standards, because the outcomes for both are CTRs or SARs." — Compliance Technology Advisor, Financial Services

Forrester Research reports that "Financial institutions that implement integrated risk and compliance platforms report a 25–40% reduction in total cost of compliance compared to those maintaining siloed solutions."

PART II: SYSTEM EVALUATION AND MARKET ALTERNATIVES



1. Current Risk Systems Assessment

1.1. Fraud Risk Management

One of the most entrenched categories in the risk technology landscape is card fraud detection, where the consensus market leader remains Falcon by FICO.

Leveraging data from 96% of card transactions in the U.S., Falcon uses a network-effect model to detect anomalies and predict fraudulent patterns across the ecosystem.

"FICO for me is the Cadillac in the industry... We reduced our losses by about 35% in ATM transactions just by getting onto the current version." - Head of Operations, Regional Bank

That versioning detail is important: while Falcon is powerful, its performance depends heavily on running the most up-to-date release. Institutions using Falcon via a service bureau model, like those managed by FIS,are often a few versions behind, which significantly reduces detection accuracy.

Gartner supports this dominance: "Card fraud detection remains a specialized domain where network effect and consortium data provide significant advantages to established solutions."

Market Alternatives:

- **SAS Fraud Management:** Best for banks with in-house technical teams that can customize models
- **Feedzai:** A cloud-native platform boasting a 50% false positive reduction
- **DataVisor:** Focuses on unsupervised machine learning to catch novel fraud types
- **ACI Proactive Risk Manager:** Offers cross-channel fraud coverage at an enterprise level

Key Attributes of Falcon (FICO):

- Real-time card fraud detection with cross-bank network intelligence
- Dominant position in the U.S. market
- Performance degradation if not kept current or run in tightly controlled vendor environments

1.2. AML and Financial Crime Compliance

AML compliance platforms are becoming more diverse, but the field is still dominated by a handful of major players. Among them, Actimize by NICE is widely adopted by large and mid-sized institutions for its strength in transaction monitoring and wire/ACH use cases.

"*Actimize is really good for ACH and wire monitoring... One bank was mandated by regulators to move to it because it's just stronger for AML/BSA transaction monitoring."* — Head of Operations, Regional Bank

Actimize is feature-rich but complex. Implementation timelines often exceed 12–18 months, especially in environments requiring deep customization. Its rule-based system design also poses challenges in tuning false positives without significant effort.

Prime Compliance Suite (PCS) by FIS is another prominent platform, particularly among institutions already committed to the FIS core. While it offers basic AML, KYC, and regulatory filing tools, its capabilities are narrower compared to Actimize or newer AI-based options.

Key Observations:

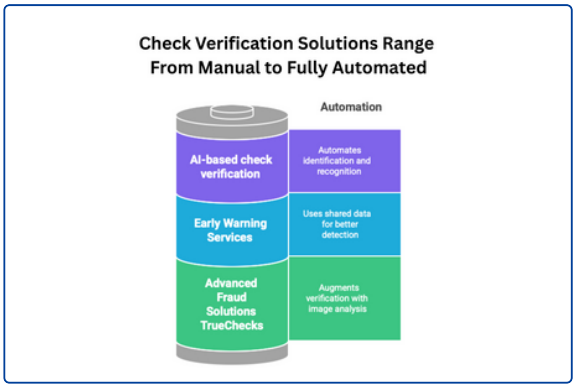
- Actimize leads in ACH/wire AML monitoring but requires lengthy and expensive deployment
- PCS fits more neatly into existing FIS ecosystems but lacks advanced analytics

Market Alternatives:

- **Oracle FCCM:** Strong enterprise platform with embedded AI and case management
- **Verifin:** A cloud-native platform gaining converts from institutions looking to move off Actimize
- **BAE NetReveal:** Entity-based detection and analytics across customer networks
- **Quantexa:** Specializes in relationship mapping and visual network analysis, often layered on top of other platforms

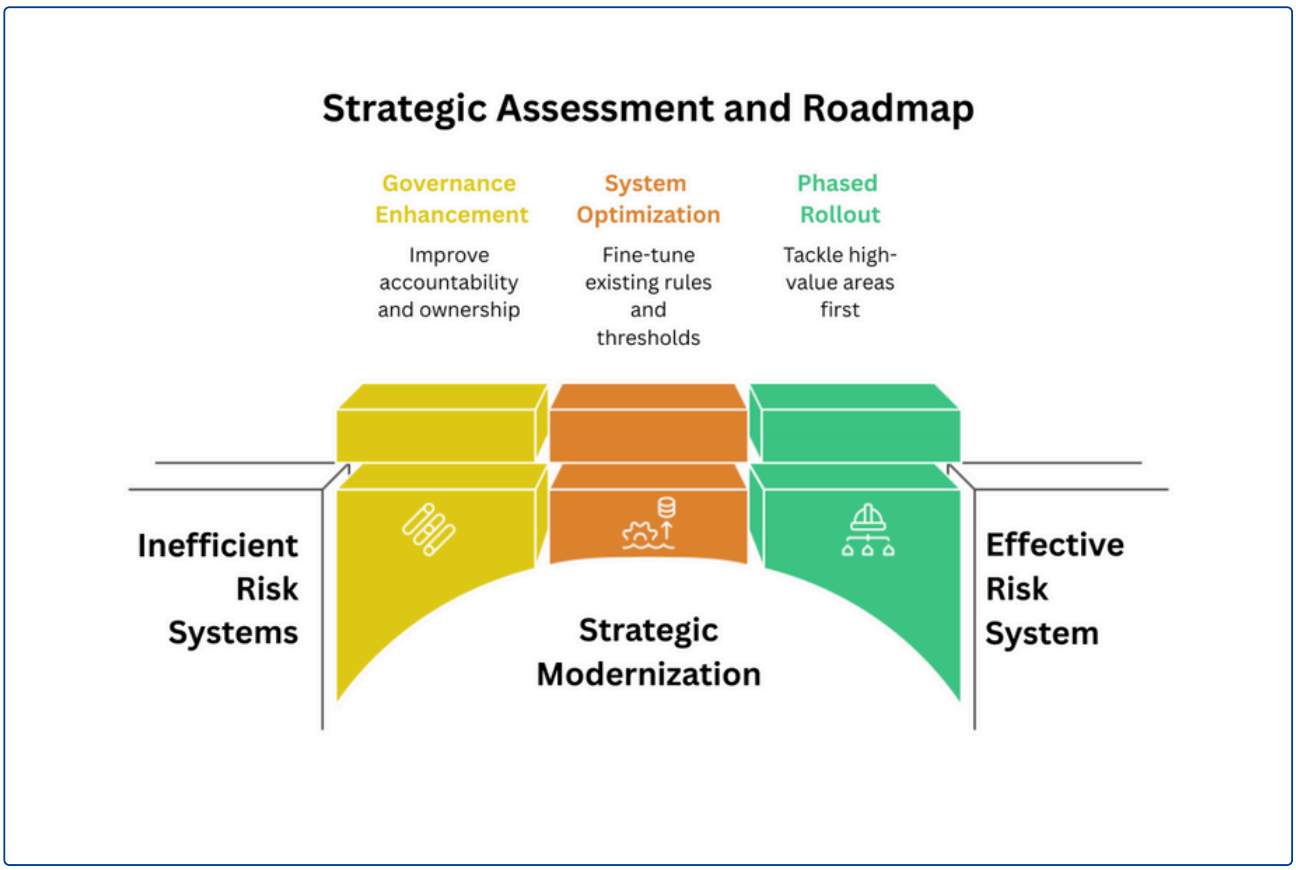
Emerging Alternatives:

- **Advanced Fraud Solutions TrueChecks:** Adds image analytics to check verification workflows
- **Early Warning Services:** Leverages a consortium model similar to FICO's for cards
- **AI-based check verification:** Still nascent but evolving to automate check stock identification and pattern recognition



The check space is unlikely to see a flood of innovation, but incremental improvements, particularly around automation, are helping reduce labor requirements and improve fraud detection.

PART III: STRATEGIC ASSESSMENT AND ROADMAP



1. Evaluation Framework

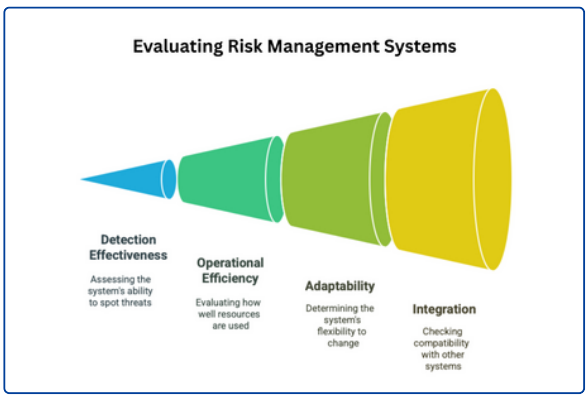
1.1 Risk Management Effectiveness

Risk systems should do more than just catch bad behavior—they need to catch the right things, do it fast, and avoid wasting resources. Here's how to size them up:

- **Detection effectiveness:** Can it actually spot the threats you're worried about?
- **Operational efficiency:** Are analysts buried in junk alerts or focused on real risk?
- **Adaptability:** How quickly can the system pivot when fraud patterns shift?
- **Integration:** Does it play play well with upstream/downstream systems?

"*The question you want to ask is: are they still stuck with traditional methods, or are they leaning into newer approaches?*" — Compliance Tech Advisor

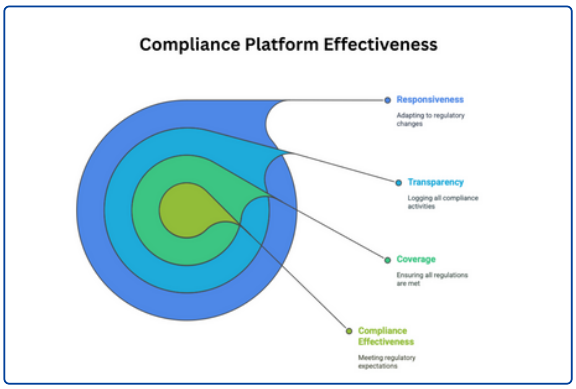
McKinsey puts it bluntly: the best banks are moving from check-the-box compliance to risk tools that improve customer experience and decision-making.



1.2 Compliance Effectiveness

Regulators expect coverage, transparency, and responsiveness. A solid compliance platform should:

- Cover all required regs without gaps
- Log everything—alerts, actions, investigations
- Generate audit-ready reports with minimal human lift
- Adapt fast when regulations change



"AML is in the spotlight. TD got hit hard, and more banks are likely next." — CTO, Regional Bank

Documentation and adaptability aren't just nice-to-haves. They're table stakes if you want to avoid fines and scrutiny.

- **1.3 Integration with Business Strategy**

Risk and compliance shouldn't sit in a corner. They need to be wired into how the business runs:

- **Customer Experience:** Don't let security kill the user journey
- **Operational Synergies:** Shared data, shared processes = less rework
- **Scalability:** Can it grow with your business?
- **Cost Efficiency:** Are you spending smart—not just spending more?

FRAML: When It Does—and Doesn't—Make Sense

While many institutions are exploring or adopting FRAML (Fraud + AML convergence) models, it is not a one-size-fits-all solution. A unified fraud and AML operation can drive efficiency and insight under the right conditions, but it also introduces complexity and requires alignment.

Figure: When FRAML Makes Strategic Sense

FRAML Makes Sense When…	FRAML May Not Be Justified When…
Transaction and alert volumes are high, creating investigative overlap	Referral volume between fraud and AML is low (e.g., <100/month)
Data is already centralized or integrated across fraud and AML systems	Data remains siloed and integration would require major lift
Platform modernization is underway, allowing alignment of workflows	Teams are using legacy tools with no immediate replacement path
Cross-domain patterns (e.g., mules, layering) require shared detection	Fraud and AML case types are highly distinct with little overlap
Governance supports unified oversight across risk domains	Compliance constraints (e.g., SAR access rules) require separation
Institution is prioritizing centralized operational risk management	Current operating model is stable and resource bandwidth is limited

EY puts it this way: more banks are treating risk/compliance tech as a strategic asset, not just a cost of doing business.

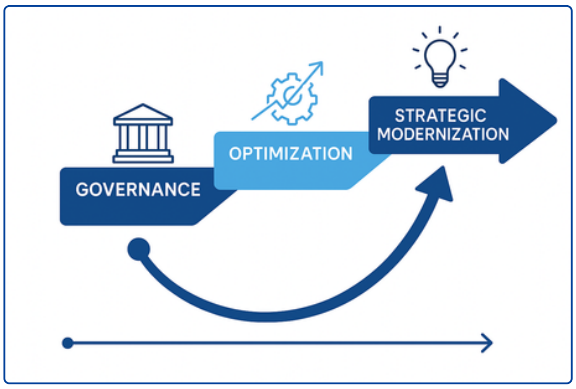
- **1.3 Integration with Business Strategy**

Risk and compliance shouldn't sit in a corner. They need to be wired into how the business runs:

- **Customer Experience:** Don't let security kill the user journey
- **Operational Synergies:** Shared data, shared processes = less rework
- **Scalability:** Can it grow with your business?
- **Cost Efficiency:** Are you spending smart—not just spending more?

2. Implementation Approaches

2.1 Governance Enhancement



Before upgrading anything, tighten up governance. You'd be surprised how much lift you can get from better accountability.

Before upgrading anything, tighten up governance. You'd be surprised how much lift you can get from better accountability.

- **Ownership:** Know who owns what—tech, tuning, performance
- **Performance tracking:** Regular reviews of false positives and catch rates
- **Vendor accountability:** Strong SLAs and real escalation paths
- **Change control:** Clear process for tuning or swapping rules/models

"*At the very least, look at the trend lines: is it getting better or worse month over month?*" — Payments Exec

Deloitte says banks with strong governance report 30% higher satisfaction and 25% lower maintenance costs. That's real.

- **Fine-tune the rules:** Start with what's generating the most noise
- **Revisit thresholds:** Adjust to actual risk appetite
- **Tighten integrations:** Better data flow = better alerts
- **Train your people:** Make sure they actually know how to use the tools

If you're waiting on a vendor for every tuning change, you're going to fall behind." — Payments Exec

Gartner backs this up: systematic tuning can cut false positives 20–30% in a year.

2.3 Strategic Modernization

When you're ready to think long-term, take a phased approach. Build momentum, don't bite off everything at once:

- **Phase your rollout:** Tackle highest-value areas first
- **Build internal talent:** Don't outsource critical thinking
- **Get the data right:** Consolidated, clean, and queryable
- **Leverage cloud smartly:** Flexibility + scale = long-term wins

McKinsey's research shows the banks that win at modernization are the ones that start small and scale smart.

3. Recommendations and Future Outlook

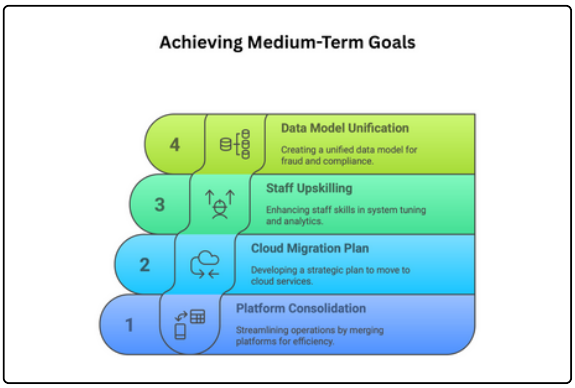
3.1 Short-Term Actions

- Start measuring vendor and internal team performance—quantify it
- Take back some control of system configs
- Begin monthly reviews of alert trends and detection effectiveness
- Reevaluate alert thresholds based on actual business impact

KPMG notes these actions alone can improve efficiency 15–25% within a year.

3.2 Medium-Term Initiatives

- Explore platform consolidation where it adds efficiency
- Develop a phased cloud migration plan
- Upskill staff on system tuning, analytics, and case workflows
- Unify your data model across fraud and compliance

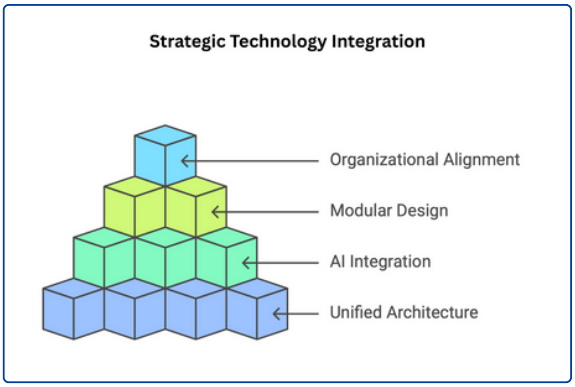


"The real unlock is when AML and fraud teams stop duplicating effort." — COO, Commercial Bank

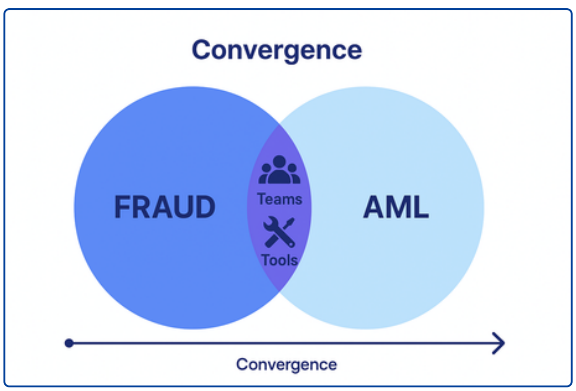
Deloitte estimates convergence savings between 15–20% with a side benefit of better investigative outcomes.

3.3 Long-Term Vision

- Build toward a unified risk/compliance architecture
- Bake AI into your detection strategy
- Go modular with API-first architecture
- Align how the org operates with how the tech is structured



Gartner again: "By 2025, 50% of banks will use AI/ML in AML, reducing false positives by 35%+."



Key Takeaways

Technology Landscape

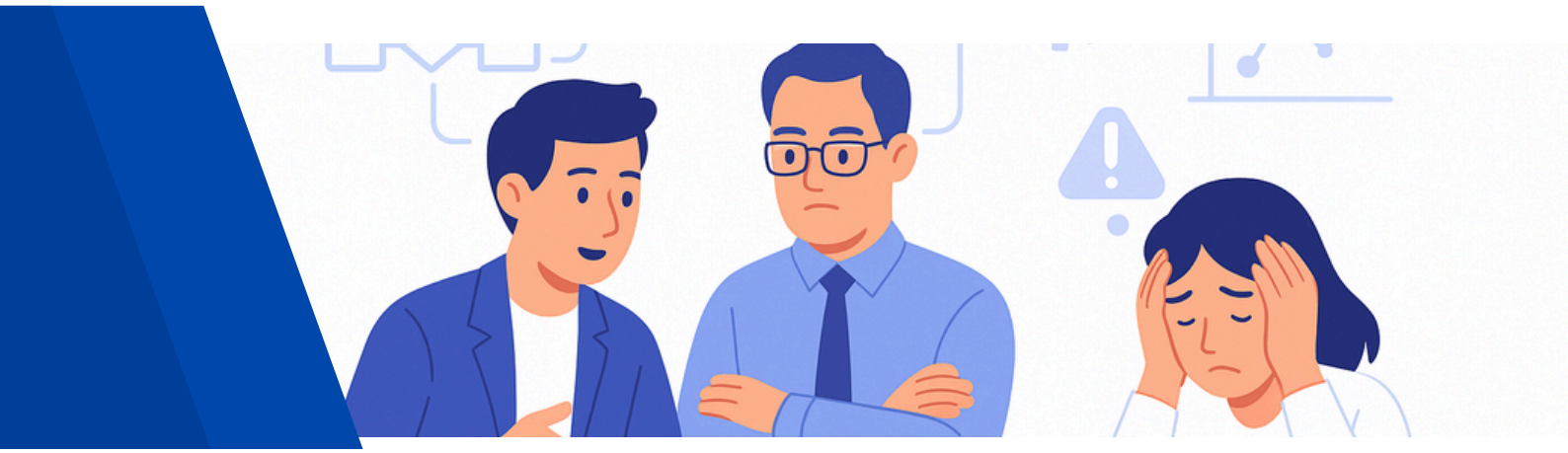
- Specialized tools (e.g., Falcon for card fraud, Actimize for AML) still dominate specific domains, particularly where volume and performance require deep focus.
- Larger institutions are leaning toward enterprise platforms for unified governance and AI integration, particularly Oracle FCCM.
- AI/ML models are proving effective: reducing false positives by up to 40% while improving detection, though governance and explainability are still critical hurdles.
- Behavioral analytics and network-based models are slowly replacing static, rules-based systems—especially in AML and fraud fusion areas.

Operational Models

- Most banks retain Centers of Excellence for compliance tech due to the specialized knowledge required and sensitivity of tuning risk parameters.
- Hybrid governance is now common: architectural oversight in IT, but operational control remains firmly within the business.
- False positives are not just inefficient—they represent a blind spot in risk mitigation when analysts are overwhelmed and high-risk signals are missed.

Vendor Strategy

- Managed services can constrain control, delay tuning, and restrict versioning—impacting effectiveness unless banks develop internal config expertise.
- Few institutions are comfortable with fully outsourcing fraud/AML tuning; control and transparency are seen as essential for responsiveness and regulatory compliance.



Key Takeaways - Continued

Convergence & Integration

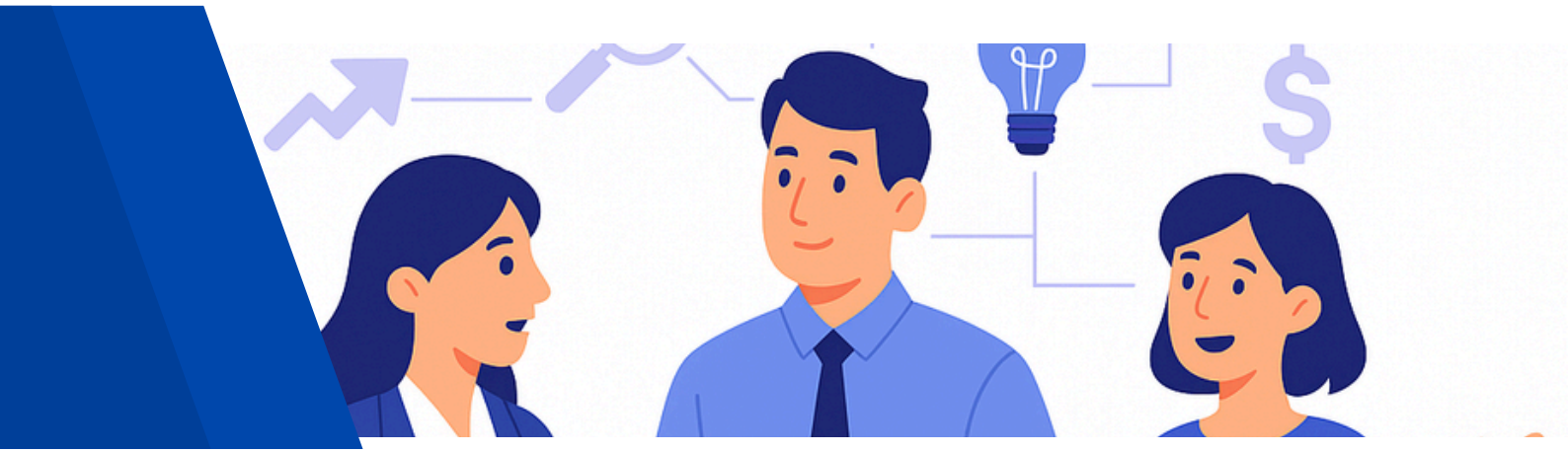
- The shift toward FRAML (fraud + AML) is real and growing. Investigation teams are merging, tools are consolidating, and case management is being standardized.
- Shared data architectures and integrated workflows create cost efficiencies (15–20% reductions reported) and improve investigator effectiveness.

Strategic Decision Drivers

- Total Cost of Ownership is shaped more by operations than by licensing—analyst headcount, alert volumes, and tuning cycles drive the real costs.
- ·Build vs. Buy isn't binary: most institutions buy core detection engines but invest heavily in configuration, investigation workflows, and integrations.
- System effectiveness depends more on implementation and governance than on the vendor selected.

Maturity Pathways

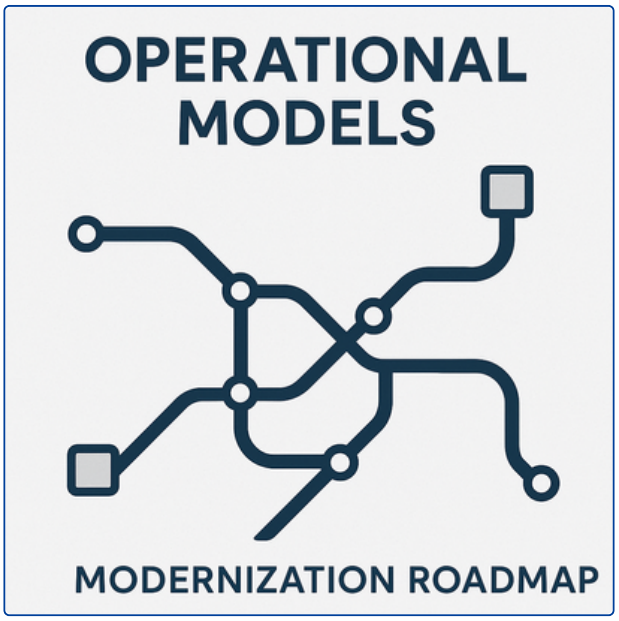
- Governance and tuning drive short-term wins: 15–30% efficiency gains are possible without platform replacement.
- Cloud adoption is on the rise, but most banks are still in early stages—hybrid environments are the norm.
- Modernization is best tackled incrementally: phase implementations, focus on high-risk/high-volume areas, and build internal expertise.



Key Takeaways - Continued

Market Outlook

- By 2025, AI/ML will be standard in AML monitoring for top-tier institutions.
- Regulatory expectations around explainability, oversight, and tuning transparency will tighten.
- Institutions that retain config control, build investigative capability in-house, and unify data architectures will lead in compliance effectiveness and efficiency.



Conclusion

The risk and compliance technology stack is undergoing serious transition. Some institutions are leaning into AI, convergence, and cloud—but many are still held back by legacy vendors, siloed data, and manual processes.

The message from the market is clear: effective compliance is no longer just about meeting regulatory minimums. It's about speed, adaptability, and control.

Institutions that treat compliance and risk systems as strategic assets—investing in configuration expertise, integrating data, and enforcing performance accountability—will reduce costs, increase effectiveness, and better position themselves for regulatory and operational resilience.

APPENDIX: GLOSSARY OF KEY SYSTEMS

System	Owner	Primary Function	Market Alternatives
Falcon	FICO (via FIS)	Card fraud detection using network-wide scoring	SAS Fraud Mgmt, Feedzai, ACI PRM, DataVisor
Prime Compliance Suite	FIS	AML monitoring, KYC scoring, SAR/CTR filing	Oracle FCCM, Verifin, BAE NetReveal
Actimize	NICE (via FIS)	AML and fraud platform (especially ACH/wire)	SAS AML, Verifin, Oracle AML, ThetaRay
Oasis (Argo)	FIS / Fiserv	Check fraud (payee positive pay)	Advanced Fraud Solutions, Jack Henry, AI-based checks
FraudChex	FIS	Check verification and fraud monitoring	Early Warning, Deluxe, CrossCheck

REFERENCES

1. Gartner Financial Services Research, "Predicts 2023: Financial Crime Compliance Technology"
2. Forrester Research, "The Total Economic Impact of Integrated Risk Management"
3. Aite-Novarica, "AML Technology Benchmark Study 2023"
4. McKinsey Global Banking Annual Review 2023
5. Deloitte Financial Services Risk & Compliance Survey 2023
6. EY Global Banking Technology Transformation Report
7. KPMG Financial Services Technology Insight Report 2023
8. Federal Reserve Supervision Workshop on Model Risk Management
9. OCC Semiannual Risk Perspective, Fall 2023
10. FinCEN Director Andrea Gacki, ACAMS AML Conference 2023
11. The Clearing House, "True Cost of Financial Crime Compliance Study"
12. ACAMS Today, "Balancing Risk and Efficiency in AML Monitoring"

STAY AHEAD
SCAN TO SUBSCRIBE
TO OUR UPDATES

HAVE QUESTIONS OR WANT MORE INSIGHTS?

If you have questions about this report or would like a similar intelligence briefing focused on other areas of the banking or finance industry—such as core system modernization, digital onboarding, payments, or operational resilience—we'd love to hear from you.

Reach out to our team at
info@coresystempartners.com
or
Visit
coresystempartners.com

To start a conversation.