

# Overcoming Deployment Challenges for Financial Crimes Platforms

by

**Brian Stoeckert**  
stoeckert\_brian@bah.com

**James Flowe**  
flowe\_james@bah.com



**Contents**

Introduction .....1

Fragmented Approach to Fraud Prevention .....1

Industry Consolidation and Convergence .....1

The Ecosystem: Supply Chain Technology Providers and Financial Institution Stakeholders .....2

Potential Pitfalls.....2

    Unrealistic Expectations .....2

    Lack of Strategic Vision and Senior Management Sponsorship .....2

    Delaying Definition of Reporting Requirements .....3

    Planning without Integrating Competing Priorities and Release Schedules.....3

    Inconsistent Stakeholder Support .....4

Conclusions .....5

    Avoiding Pitfalls with Third Party Expertise .....5

    Invest in Partnerships with Industry Experts .....5

    Convergent Risk Management for Financial Institutions .....6

About Booz Allen.....8

# Overcoming Deployment Challenges for Financial Crimes Platforms

## Introduction

*In today's dynamic financial crimes universe, sophisticated global syndicates continue to emerge and exploit a growing number of consumer electronic banking transactions. As a result, bank customers are increasingly vulnerable to illicit activity and financial institutions worldwide face significant operational, brand and reputational risks. Add to this, mounting regulatory pressure and aggressive law enforcement actions, and banks have no choice but to realistically acknowledge and assess the increasing frequency and variety of illicit activity. They must launch a proactive, vigilant response to financial crimes. This paper summarizes several inherent, real-world challenges encountered by banks of all sizes attempting enterprise-wide or channel-specific deployments. It provides insights and recommendations to overcome implementation obstacles, leverage opportunities, and achieve the organizational objectives associated with optimal deployment. By optimizing their enterprise financial crimes platforms, financial services organizations can vigorously enhance the protection and retention of customer relationships.*

## Fragmented Approach to Fraud Prevention

During the past decade, financial institutions have recognized the urgent need to address escalating fraud and money laundering activities that threaten the security of customer accounts across all delivery channels. Technology vendors have responded by offering a broad range of tools and platforms, such as detection and alerts, transaction monitoring, fraud prevention, and analysis and case management. These products have helped financial institutions combat financial crime. But, despite the continually enhanced capabilities of these risk management products, few financial institutions have successfully deployed an enterprise-wide financial crimes infrastructure. Typically, financial services organizations have

implemented disparate anti-money laundering (AML) and anti-fraud applications, technologies and systems in department silos. These products may address various types of alleged unlawful activity, but do not offer an integrated risk management framework. This fragmented approach to financial crimes detection and prevention allows criminals to execute malicious cross-channel illicit finance. Behavior that appears to be normal in one banking channel often proves to be suspicious when viewed more holistically across the institution landscape.

## Industry Consolidation and Convergence

During the past decade, most midsize and large financial services institutions have implemented transaction monitoring and case management tools. However, these systems are nearing end of life and can no longer be customized effectively to address evolving needs. As part of an effort to extend the scope, functionality and efficiency of financial crimes systems across channels and products, banks now want to upgrade or migrate to another vendor.

In the past 10 years, there has been a lot of movement in the technology market. After acquiring smaller entities, major platform players are now positioned to offer a broader range of more refined products and services. The latest technology platforms integrate data from multiple vendor tools and consolidate additional capabilities, such as Know Your Customer verification or due diligence, with core functionality, offering a more comprehensive approach to risk management.

In addition to technology advancements, today's financial institutions bring a more knowledgeable perspective to financial crimes platform deployments. In the early years of the 21st century, financial organizations implemented solutions that were AML driven and mostly reactive, in an effort to adhere

to regulatory obligations. Today's marketplace is more proactive. Banks try to address the challenges posed by a converging AML and fraud environment. Infrastructure vulnerabilities are exploited across channels. As a result, banks need to create a synergized and cost-effective defense strategy that transcends disconnected organizational silos. Whether a financial institution is forklifting an existing AML solution or implementing a new system to combat fraud, an enterprise view of risk management reduces exposure, loss, and the likelihood of regulatory action.

### **The Ecosystem: Supply Chain Technology Providers and Financial Institution Stakeholders**

Regardless of a financial institution's size, geographical reach, or status on the maturity curve in addressing financial crimes, all platform deployments involve supply chain vendors and internal stakeholders. Each brings their own self-interests, pain points and competing priorities that drive or impede adoption. On the supply side, multiple vendors provide financial crimes monitoring in real time or batch detection mode, analytics and case management solutions, technology and integration, and consulting services. Within the financial services organization, stakeholders include risk management groups (fraud, AML, operations, risk compliance), information technology (IT), and lines of business.

At the outset of an engagement, stakeholders usually agree on the need to implement a financial crimes platform. But few have deployment experience, which often leads to unrealistic expectations of achievable outcomes, and unclear definitions of ownership and day-to-day accountability. A completely different operational approach is required for responding to and managing the information that will be generated by the new tools put in place. But since this change management paradigm rarely is addressed at the start of the engagement, it proves difficult, if not impossible, to define expected business outcomes and lay the foundation for communicating success following deployment.

## **Potential Pitfalls**

### **Unrealistic Expectations**

Once a financial institution decides to implement an enterprise financial crimes platform, bringing in competing technology vendors to describe their offerings is one of the first steps. Problems arise in this phase due to disparities between the products' "advertised" capabilities and its actual integration with a specific bank's systems. The vendor claims it can meet the financial institution's stated business requirements. However, as the customization process unfolds, discrepancies and hurdles surface. For example, a software vendor may sell a global and centralized consumer centric approach. But if the bank's legacy data management structures are account versus consumer driven, the new technology platform will not deliver all the attributes demonstrated during the sales pitch. Inaccurate mapping of tool functionality to existing infrastructure leaves the financial services customer with a solution that falls short of the vision.

Related to the initial discrepancy between a solution's advertised and actual capabilities is how the initiative is implemented. Technology vendors typically sell the solution to the financial institution's line of business stakeholders—the ultimate owners and end users. However, as implementation gets underway, these initiatives typically are managed and viewed as technology projects instead of business projects, even though business efficiency and return on investment are the stated goals.

New information often surfaces during the discovery process, creating new challenges and opportunities throughout implementation. Successful deployments feature clear and consistent communication among stakeholders regarding ownership and management of these unanticipated disruptions.

### **Lack of Strategic Vision and Senior Management Sponsorship**

If a business unit does not feel acute pain associated with a fraud threat, such as losses, it is unlikely to fund a financial crimes infrastructure initiative. In

addition, it will not change its business processes to support an initiative without a clear business case and return on investment defined in the organization's strategic vision. Many financial institutions embarking on these deployment projects lack a supporting strategy, often because no member of the senior leadership team owns or champions a mandate for financial crimes infrastructure implementation.

Banks should not proceed with an enterprise financial crimes infrastructure initiative without a clear risk management operational strategy that defines and unifies business benefits for all stakeholder groups that will influence and participate in deployment. They cannot implement an enterprise solution without buy-in across the organization, and senior management leadership is required to facilitate that cooperation.

#### **Delaying Definition of Reporting Requirements**

Once the enterprise financial crimes strategy is in place, business managers are often unsure how to execute it and report on performance. During the early stages of the project, stakeholders are keenly focused on defining business and system requirements, choosing vendors, procuring technology, and, most importantly, determining how to activate the system on time and on budget. In this phase, reporting requirements are simply not a priority. However, when these issues are not addressed up front, business managers are left with inadequate reporting mechanisms to measure performance, manage effectiveness, maximize efficiency, and balance resources. They lack reporting procedures to deliver on strategy, as well as communicate the ongoing business impact and benefits of the new financial crimes infrastructure.

Transaction monitoring and case management tools deliver fundamental reporting capabilities. But in order to derive the full value of this functionality and accomplish the financial institution's specific risk management objectives, implementation teams must design optimized dashboards that move beyond baseline reporting and data aggregation. Standard reporting mechanisms must be augmented to measure

business impact—such as reductions in exposure and loss—and help the financial institution achieve significant and sustainable process improvements. Enhanced reporting mechanisms transform information into knowledge. Integrating performance analytics aligned with organizational objectives enables the system to provide workflow visibility and help managers effectively leverage resources to boost productivity and operational efficiency—but only if reporting requirements and actionable metrics are baked into the infrastructure from the start.

Tackling reporting requirements at the start of the project is also important because of the short term engagement of subject matter experts (SME). With budget and timeline constraints, early-stage SMEs typically leave the team after completing their tasks in the initial phase. During the first several months of the project, these consultants analyze all current business processes and construct a clear cross-channel view of how the tool will be used throughout the organization from an operational perspective. However, when these SMEs are no longer engaged, a valuable resource is lost. It becomes increasingly difficult to determine how to quantify, validate and articulate post-implementation business results and value to internal constituents and to regulators. The project often erroneously shifts from a business to a technology initiative at this time.

Postponing the effort to define and align reporting requirements with strategy is a common fallacy of enterprise technology deployments. But if processes for measuring and managing performance are not integrated into the infrastructure implementation plan, the organization will face significant challenges in documenting and communicating project success and tangible business results.

#### **Planning without Integrating Competing Priorities and Release Schedules**

In addition to defining reporting requirements early on, another critical element of the planning process is working with business partners, especially vital IT support. Implementation teams should ask business partners about their other project roadmaps,

priorities and commitments for the next 12 months, as well as time requirements for this deployment. A pragmatic approach to timeline development will enable realistic scheduling of the financial crimes infrastructure deployment based on IT bandwidth and availability. With prior planning, this enterprise project can potentially avoid getting sidetracked by other business unit initiatives viewed as more important revenue generators. This approach not only facilitates successful implementation, but also secures critical ongoing IT support for effectively managing the system long after deployment.

In addition to holiday and vacation schedules, it is important to map software release schedules against the project plan. Different versions of technology platforms are optimized for transaction monitoring versus case management needs, for example, or for the ACH/wire channel versus general checking. It is also critical to engage in due diligence up front and define the delta between currently available products and new releases to determine if waiting for a new version is justified based on business requirements and strategic objectives.

### **Inconsistent Stakeholder Support**

Financial crimes platform deployments can last six months or more. Although implementation teams may have secured IT's commitment as recommended above, it is not uncommon to lose individual IT and risk management tacit knowledge experts to other projects or roles during the duration of the project, especially in today's dynamic workforce environment. These investigators and analysts bring unique understanding of the kinds of data AML and fraud experts need, as well as of related internal processes. Therefore, implementation teams should secure their continuous involvement in the project whenever possible. Losing their ongoing commitment can impact project ownership, urgency, visibility, vision and scope.

Also, the software vendor team and the IT architect and system analyst supplied by the infrastructure vendor may not be on site and dedicated exclusively to the enterprise project. Instead they may function as on-call SMEs, which could cause delays.

With inconsistent stakeholder support, the project could be put on hold. Its scope and deployment plans could be revisited, and budgets reevaluated.

## **Hypothetical Scenario**

A top 20 bank, with a decentralized financial crimes organization, was growing quickly due to acquisitions. It deployed a leading transaction monitoring, analytics and case management solution in its AML area. AML then led an initiative to migrate the solution to the bank's fraud organization, as part of an effort to extend the reach of the vendor's tool in the enterprise and gain more control over its use. Stakeholders from IT, risk management, and lines of business recognized that this deployment would require fundamental changes in daily operations, as well as additional resources. Subsequently, the leader of the fraud organization took ownership of the project to circumvent AML dictating how his group would operationalize the tool. The lack of an executive-sponsored enterprise strategy defining the

exposure and reputational risk faced by this institution, and representing the interests of all stakeholders—coupled with an unrealistic project plan and timeline—quickly derailed this project. In addition to ownership transitioning from the AML silo to the fraud organization well after the project was underway, the scope of the initiative changed twice. And, since competing IT priorities were not taken into account during the planning phase, the go-live date was unrealistic, and the architectural design milestone was delayed by more than two months, essentially throwing the project into limbo. The subject matter expert consultants were long gone by then, and internal IT staff members were committed to other projects.

This situation would lead to significant delays and cost overruns. A successful financial crimes platform deployment would be unattainable.

## Conclusions

### Avoiding Pitfalls with Third Party Expertise

Once funding is allocated for an enterprise financial crimes deployment, the chain of command signs off on the project plan, and internal and external partners are in place. At this point, it is tempting to move full steam ahead with system implementation and worry about optimization later. However, without an enterprise financial crimes strategy sponsored by senior management and supported by all stakeholder groups, implementation teams cannot define the performance metrics for the new infrastructure that will enable them to verify and communicate business impact. Similarly, IT and business line involvement can make or break the initiative, so it is important to understand stakeholder schedules, processes and requirements, and confirm their commitment to resource allocation before finalizing the project plan and timeline.

All of these potential deployment pitfalls can escalate vendor dependency and lead to significant cost overruns. When the scope or business requirements associated with a financial crimes installation are unclear from the start or change during implementation, the vendor holds the institution financially accountable for additional optimization services. This results in budget conflicts between the bank's internal departments as they negotiate how to accommodate the increased costs.

These challenges and the cost overruns associated with them are, of course, not unique to the deployment of financial crimes infrastructure. The Standish Chaos Reports indicate that in 2009, 24 percent of major software implementation projects failed, 44 percent were challenged, and only 32 percent succeeded. Miscommunication between business units and IT contribute to a 66-percent project failure rate, costing U.S. companies at least \$30 billion annually, according to Forrester Research.

All successful enterprise infrastructure initiatives require a clear strategy, senior management leadership, the ability to effectively measure and manage performance and business impact. They also need a comprehensive understanding and integration of stakeholders' competing priorities and schedules as part of realistic project planning. Only an objective third party with industry-specific expertise can effectively represent the collective business interests of all stakeholder groups and effectively mitigate the cost impact of unanticipated project requirements. Financial institutions require an advocate with deep understanding of current technology offerings, risk management and compliance best practices, and the organization's history and current position on the financial crimes maturity curve.

### Invest in Partnerships with Industry Experts

Given the complexity of financial crimes platform deployments and constantly evolving technology offerings, financial institutions often turn to third-party consultants. When selecting an implementation advisor, it is critical to identify an objective partner that brings not only business acumen, but also a proven track record in the financial services industry and no allegiance to any particular technology vendor or offering.

Recalling the ecosystem introduced in the first section of the paper, platform vendors have a vested interest in selling software. Infrastructure providers want to protect and manage their client relationships, and internal stakeholders often voice objectives that conflict with broader organizational goals. But financial institutions need a player whose reason for engagement is to ensure the financial institution's successful management of financial crimes. They need an advocate whose focus extends beyond the technology, integration and consulting revenue. They require a player who also concentrates on the end game—the new financial crimes infrastructure that delivers return on investment via an improved risk management posture.

### **Convergent Risk Management for Financial Institutions**

Booz Allen Hamilton serves in this critical value-add advocacy role as an objective, independent third-party liaison. We represent the collective interests of all stakeholders for the successful deployment of a financial crimes infrastructure based on core values and strategy. We ensure that the strategy driving the initiative has the support of key constituents and consistently aligns with the expected business benefits defined by all players. Our consultants bring proven, hands-on operational expertise and tacit knowledge to every stage of planning, deployment and optimization of current technology tools and platforms for financial crimes infrastructure. We have a deep understanding of operational, technology, regulatory, cultural and political challenges specific to the complex and dynamic convergent risk management environment that permeates today's financial services industry. We possess the industry-specific subject matter expertise to help develop new analytic models to improve a financial institution's risk posture in a constantly evolving market.

Booz Allen Hamilton's convergent risk management consultants will help integrate performance analytics into standard reporting mechanisms so that financial institutions can consistently connect individual stakeholder group objectives to broader organizational goals, and achieve and communicate the desired outcomes defined in their enterprise financial crimes strategy.

While market consolidation has resulted in technological advances that deliver broader product capabilities to financial institutions, integration challenges remain as many solutions are complex hybrids of former offerings. We facilitate and coordinate vendor relationships that ensure the most successful financial crimes infrastructure implementation for our client organization.

### ***Booz Allen's Core Competencies and Market Expertise***

- Mission Engineering®
- Enterprise Financial Crimes Strategy
- Change Management/Organizational Development
- Risk Management Technology Tools and Solutions
- Practitioner Support and Managerial Oversight in all Risk Management Operational Disciplines
- Optimization of Off-the-Shelf Analytics Systems
- Deployment (all phases)

Implementations fail because technology providers and business consultants lack the industry expertise to address business process and change management complexities. Technology providers and business consultants also do not possess a comprehensive understanding of achievable business results for financial institutions at various stages of the financial crimes maturity curve.

Put your financial crimes infrastructure deployment in the hands of an advocate that will ensure your vision becomes a reality. Booz Allen Hamilton's convergent risk management professionals provide financial institutions with an enterprise approach to proactive management of converging risks and regulatory compliance requirements. Our practice areas include financial intelligence and analytics, financial crimes, cybersecurity, operational risk and compliance management.

## About the Authors

**Brian Stoeckert** is a recognized expert in financial crimes and specializes in convergent risk management, merger and acquisitions, financial intelligence in anti-money laundering, fraud, counter terrorist financing, and open source intelligence methods. He has managed enterprise-wide BSA/CTF/Fraud program platform deployments and asset integration through mergers and acquisitions. Mr. Stoeckert also leads the counter terrorism finance training program for commercial markets. He is frequently called upon by financial crimes prevention organizations to serve as an expert speaker and instructor at conferences and training sessions. He received his juris doctor from New York Law School and his bachelor of arts from Stony Brook University. He is a Certified Fraud Examiner (CFE) and a Certified Anti-Money Laundering Specialist (CAMS). Mr. Stoeckert is the recipient of the 2011 ACAMS Volunteer of the Year Award.

### Contact Information:

**Brian Stoeckert**

Associate  
stoeckert\_brian@bah.com  
917-554-9903

**James Flowe** specializes in financial crimes convergent risk management and is a leader in operations efficiencies with an emphasis on strategy, process, project, and change management. He is recognized for creative and innovative ways in supporting strategic and tactical initiatives in leading successful business solution implementations. In a trusted advisor relationship, Mr. Flowe has led business requirements and gap analysis efforts to determine client needs in solution deployment, optimization, data mapping, use cases, and facilitated workshops with business units on best practices in rolling out new operational processes. He focuses on organizational design and process work-stream solutions that include ACH/Wire, real time fraud monitoring, enterprise case management, AML transaction monitoring, know your customer, and due diligence. Mr. Flowe received his bachelor of science in finance with real estate concentration from East Carolina University.

**James “Jay” Flowe**

Associate  
flowe\_james@bah.com  
704-591-1552

## About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, Booz Allen is a leading provider of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. In the commercial sector, the firm focuses on leveraging its existing expertise for clients in the financial services, healthcare, and energy markets, and to international clients in the Middle East. Booz Allen offers clients deep functional knowledge spanning strategy and organization, engineering and operations, technology, and analytics—which it combines with specialized expertise in clients’ mission and domain areas to help solve their toughest problems.

The firm’s management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate

needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining a consultant’s problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm’s many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 25,000 people, and had revenue of \$5.59 billion for the 12 months ended March 31, 2011. *Fortune* has named Booz Allen one of its “100 Best Companies to Work For” for seven consecutive years. *Working Mother* has ranked the firm among its “100 Best Companies for Working Mothers” annually since 1999. (NYSE: BAH)

*To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit [www.boozallen.com](http://www.boozallen.com).*

## Principal Offices

Huntsville, Alabama	Indianapolis, Indiana	Philadelphia, Pennsylvania
Sierra Vista, Arizona	Leavenworth, Kansas	Charleston, South Carolina
Los Angeles, California	Aberdeen, Maryland	Houston, Texas
San Diego, California	Annapolis Junction, Maryland	San Antonio, Texas
San Francisco, California	Hanover, Maryland	Abu Dhabi, United Arab Emirates
Colorado Springs, Colorado	Lexington Park, Maryland	Alexandria, Virginia
Denver, Colorado	Linthicum, Maryland	Arlington, Virginia
District of Columbia	Rockville, Maryland	Chantilly, Virginia
Orlando, Florida	Troy, Michigan	Charlottesville, Virginia
Pensacola, Florida	Kansas City, Missouri	Falls Church, Virginia
Sarasota, Florida	Omaha, Nebraska	Herndon, Virginia
Tampa, Florida	Red Bank, New Jersey	McLean, Virginia
Atlanta, Georgia	New York, New York	Norfolk, Virginia
Honolulu, Hawaii	Rome, New York	Stafford, Virginia
O'Fallon, Illinois	Dayton, Ohio	Seattle, Washington

*The most complete, recent list of offices and their addresses and telephone numbers can be found on [www.boozallen.com](http://www.boozallen.com)*