Fighting organised crime in an organised way

How can your strategy to combat fraud while achieving regulatory compliance be more central to your long-term business strategy?

An alternative point of view.

Achieve a competitive advantage through strategic business defence

pwc

BAE SYSTEMS
INSPIRED WORK

How we see it

In a world where people, money and information move around the globe faster than ever before, financial services organisations need to be both more secure and more open. They face the twin challenges of meeting increasing regulatory requirements and counteracting the proliferation of more innovative financial crime – all the while striving to increase efficiency, minimise costs and improve the client experience to drive the bottom line.

The need to defend the institution, while fulfilling shareholder demands to deliver economic returns requires more than just a security system – it calls for something active, not passive.

To have an effective strategy to combat fraud and cybercrime, and achieve regulatory compliance over the long term, financial institutions need an enterprise-wide financial crime platform across all product lines with real-time data feeds, regardless of how many systems are currently in place.

To achieve these often conflicting outcomes, institutions need to take a broad strategic approach to combatting fraud and achieving regulatory compliance by making them central to their long-term business strategies.

The challenge

Over the years, we have seen financial institutions implement various solutions to combat fraud, cybercrime and regulatory compliance requirements. Typically, these have been deployed in an ad hoc manner, creating multiple isolated systems managing different aspects of risk and compliance. Having separate business units and products makes control and coordination more difficult.

Tactical responses like these have often been characterised by a lack of integration, between the core business systems of the enterprise and the compliance/fraud detection and prevention systems, further entrenching the silos that exist and increasing organisations' exposure to fraud.

Often, this has been due to different departments and divisions driving different strategies, and therefore applying different tactical solutions that may not always be to the benefit of the enterprise. A lack of consistency on defining financial crime within the organisation has also led to some institutions limiting it to compliance modules i.e. those imposed by the regulator, while others include the combatting of fraud within this definition.

The good news

It may seem counter-intuitive to place your vision to combat fraud and cybercrime, and achieving regulatory compliance, at the centre of your long-term business strategy, but if you consider what is required of a modern forward-looking institution to maintain a solid reputation with clients and stakeholders, the reasoning becomes clear.

To give clients and stakeholders the confidence that you are looking after their interests, you need to demonstrate that you are taking a robust, structured and coordinated approach, across all lines of service, including all product lines, regardless of how many systems are currently in place. This will give you a competitive advantage over your peers, while meeting stakeholder requirements.

Achieving the elusive 360-degree enterprise-wide view of risk, compliance, fraud, cybercrime and the internal audit landscape requires institutions to break with the existing paradigm that sees anti-money laundering (AML) and fraud investigation as different disciplines and which regards money launderers, fraudsters and cyber criminals as different types of operators. Among other benefits, breaking down traditional detection and investigation silos in this way leads to significant improvement in resource and capital efficiency.

Business defence

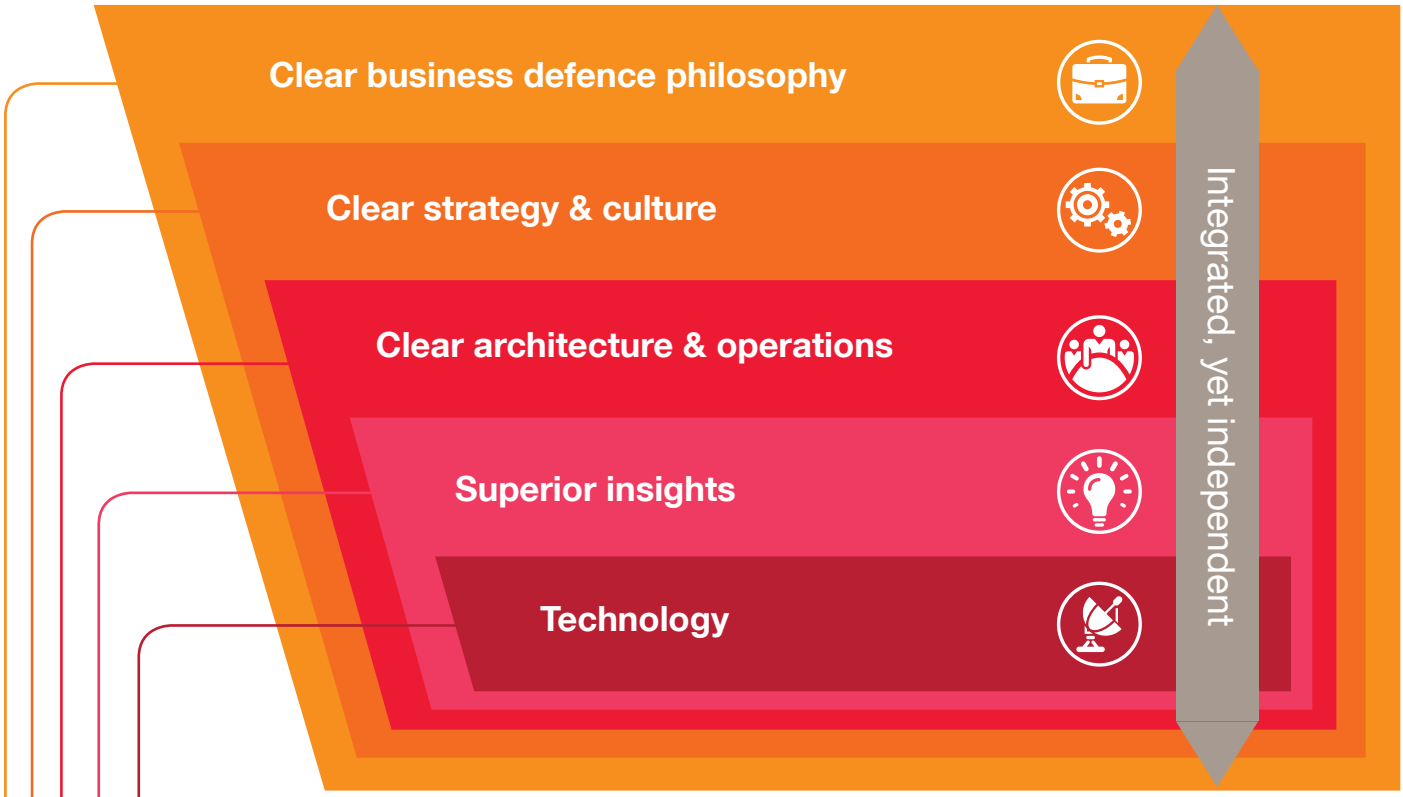
Mitigating risk and achieving regulatory compliance are conventionally seen as a cost of doing business. But what if this expense could actually deliver greater value to the organisation and increase customer experience? What if the existing mindset gave way to a progressive stance – proactive, not reactive; enabling, not limiting.

We think it can.

A business defence philosophy calls for institutions to adopt a single platform and culture across all lines of service and products to enable a predictive, responsive and intuitive machine-learning capability to deliver a 360-degree integrated view of the risk landscape, providing integrated dashboards and reporting across fraud and compliance.

Modern approach to business defence

Effective business defence starts in the boardroom with a clear enterprise-wide philosophy that holistically encompasses risk, compliance, fraud, cybercrime and the internal fraud landscape.



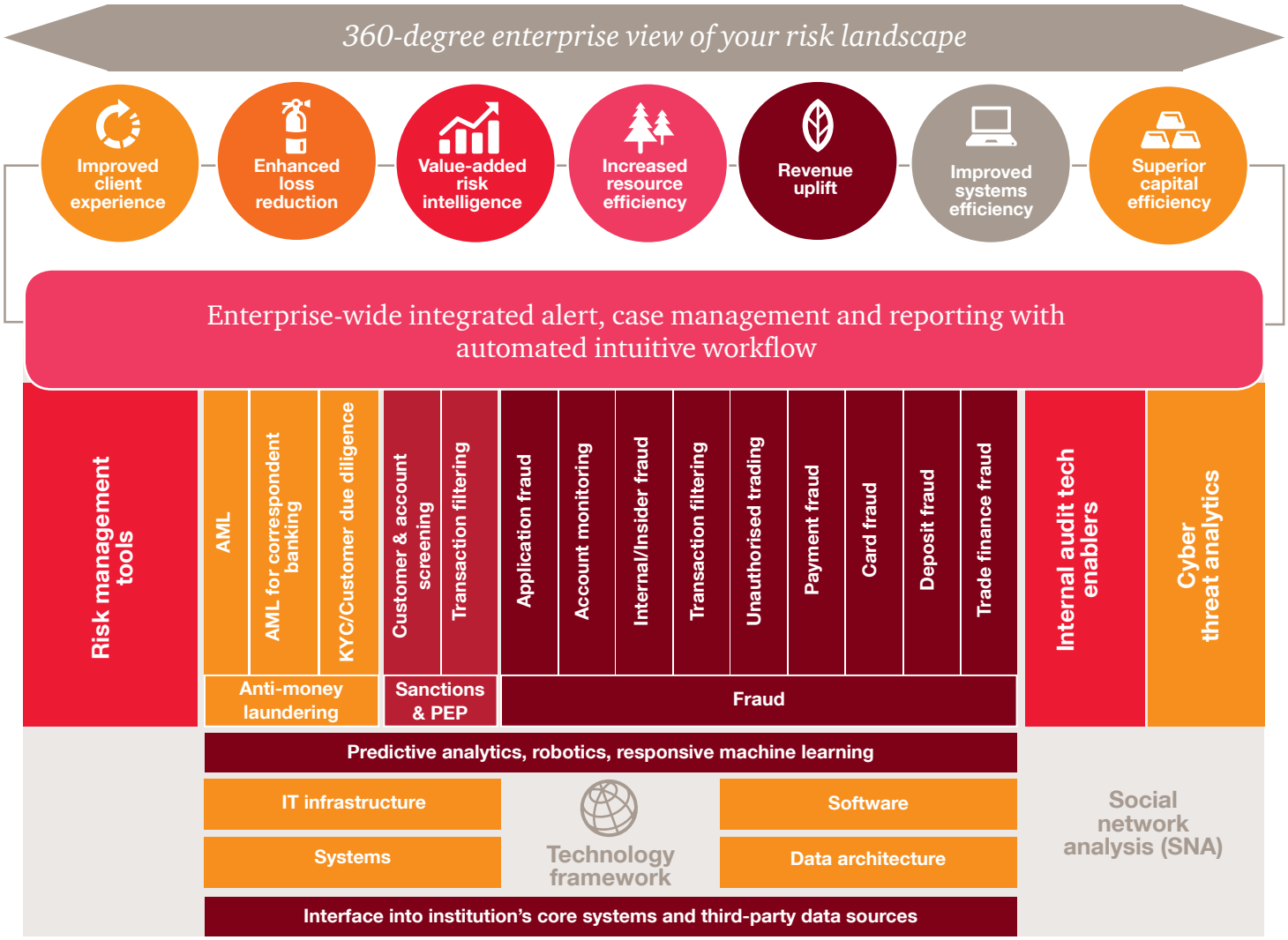
- Enterprise-wide view of risk, compliance, fraud, cyber and internal fraud landscape enabled through integrated dashboards and reporting, common case management and investigation tools. Requires a clear, proactive philosophy to counteract fraud.
- To comply with the regulator and combat fraud across all lines of service including product lines, regardless of how many systems are currently in place through defending the institution while fulfilling shareholder demands. Requires a clear strategy and cultural approach.
- Agile, future-proof environment for the holistic management of risk across the enterprise enabled by platform stability, accuracy of detection, low false positive rates, lower total cost of ownership and greater performance.
- Single version of the truth with regard to client data across the enterprise enabling integrated dashboards and reporting across fraud and compliance resulting in predictive, responsive and machine learning capability to build more accurate risk profiling of clients, more accurate pricing of clients including forward looking detection models.
- Deploy enterprise platform that delivers advanced capabilities to address/enable organisational and environmental factors through future-proof detection capability, scalability to absorb exponential increases in transaction volume and leverage current and future technology innovation to enable institutions to proactively address the dynamic regulatory and business environment in which they operate and innovate.

Enterprise-wide view of your risk landscape

The challenge is to coordinate the various risk and control functions effectively and efficiently to limit gaps and not create the environment for unnecessary duplications of coverage of the lines of defence, e.g. operational management, risk and compliance functions, and internal audit. A common platform and shared processes that align enterprise efforts and creates agility, consistency and efficiency will facilitate a transparent and risk-enabled decision making process across the lines of defence.

It will reduce duplication and do away with silos, allowing companies to allocate resources to highest risk areas, enhancing the overall outputs of the compliance functions while delivering higher quality information across the business.

An integrated technology platform does not infer changes to the Institution's operating model and levels of autonomy between, for example, compliance- and fraud-focussed teams. It will follow an integrated yet independent approach.



Evolving from reactive to proactive

Ultimately, to combat fraud and cybercrime, and achieve regulatory compliance effectively while ensuring that your organisation is agile enough to respond to stakeholder demands, you will need clean and/or connected data for the organisation, housed in a single repository. This will provide a single version of the truth with regard to client data across the enterprise, enabling integrated dashboards and reporting across fraud and compliance functions.

More importantly, it must facilitate the introduction of a predictive, responsive and intuitive machine-learning capability to provide forward-looking detection models. These advances will also enable the organisation to build more accurate client risk profiles, resulting in greater pricing accuracy and driving more efficient client relationship management.

This strategic approach takes a long-term view of the enterprise, but we believe it will enable institutions to achieve competitive advantage from their financial crime investment and create an agile, future-proof environment for the holistic management of risk, fraud and client relationships across the organisation.

Business defence capabilities

By providing clarity of purpose at every level, this approach cuts through the complexity that the proliferation of financial crime and risk management solution vendors can create.

There is a set of foundation-level capabilities that most of these vendors can provide, which address basic regulatory, business and functional requirements and generally satisfy a set of entry-level demands that institutions require to remain compliant and address financial crime losses.

These basic capabilities are necessary, but they are not sufficient to allow institutions to either extract competitive advantage from their financial crime investment or to create an agile, future-proof environment for the holistic management of risk across the enterprise.

To achieve true business defence, we believe institutions need to deploy technologies that exhibit advanced detection and prevention capabilities, while simultaneously addressing organisational and environmental factors that influence the commission of, and ultimately combatting of various forms of financial crime.

The journey to defence

The effectiveness of regulatory technologies has until now been undermined by the after-the-fact nature of their deployment into an institution's business and technology landscape. This has been driven by rapidly-changing regulatory and compliance frameworks and the global proliferation of technology-enabled financial crime.

This has led to a lack of integration, not only between the core business systems of the enterprise and the compliance and fraud departments, but also between the respective compliance and fraud systems.

Today, we see institutions possessing multiple systems ostensibly addressing the same basic problem: the reduction of risk-related losses and the adherence to regulatory requirements.

It doesn't need to be this way.

Institutions are increasingly looking for strategic and long-term partners that have the appropriate technology as well as functional and technical ability to provide the most appropriate solutions for their operations.

PwC and BAE Systems have made the long-term commitment and strategic vision – coupled with the technology, functional and technical capabilities – to provide the most appropriate integrated enterprise-wide risk management, compliance and fraud solutions.

The technological foundation of our approach is a business defence platform, a risk, fraud and compliance solutions suite that is used across the world by major banks and insurers, governments and law-enforcement agencies to provide intelligence and combat criminal threats.

PwC Africa-BAE Systems

PwC Africa and BAE Systems have entered into an alliance offering financial crime solutions to help financial institutions address the growing challenges they face on the continent.

BAE Systems is a global leader in fraud, regulatory compliance and cybercrime solutions and offers a portfolio of proprietary software products.

The alliance brings together the expertise of PwC in cyber, fraud and regulatory consulting and the long heritage BAE Systems' has in providing major global banking and insurance customers with leading fraud, regulatory compliance and cybercrime solutions.

The product and service offering is based on the proven BAE System's NetReveal® financial crime and compliance solutions suite, which targets fraud and helps ensure regulatory compliance, while supporting an integrated, enterprise-wide view of financial crime risk management.

NetReveal® provides a truly enterprise-wide platform to fight financial crime across the broad spectrum of fraud and compliance.

Delivery and support capabilities for NetReveal® have been jointly developed by BAE Systems and a PwC EMEA implementation team based in Johannesburg.

The team has the ability to support EMEA territories with rapid and comprehensive access to a proven enterprise-wide business defence tools, support mechanisms and expertise.

This means that, regardless of their location, financial institutions in EMEA can now rapidly and comprehensively target financial crime and meet regulatory requirements.

Let's talk

We believe your strategy to combat fraud, cyber risks and achieve regulatory compliance should be central to your overall long-term business strategy.

If you're looking for strategic, long-term partners that have the expertise supported by the appropriate technology as well as functional and technical ability to provide the most appropriate integrated enterprise-wide risk management, compliance, fraud and cybercrime solution suite for your business, let's talk. We look forward to the opportunity to explore the concepts discussed here with you and discuss your needs.

Contacts

Ricardo Rosa

Consulting Leader Africa
Office: +27 (11) 797 5602
Mobile: +27 (0)82 490 6081
ricardo.rosa@pwc.com

Leo Holesgrove

Business Defence Leader
Office: +27 (11) 797 4676
Mobile: +27 (0) 833938795
leo.holesgrove@pwc.com