WINNING AT THE POINT OF ATTACK

WITH INTEGRATED FINANCIAL CRIME OPERATIONS

accentureconsulting

Global losses associated with financial crimes continue to climb year over year. Managing the risks associated with money laundering, fraud and cyber has never been a more timely imperative for financial institutions to protect their clients, employees and reputation while enhancing the resilience of the global financial system.

Our experience indicates that financial institutions can significantly increase both efficiency and effectiveness of their financial crimes risk management framework. We believe institutions can raise efficiency by as much as 30 percent – with substantial improvements in resilience and client experience – through a more integrated operating model for financial crime risk management. Transforming financial crimes risk management requires a dual focus, addressing "above the line" improvements to the client experience as well as "below the line" operational excellence that, while not visible to clients, can generate significant economic benefits. As our title indicates, this paper concentrates on below the line initiatives.

Strengthening the operational performance of anti-money laundering (AML), fraud and cyber controls requires coordination across all lines of defense and calls upon stakeholders to make trade-offs for the benefit of the enterprise.

"When integrating financial crime controls within their operating model, financial services firms benefit from greater resiliency and efficiency while delivering an enhanced client experience."

There is no single proven solution for integrating the delivery of financial crimes controls. Leading institutions, however, are making significant investments in data and infrastructure, building the foundation for using analytics and intelligent automation to extract greater value from applications and increase the productivity of financial crimes officers. Through our own research, and through extensive experience with financial services clients, we have identified five common challenges for financial institutions to address.

We have established 12 guiding principles to address these common challenges and help financial institutions realize the qualitative and quantitative benefits associated with greater integration of financial crimes controls within their operating models. Applying the 12 principles helps create a future functional blueprint for financial crimes risk management, retaining the integrity of component risks (such as AML, fraud and cyber) while increasing convergence opportunities within both the first and second lines of defense.

In 2018 alone, over $30 billion global card losses associated with fraud are expected.[1]

ATTACKING A COMPLEX GLOBAL PROBLEM

Financial crime is a global problem, encompassing a wide range of illegal activities such as drug dealing, human trafficking, sales of illegal arms and marketing of counterfeit goods, and the sums involved are enormous.

Depending on estimates, the value of AML-based crimes can range between $704 and $893 billion, fraud-based crimes are estimated at over $183 billion, while cyber-based crimes are estimated in the $600 billion to $3 trillion range. As for the global trade in illegal drugs it is estimated at between $426 and $652 billion.[2]

Criminals are often able to change their attack strategies faster than institutions can react. The speed of innovation – represented, for example, by new payment systems and the rise of cryptocurrencies – as well as the increased velocity, variety and volume of data pose significant obstacles for firms seeking to keep up with perpetrators of financial crime. At the same time, clients seek services on demand; Accenture research indicates, for example, that 68 percent of Generation Z consumers surveyed want instant person-to-person payments.[3]

Another problem is the scarcity of the digital skills needed for supervision and quality control of crime prevention activities. Even among "digital transformer" firms, nearly two-thirds (61 percent) of firms surveyed by Accenture said they have difficulties in attracting and retaining top digital talent.[4] Adding additional pressure is the increasing complexity and new demands of regulations, such as the reporting of cyber events under the Financial Crimes Enforcement Network Bank Secrecy Act (FinCEN BSA) requirements.

DELIVERING RESILIENCE, EFFICIENCY AND A BETTER CUSTOMER EXPERIENCE

We believe that, for optimal effectiveness and efficiency, a more integrated model should be used to coordinate financial crimes controls across all three lines of defense.

When properly designed and implemented, a more integrated financial crime risk management program can deliver benefits in three key areas:

1. Resilience

Proactively identifying and mitigating a rapidly changing risk environment through capability that is prepared for future industry demands. For example, the organization should aim to avoid all regulatory fines while delivering consistent reviews of its digital products. Some fraud losses are inevitable, but they should remain within the firm's established risk appetite.

2. Efficiency

Improving execution across lines of defense and leveraging common capabilities for scalable, efficient infrastructure. As a desired outcome, the timeframe for investigation closure should shrink and utilization of investments for multiple purposes should increase.

3. Client Experience

Making real-time, risk-based decisions that reduce friction for the client, with controls that constantly learn from interactions. For example, through greater integration of controls within their operating models, financial institutions can reduce the time needed for client onboarding by 20 to 30 percent and the time for fraud case resolution by 15 to 30 percent. Clients' trust in the organization should increase, reducing "churn" and making client acquisition easier.

Of these three main areas, resilience and efficiency are generally "below the line," focusing on operational excellence to execute higher quality controls at a lower cumulative cost. The client experience – with its emphasis on retention and increased trust – is generally "above the line" and will be addressed in a separate paper.

Reduce time needed for client onboarding by 20-30% and reduce time for fraud case resolution by 15-30%

FINDING THE RIGHT CONTROL STRUCTURE

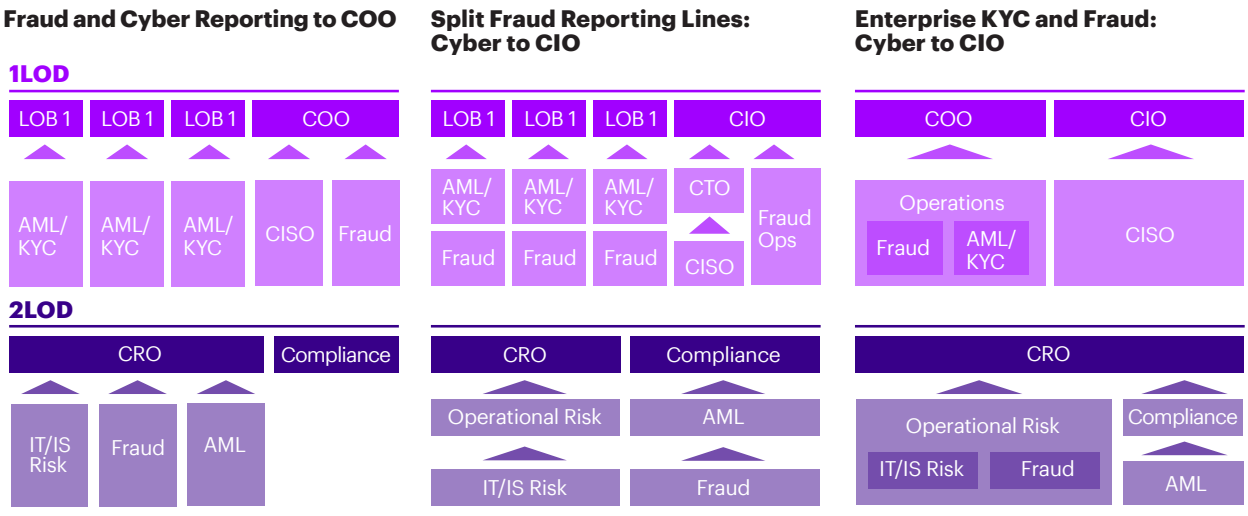
Accenture's experience indicates that finding the preferred focus for improving operational performance requires evaluation and selection of sometimes contrasting priorities.

Making a trade-off between the individual priorities of senior managers, such as the Chief AML Officer, the Chief Information Security Officer (CISO) and other key roles, in order to arrive at the best solution for the institution is often essential. Three factors can determine the path chosen by each financial institution:

- Governance – whether leadership for the transformation comes predominantly from the first or second line of defense, or is technology led;
- Risk appetite – how closely a financial institution seeks to protect against losses and/or data breaches as the product offerings expand within a digital agenda; and
- Investment expectations of senior management – whether transformation is viewed as a key opportunity to bend the cost curve of risk management.

There is no single or best formula for operational improvement, as evidenced by the multiple operating models seen today. Figure 1 below shows three examples of organizational structures to support the delivery of financial crime controls.

Figure 1. Examples of Organizational Constructs for the Delivery of Financial Crime Controls



LOB: Line of business, LOD: Line of defense

Source: Accenture, March 2018

Regardless of the model chosen, we typically encounter five common challenges:

Challenges	
Organizational Fragmentation	Organizational fragmentation across AML, fraud and cyber domains, leading to opportunistic rather than strategic asset sharing and investment (such as the use of artificial intelligence or the sharing of threat intelligence).
Inconsistent Execution	Inconsistent execution of the three lines of defense principle, leading to gaps in coverage in areas such as risk advisory support, misalignment of resources and overlap in the delivery of controls such as testing and case management.
Absence of Holistic IT Architecture	Absence of holistic IT architecture, leading to duplicative investments, longer application upgrade cycles, and tactical rather than strategic approaches to planning technology projects such as the adoption of cloud infrastructure.
Lack of Common Data and Process Taxonomy	Lack of a common data and process taxonomy, adding complexity to working with data teams and creating difficulties in governing data assets and exposing accountable officers to challenges with control attestation. In our experience, this can be a root cause of inefficiency in the technology infrastructure as well as organizational fragmentation, necessitating near term focus.
Lack of Dedicated Career Path	Lack of a dedicated career path for financial crime professionals, increasing turnover risk, hampering the development of future-focused skills such as non-financial risk quantification and forensic investigation, and reducing opportunities to create fungible resource pools to serve AML, fraud and cyber-crime needs.

In addressing these concerns, we recommend 12 principles for financial institutions to help achieve the qualitative and quantitative benefits associated with greater integration of financial crime controls within their operating models. These can be seen in the sidebar on page 7.

ORGANIZATIONAL FRAGMENTATION

1. Governance. Establish an integrated, empowered forum that meets on a regular basis so that discretionary spending supports a "build once, use often" approach to capability delivery across AML, fraud and cyber activities, for example across data and technology assets.

2. Monetization. Identify opportunities to monetize in-house capabilities by allowing peer institutions to use these capabilities on a paid subscription basis.

3. Client Centricity. Establish a 360-degree view of each client, using analytics to support proactive investigations and to better target resources such as control testing.

INCONSISTENT EXECUTION OF THREE LINES OF DEFENSE PRINCIPLES

4. Shared Services. Capture opportunities to deliver common controls such as threat intelligence, testing and analytics across all financial crimes domains, leveraging enterprise GRC (Governance, Risk and Compliance) where available.

5. Case Management. Standardize the definition of a "case" as opposed to an "alert" or an "issue" across financial crime domains, again leveraging enterprise GRC.

ABSENCE OF HOLISTIC "IT" ARCHITECTURE

6. Artificial Intelligence (AI). Deploy a holistic strategy for the use of AI across all financial crime domains and pursue a similar strategy for adoption of further innovation (such as blockchain) at scale.

7. Cloud. Migrate applications to cloud-based infrastructure where feasible, and for a more modular and scalable infrastructure.

LACK OF COMMON DATA AND PROCESS TAXONOMY

8. Data Management. Appoint a data officer to partner with the enterprise Chief Data Officer to improve and maintain data quality in each financial crime domain, including development of a framework that can support controls such as data loss protection.

9. Taxonomy. Establish traceability from financial crime regulations and business strategies to affected policies, risk categories, and procedures and controls, tracking by line of business or entity.

LACK OF DEDICATED CAREER PATH

10. Job Market Differentiation. Develop a unique value proposition in the financial crime talent market, distinguishing the organization through its innovative training methods, its job rotation program, or its accelerated promotion path for "hot" skills.

11. Resource Fungibility. Capture opportunities for shared resource pools – for capabilities such as management reporting or control testing – serving AML, fraud and cyber-crime teams.

12. Talent Business Case. Review the business case for hiring talent to reflect complexity and the acceleration of improvement in the risk environment under digital transformation, in addition to cost.

CONVERGING AND STRENGTHENING LINES OF DEFENSE

The 12 principles can serve as the basis for a functional blueprint for financial crimes risk management that retains the integrity of component risks while increasing opportunities for convergence in the first and second lines of defense. This can be addressed either functionally – through the business process – or technically via the data and IT architecture.

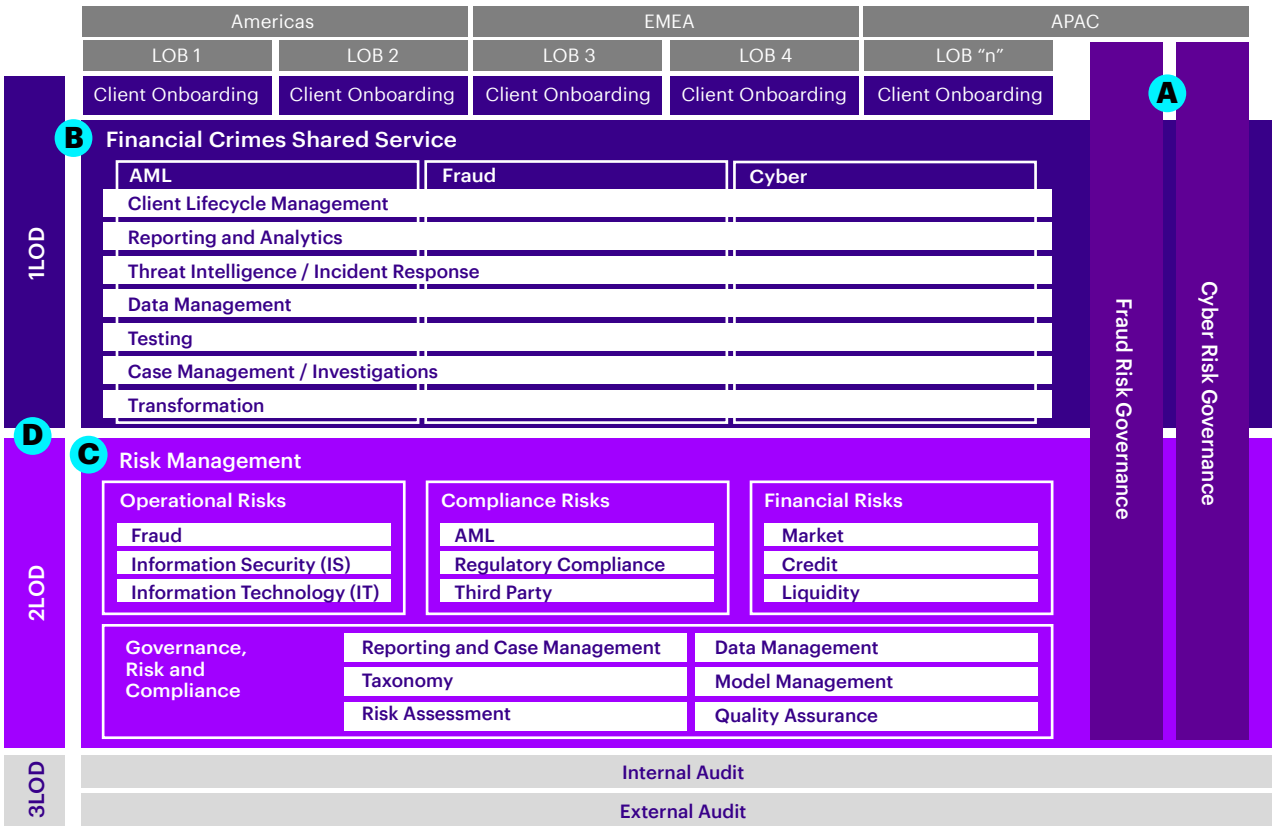
As seen in Figure 2, **A** governance of fraud and cyber requires front-to-back management across lines of defense and balancing resources among competing priorities including new product development, delivery of controls through a financial crime shared service, or second line oversight.

B Common risk management activities in the first line can be identified and addressed within a shared services construct, establishing greater consistency in execution, efficiencies in delivery, and additional career development opportunities, while retaining the integrity of individual risk types.

C Greater functional integration within the first line is then reflected in the second line of defense, as enterprise-wide GRC opportunities are captured while the organization retains unique controls for operational, compliance and finance risks.

Finally, **D** further innovation in the operating model generates additional benefits in how activities are delivered. These include the use of managed services and industry utilities, and the exploitation of opportunities to monetize delivery of controls by offering them on a subscription basis to other financial institutions.

Figure 2. A Future Blueprint for Increased Functional Integration



LOD: Line of Defense

Source: Accenture, March 2018

EFFICIENCY AND EFFECTIVENESS THROUGH DATA AND IT TRANSFORMATION

Improved integration of business processes is dependent upon a more holistic data and technology architecture. Both elements need to transform together to be mutually supportive and optimally effective.

Leading financial institutions are making significant investments in data and infrastructure. A well-designed technology architecture makes it easier for new technologies such as analytics and intelligent automation to extract greater value from applications and to increase the productivity of end users. Figure 3 illustrates how such an architecture can improve both the efficiency and the efficacy of financial crime risk management.

As seen in the illustration, a sourcing layer aggregates internal and external data to enable the use of one common data set, with appropriate sharing of data elements, structured within the boundaries of enterprise risk and control taxonomy.

Investment in infrastructure supports the processing of big data while providing sufficient storage to allow for auditable evidence of all actions taken, using the cloud for added flexibility.

An application layer supports individual functions such as sanctions screening for AML and fosters operational efficiencies for new shared capabilities such as threat intelligence.

At scale, front to back intelligent automation delivers the innovation needed to improve business outcomes, including robotics to support know your customer (KYC) data gathering, artificial intelligence to identify false positives, natural language processing for document review, and natural language generation to draft decision-related documents.

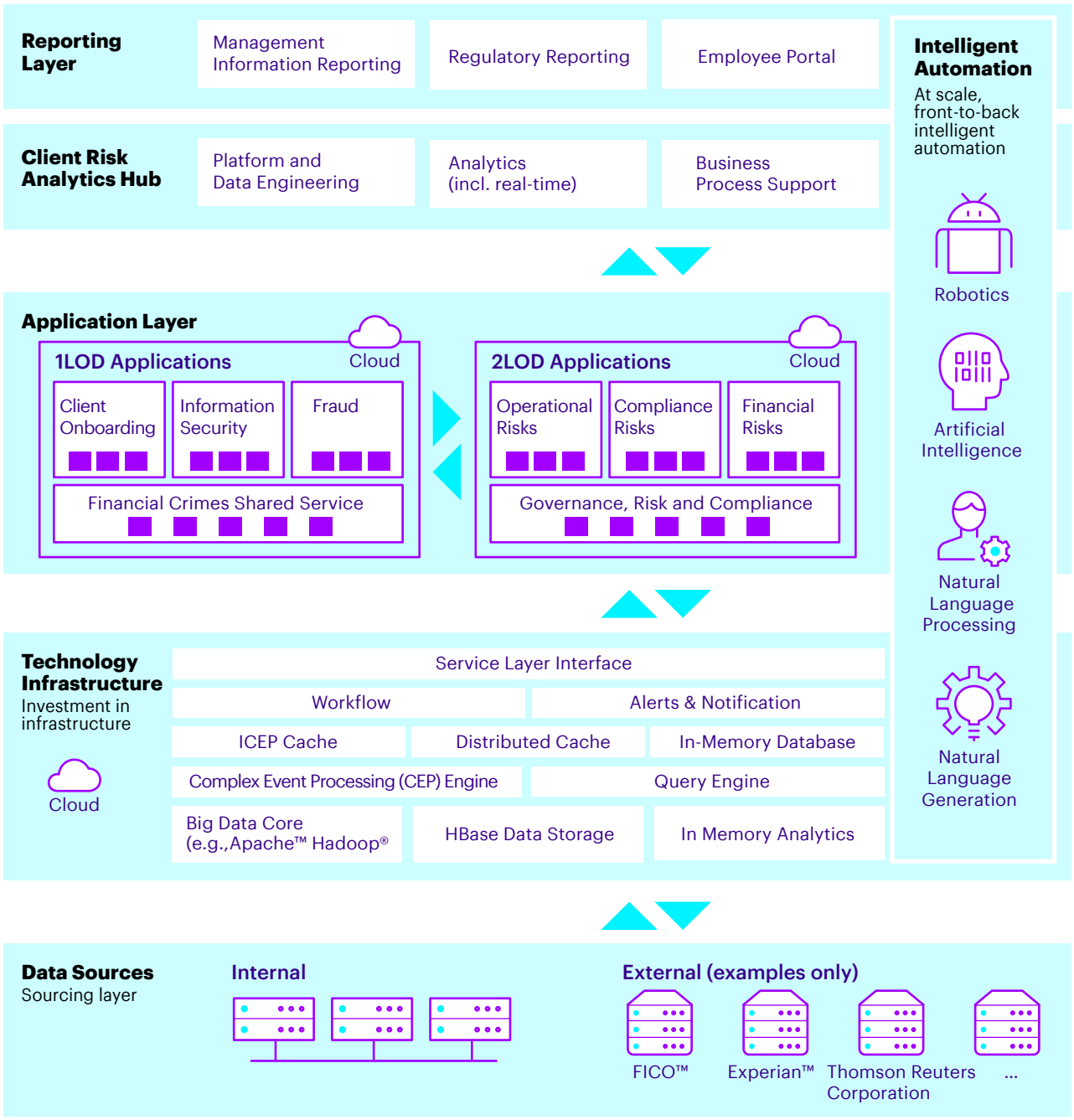
A client risk analytics hub facilitates investigations, drives continuous tuning of surveillance scenarios in applications, and provides enterprise-wide capability for obtaining 360-degree views of each client.

Finally, a reporting layer allows users to review financial crime threats holistically, supporting risk-based decisions and improving the efficiency of regulatory reporting.

Organizations are bringing these theories to life by transforming specific processes, with transaction monitoring providing a good example of a business process that companies are beginning to re-engineer.

Figure 3. Driving Towards a More Holistic Data and IT Architecture

Illustrative technology architecture (non-exhaustive)



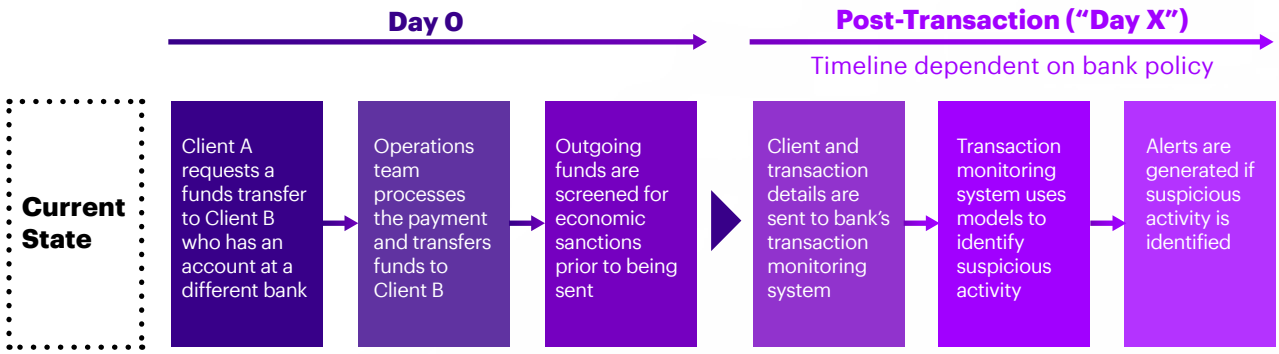
iCEP: Intelligent CEP
FICO: A credit score developed by Fair Isaac Corporation
LOD: Linked Open Data

Source: Accenture, March 2018

USE CASE

TRANSACTION MONITORING

Greater integration of AML, fraud and cyber controls can have tangible client experience, resiliency and efficiency benefits for any financial crimes use case. Here, transaction monitoring is featured as an example.



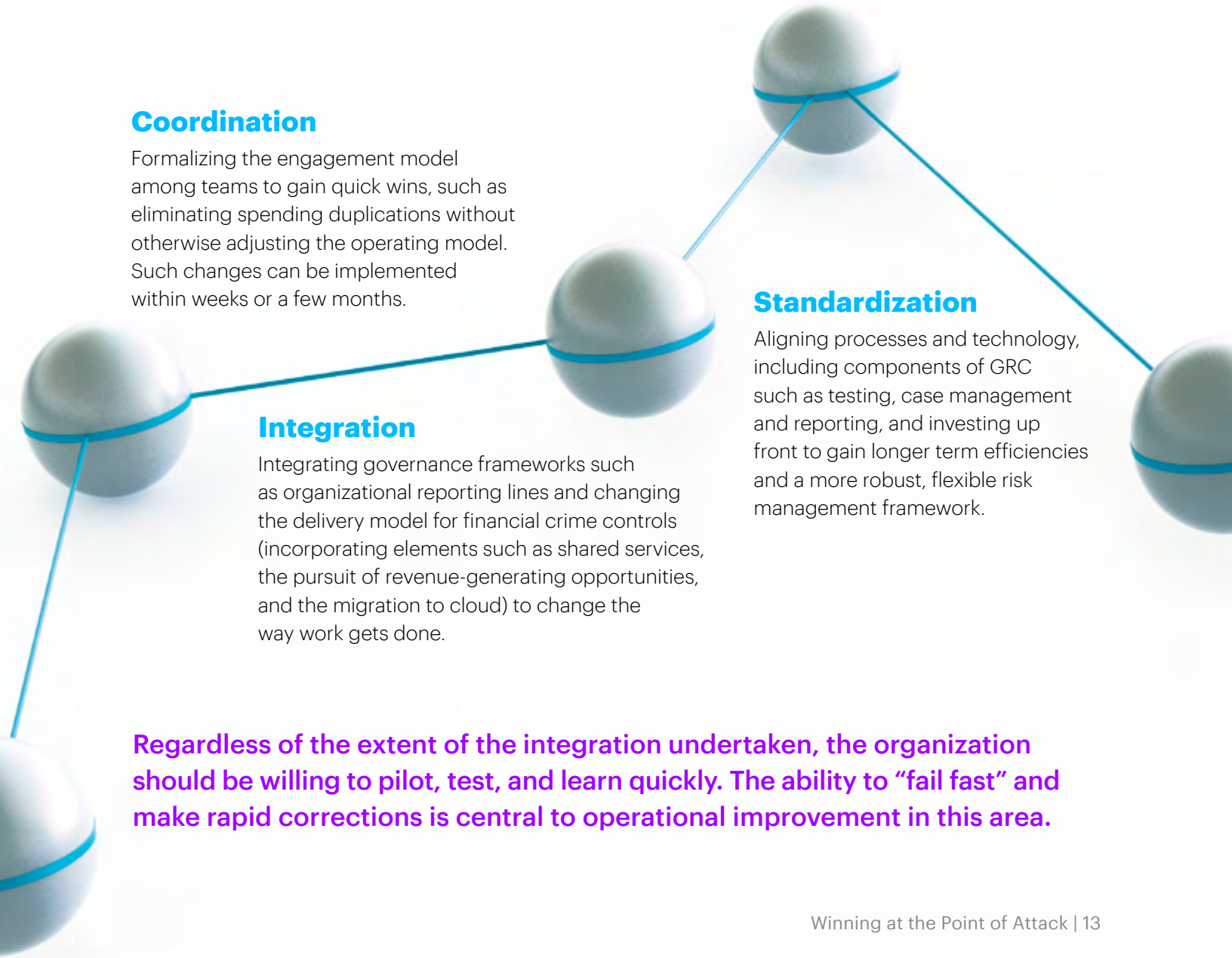
Examples of Future State Opportunities

Enhanced Client Experience	
Analytics identifies transaction amount and destination data based on prior behaviors and for Client A to validate	Successful transaction generates report back to Client A of value and pattern of payments to Client B
Resilience	
Enhanced authentication layers confirm Client A's intent to transfer money to mitigate fraud risk should payment context vary from typical behavior	In the event of an alert, the IP address of the device originating the transaction is automatically added to an enterprise security watchlist
Efficiency	
Screening of payment utilizes common control infrastructure within shared service	Artificial intelligence at scale drives synergies and permits self-tuning of models to increase efficiency and quality of alerts

Source: Accenture, March 2018

SETTING OUT ON THE INTEGRATION JOURNEY

Financial institutions make a significant strategic choice when they seek to integrate AML, fraud and cyber-crime activities. Firms have different definitions of what "integration" is in the context of AML, fraud and cyber risk management and may also differ in their appetite for integration and their commitment to up-front investment. Broadly speaking, firms can "land" in several places, including:



Coordination

Formalizing the engagement model among teams to gain quick wins, such as eliminating spending duplications without otherwise adjusting the operating model. Such changes can be implemented within weeks or a few months.

Integration

Integrating governance frameworks such as organizational reporting lines and changing the delivery model for financial crime controls (incorporating elements such as shared services, the pursuit of revenue-generating opportunities, and the migration to cloud) to change the way work gets done.

Standardization

Aligning processes and technology, including components of GRC such as testing, case management and reporting, and investing up front to gain longer term efficiencies and a more robust, flexible risk management framework.

Regardless of the extent of the integration undertaken, the organization should be willing to pilot, test, and learn quickly. The ability to "fail fast" and make rapid corrections is central to operational improvement in this area.

CONCLUSION – MAKING FINANCIAL CRIME RISK MANAGEMENT WORK

CHANGING THE ENDING FOR FINANCIAL CRIME RISK MANAGEMENT

The idea of transforming AML, fraud and cyber risk management through integration is not a new concept and firms have tried different approaches with varying degrees of success. Integration can yield significant benefits for financial services firms, but it can be a difficult undertaking with many potential pitfalls. We have seen firms avoid or eliminate these pitfalls by taking specific steps including:

Potential Pitfall	Success Factor
Oversimplifying the integration	Calibrating the level of integration to be pursued across AML, fraud and cyber, recognizing the unique nature of each risk and making sure that controls are not compromised.
Fixating on one strategy	Retaining flexibility to adjust for changes in the regulatory environment, as well as changes in business strategy or technological innovations that may disrupt the environment.
Key person dependencies	Effective succession planning to help diffuse dependencies on key people, both in transition and in newly created leadership roles.
Diluting key risk management principles	Allowing the business to own, understand, identify and manage risks in line with regulatory expectations.
Neglecting change management	Managing transformation as a cultural and capability change, with thoughtful communications and training to create understanding and buy-in among stakeholders.

ABOUT THE AUTHORS

Chris Thompson

Chris Thompson is a Senior Managing Director, based in New York and leading the Accenture global Financial Services Security and Resilience practice. The Security and Resilience practice helps clients manage cyber risk: the subversion of information risk controls for the agenda of the perpetrator. It unifies security, operational risk, fraud and financial crime and provides end-to-end services across strategy, simulated attacks, consulting and managed service delivery. Chris has over 20 years of experience in large-scale change programs, working with some of the world's leading retail, commercial and investment banks.

Jon Narveson

Jon is a Managing Director with Accenture Finance & Risk and serves as the North America Risk Management Capability Lead. Based in Charlotte, N.C., Jon works with major financial services institutions to develop risk-based strategies, controls and risk mitigation programs to manage high impact and emerging risks and issues including operational risk, cyber risk, fraud and financial crime, and financial risk.

Ben Shorten

Ben is a Senior Manager with Accenture Finance & Risk. Based in New York, Ben serves as the Compliance Transformation Offering Lead for Accenture in North America. Ben has extensive experience working with investment banks, retail banks and insurance providers in North America, the UK, and continental Europe to define compliance strategy in response to regulatory and government mandates and ongoing changes in the financial services ecosystem.

Gregory Ross

Gregory is a Senior Manager in Accenture's Finance & Risk practice, with responsibility for the Fraud Management Consulting area. Gregory brings his experience and knowledge in the areas of resiliency, regulatory & compliance, and operational risk management processes and technology solutions to help financial services organizations strategize and deliver robust and streamlined risk management capabilities. He also has deep experience driving strategy design and implementing risk management functions, as well as executing key risk management processes at-scale. Gregory also has significant experience organizing and running large-scale, regulatory-driven enhancement programs.

Acknowledgment

The authors would like to thank the following Accenture employees for their important contribution to this document:

Philippe Guiral

Michael Sinitiere

Suzanne Carlson

Brendan Taylor

Justin Burul

REFERENCES

1 "Driving the Future of Payments – 10 Mega Trends," Accenture 2017. Access at: https://www.accenture.com/t20171012T092409Z__w__/us-en/_acnmedia/PDF-62/Accenture-Driving-the-Future-of-Payments-10-Mega-Trends.pdf

2 AML-based crimes include: Illegal weapons trafficking, human trafficking, cultural property trafficking, illegal wildlife trafficking, illegal fishing, illegal logging, illegal mining, crude oil theft, and counterfeit goods. Sources: "Transnational Crime and the Developing World," Global Financial Integrity, March 27, 2017. Access at: http://www.gfintegrity.org/report/transnational-crime-and-the-developing-world/. "Trade in Counterfeit and Pirated Goods," OECD, 2016. Access at: https://www.oecd-ilibrary.org/governance/trade-in-counterfeit-and-pirated-goods_9789264252653-en.

Fraud-based crimes include: Bank deposit fraud, first party fraud, mortgage fraud, wire fraud, account takeover fraud, check fraud, identity fraud, auto fraud, online retail fraud, credit and debit card fraud. Estimate is based upon an Accenture analysis of publicly available documents.

Cyber-based crimes estimate sources: "Cybercrime 'pandemic' may have cost the world $600 billion last year," CNBC, February 22, 2018. Access at: https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html. "Cybercrime Damages $6 Trillion by 2021," Cybersecurity Ventures, October 16, 2017. Access at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Illegal drugs estimate source: "Transnational Crime and the Developing World," Global Financial Integrity, March 27, 2017. Access at: http://www.gfintegrity.org/report/transnational-crime-and-the-developing-world/.

3 "Driving the Future of Payments – 10 Mega Trends," Accenture 2017. Access at: https://www.accenture.com/t20171012T092409Z__w__/us-en/_acnmedia/PDF-62/Accenture-Driving-the-Future-of-Payments-10-Mega-Trends.pdf

4 "Being digital – Digital strategy execution drives a new era of banking," Accenture, 2015. Access at: https://www.accenture.com/t20150721T131239Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_18/Accenture-New-Era-Banking-Strategy.pdfla=en. Digital transformers are organizations which expect complete or significant transformation of their industry.

STAY CONNECTED

Accenture Finance and Risk
www.accenture.com/us-en/financial-services-finance-risk

Finance and Risk Blog
financeandriskblog.accenture.com/

Connect With Us
www.linkedin.com/showcase/16183502/

Follow Us
www.twitter.com/Accenture FSRisk

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 442,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is **www.accenture.com**.

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

180964