Deloitte.

Proudly sponsored by

IBM

Smarter counter fraud

Financial Crime Strategy Roadshow

See it first. See it through.

Know the worth of risk.

www.deloitte.com/au/financial-crime

Contents

Message from Tim Phillipps

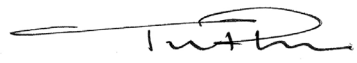
I am pleased to present the polling and breakout session responses from our recent financial crime strategy events held in Singapore, Jakarta, Hong Kong and Sydney.

These events brought together senior decision makers within the risk, compliance and legal functions where discussion focused on the barriers, drivers, risks and analytics factors involved in creating a holistic and effective financial crime strategy.

The following responses clearly indicate that financial crime is not just an event – a thing that happens. It's a constant pressure – a risk that's present at different stages in every part of financial services and corporate organizations.

Corporations need an enterprise-wide, integrated risk management strategy that accounts for the entire lifecycle – compliance, prevention, detection, investigation, remediation, monitoring, and testing. It is clear that a siloed, minimal approach will no longer cut it.

I hope you find the below responses useful in formulating your financial crime strategy. Please do reach out to my team if you would like to discuss this further.



Tim Phillipps
Global Leader - Deloitte Analytics
Global Leader - Deloitte Forensic

Event overview

In March 2014, Deloitte held Financial Crime Strategy conferences in Singapore, Jakarta and Hong Kong. This was followed by the first of the Australian events held in Sydney during May 2014. Delegates listened to presentations and were asked polling questions throughout the day before attending interactive 'breakout' sessions after lunch.

The breakout sessions were based on the Deloitte Greenhouse client experience - structured sessions which bring participants together in a state of the art space to build consensus and confidence with clear and actionable outcomes, achieving in a matter of hours what might otherwise have taken months.

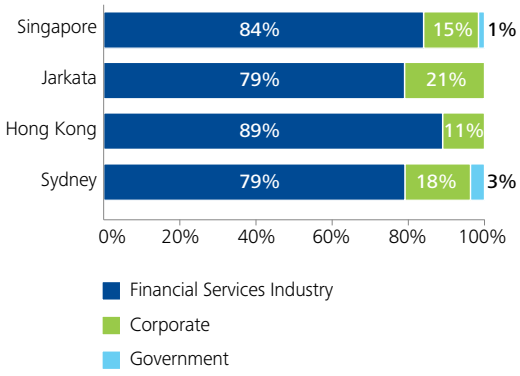
Delegates spent 15 minutes with four sets of facilitators. Discussion was focused on key financial crime strategy themes – barriers, drivers, risks and analytics. The objective of the sessions was to allow participants to share their view on the main issues they are encountering in financial crime. The below *Wordle* highlights the key themes discussed at the Sydney event.

Deloitte Greenhouse™

I really appreciated the afternoon sessions as they offered a good platform for an in-depth peer exchange. Thank you very much for this wonderful event.

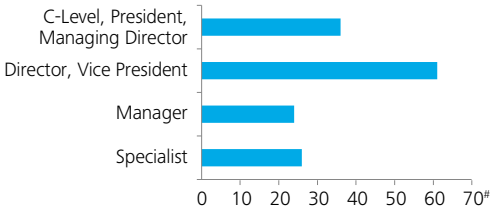
Marc Lorenz
Commerzbank AG

Delegate Industry

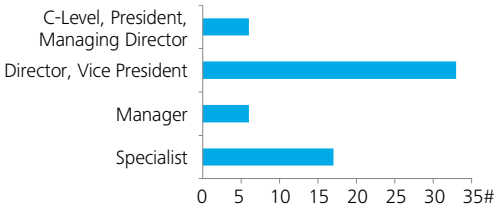


Delegate Level

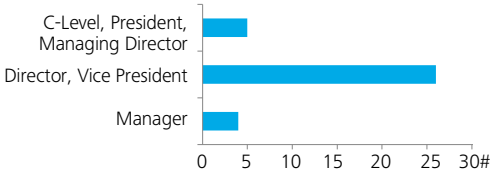
Singapore



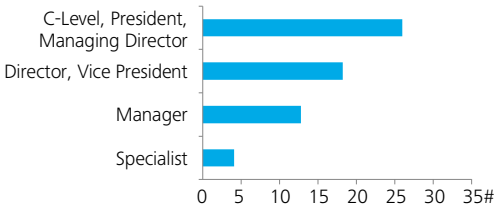
Jakarta



Hong Kong



Sydney



Key Observations:

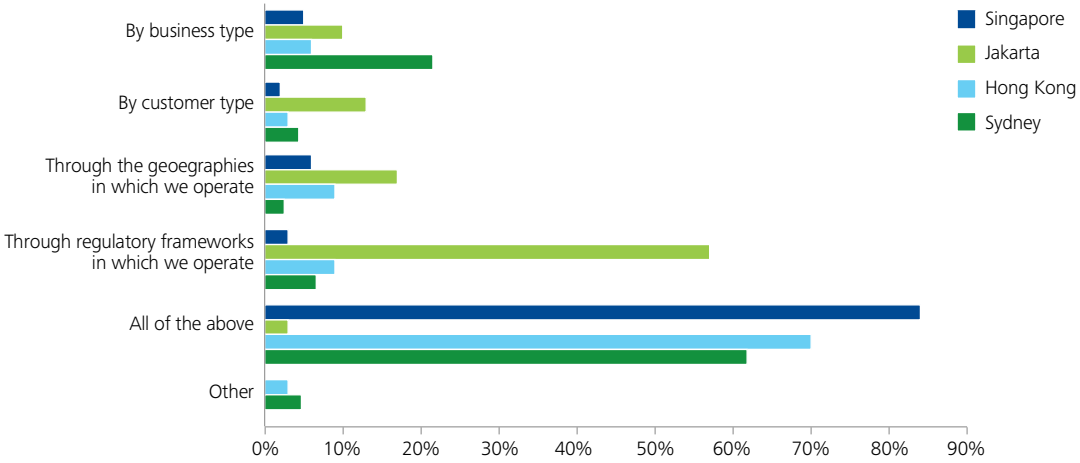
Delegates clearly recognized the need to deal with financial crime holistically and identified the following issues as critical to their financial crime strategy formulation:

- The cost – both financial and reputation – of non-compliance is increasing
- A holistic change management process is an important factor in an effective financial crime strategy
- With ever increasing and more complex threats, financial crime benchmarking should be comprehensive and conducted regularly
- There are increasing regulatory requirements from local, regional and global stakeholders
- There is an increasing need for an analytical understanding of financial crime
- The complexity of implementation and on-going management of financial crime analysis and reporting is becoming a major issue for organizations
- Technology is key in highlighting potential areas of risk and allow them to be more focused or targeted in their efforts to combat financial crime
- Organizations' financial crime approaches are constantly changing and evolving to deal with new issues

The current climate

The events began with the Chairman noting that financial crime is a well-known and widespread problem that impacts brand value and reputation, goodwill, and revenue of many organizations. Achieving greater effectiveness and efficiency by a unified approach across the spectrum of financial crime is the natural progression when it comes to understanding high risk products, geographies and customers.

How do you characterise your risk exposure to financial crime?



The majority of respondents categorize their financial crime risk exposure through a variety of means. Interestingly, Jakarta delegates characterized risk through regulatory frameworks at a much higher rate than their Singapore, Hong Kong and Sydney counterparts.

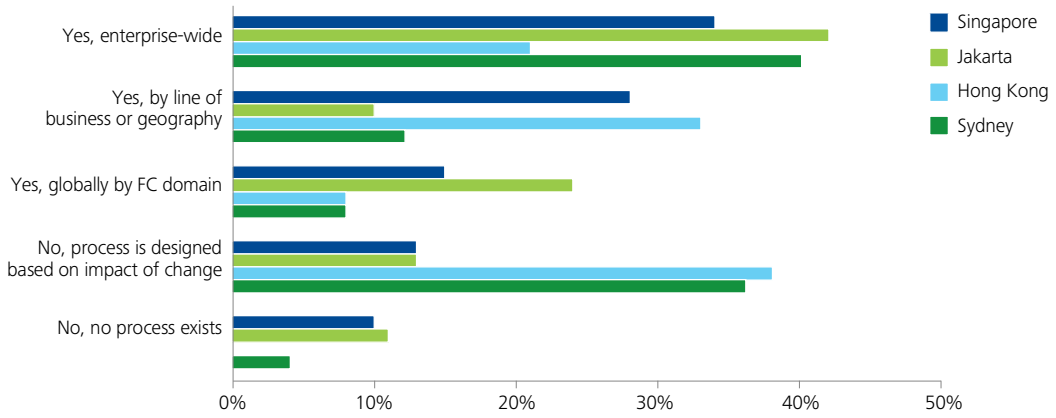
Takeaway: Financial crime risk identification is complex and varied. It is often allocated to 'siloes ' and can fall through categorization 'gaps'.

A lack of effective change management has resulted in missed products and revenue for my business.

I'm facing an inability to accurately migrate my business's systems.

The large financial penalties are a real concern for my organisation.

Do you have a process to adapt your financial crime strategy for changes in regulatory requirements and expectations?



Results across the four locations were varied. While large numbers of Singapore and Hong Kong delegates identified a line of business or geographic response to financial crime strategy adaptation, a significant amount of Jakarta (42%) and Sydney (40%) respondents concluded that an enterprise-wide process already existed in their organization.

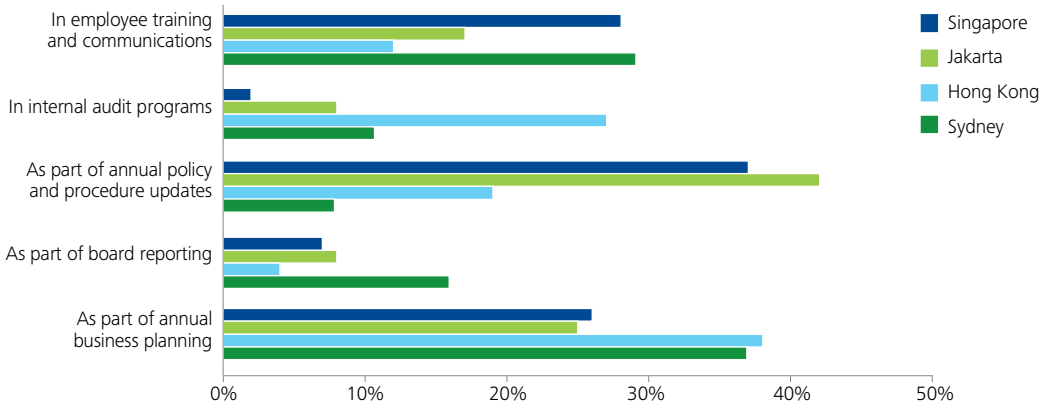
Takeaway: A holistic change management process is an important factor in an effective financial crime strategy.

Not having the correct infrastructure for upcoming and constantly changing legislation, such as FATCA, is a concern.

I'm facing increased risks to revenue associated from legacy business retention.

Failure to prevent or detect issues is often not because the programs or controls themselves are lacking. More often, it's a failure of culture and a lack of effective change management. The infrastructure to prevent financial crime may be sound, but its effectiveness still depends on execution, on individuals doing the right thing at the right time — culture is what enables and drives those appropriate behaviours.

At what point in time do you consider current financial crime events and threats impacting your peer institutions?



Singapore and Jakarta respondents were broadly aligned when assessing financial crime events and threats noting that it usually occurred during business planning or as part of the annual policy and procedure update. Interestingly, Hong Kong and Sydney delegates noted that they considered these threats during internal audit programs in conjunction with the annual business planning process.

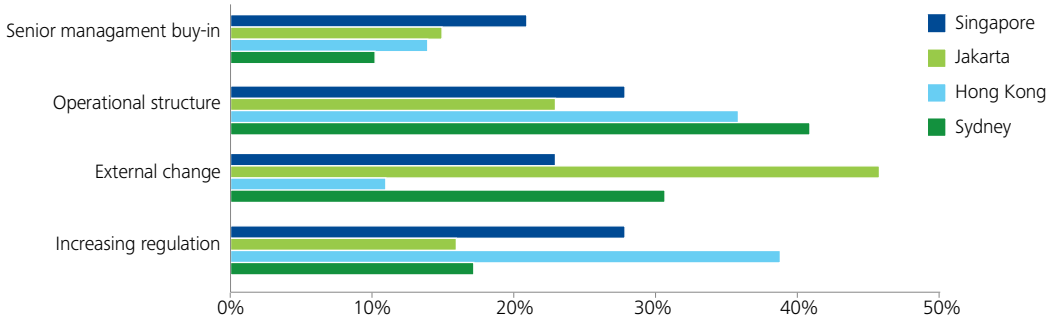
Takeaway: With ever increasing and more complex threats, financial crime benchmarking should be comprehensive and conducted regularly.

The number and complexity of new channels is increasing transactional anonymity.

I have a misalignment between staff expertise and financial crime strategy objectives.

The business's local, regional and global strategies are all key drivers.

In the context of financial crime, which of the following challenges do you consider to be your greatest?



Singapore and Hong Kong respondents both agreed that increasing regulation and their organization's operational structure posed the greatest financial crime challenge. While Nearly half of Jakarta delegates noted that their greatest challenge is related to external change such as economic, geopolitical and market drivers, Sydney delegates noted that their primary challenge is related to organizational structure.

Takeaway: Financial crime teams experience a variety of challenges with the organization's operational structure being a major factor, despite the general support of senior management for an improved approach to financial crime.

My business is not aligning with the geo-political landscape.

The current value proposition is too focused on immediate dollar savings.

I'm concerned with the emergence and influence of virtual currencies.

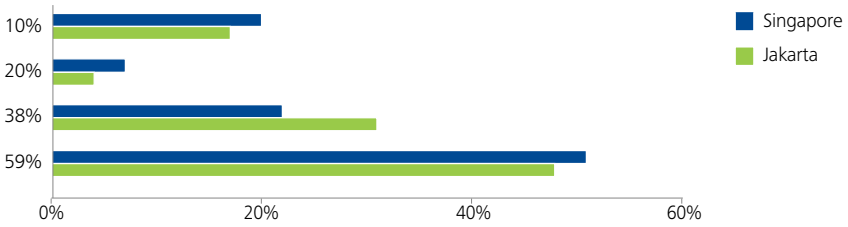
The lack of an effective change management program leaves both staff and leadership unaware of requirements.

Regulatory environment

In Singapore and Jakarta, Thomas Benedict from White & Case discussed the regulatory environment and asked the audience two questions to underline the increasing financial penalties associated with financial crime. Stewart McGlynn, from the Hong Kong Monetary Authority, noted that it is critical that organizations understand and manage financial crime risk. In Sydney, with the Deloitte Australia panel shared their experiences across the insurance, wealth management, energy and resources and banking sectors.

The financial penalties faced by corporations from actions such as internal investigations, fines, class action lawsuits and other litigation are climbing. Reputations and market standing are being damaged, or worse, lost.

In a 2013 fraud survey regarding corporations operating in the Asia-Pacific region, what percentage of Singapore corporate respondents admitted that their anti-bribery policy, while good in principle, does not work well in practice?



Half of the delegates were correct in identifying that 59% of the 2013 survey respondents admitted that their anti-bribery policy did not work well in practice.

Takeaway: There is a significant divergence between financial crime strategy, policy and practice.

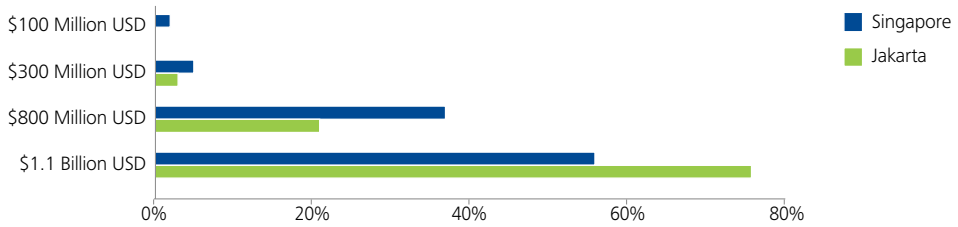
The risk to my firm's reputation is my number one concern.

I'm facing fast-moving customer demand and a similar moving regulatory environment.

There is increasing regulatory pressure on the financial services industry.

My business is not harmonizing with local and international regulations.

In February 2014, the WSJ reported that a French bank had set aside the following sum as a reserve for an expected OFAC penalty related to transactions involving Iran, Cuba and Libya?



The majority of delegates identified that $1.1 Billion USD was put aside as an OFAC penalty reserve.

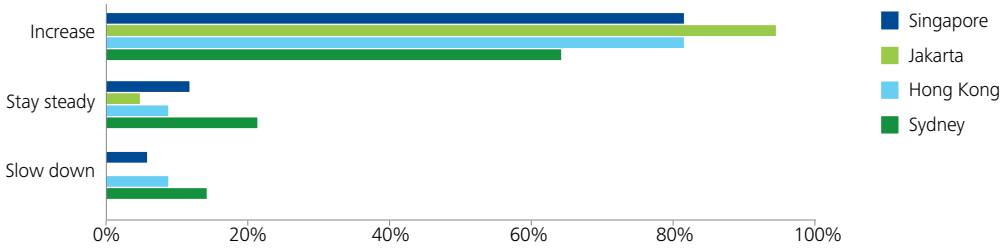
Takeaway: An ineffective financial crime strategy can have expensive consequences.

The cost of non-compliance is my major motivator.

I'm concerned that increasingly sophisticated criminals will target my organization.

I'm finding it difficult to get first-line and senior leaders ownership of financial crime risks.

In the next 5 years, will the pace and scale of regulatory change in Asia…



The vast majority of delegates across the four locations agreed that regulatory change will increase in Asia in the coming five years.

Interestingly, not one delegate in Jakarta believed that regulatory change will reduce in the coming years.

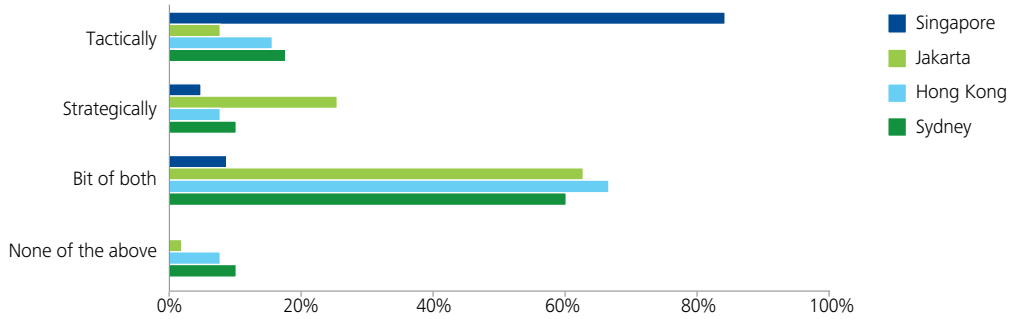
Takeaway: The regulatory network for organizations is likely to get more complicated in the years ahead indicating that an effective and adaptable change management process will be required.

The pace of regulatory change, scrutiny and expectation is a real risk to my financial crime strategy.

The frequency of regulatory change and enforcement is driving my financial crime program.

I need to understand the prevalence of specific financial crime such as tax avoidance.

Currently, how are your organizations addressing regulatory change?



Not surprisingly, the majority of respondents noted that their organization addressed regulatory change in both a tactical and strategic manner. Jakarta organizations appear to possess more of a calculated approach with 26% of respondents advising that they respond strategically.

Takeaway: Organizations are acting at each event and are not taking advantage of a strategic financial crime view.

I want to understand the potential financial cost impact on individual products.

I need to 'join the dots' between various organizational programs.

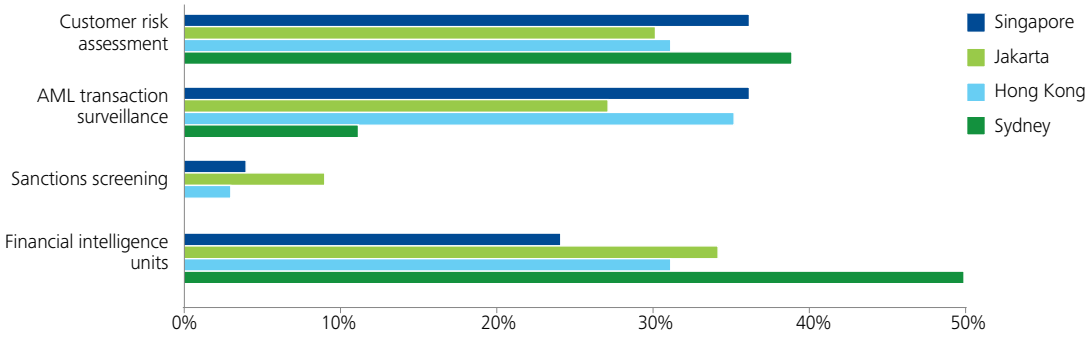
I need to identify potential resources, process and technology synergies.

Hyper-connectivity between customers and organisations is increasing.

Adding analytical value

In Singapore, Jakarta and Hong Kong Tom Scampion, Deloitte LLP, suggested that analytics was the answer to the question of how to deal with financial crime risk. In Sydney, Anthony Viel of Deloitte Australia noted that organizations will need to build technology platforms that can grow with their data and analytical needs, choosing smart systems that can adapt to evolving patterns and data sources. Overall, the emphasis today is on prevention and/or early detection; leveraging technology and analytics to proactively identify issues or potential issues before they turn into front-page news.

How do you see analytics adding value to your organization's financial crime strategy?



Delegates in all locations agreed that analytics would add value in CRA's, AML transaction surveillance and financial intelligence unit management.

Takeaway: Effective analytics can add value across the entire financial crime lifecycle.

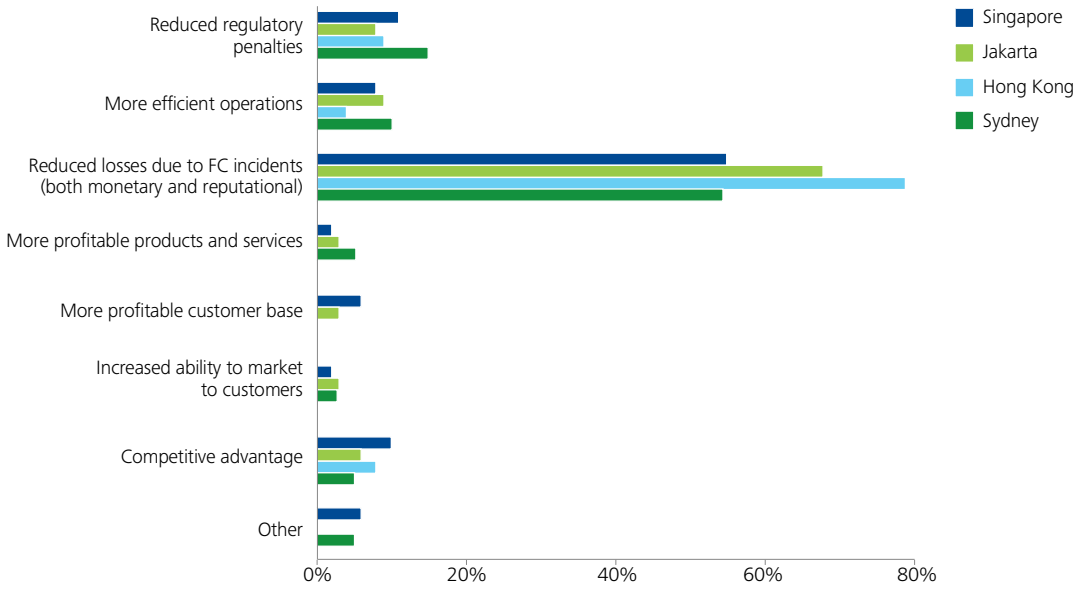
I want it to be able to model new behaviours based on historic analysis.

I want to use analytics to justify my financial crime strategy approach.

I want to reduce investigative times by focusing on target samples or risk areas.

I need a "flight plan" that includes the ability to predict, prevent, detect and report financial crime.

How does your financial program create value for your organization?



More than half of respondents in each location noted that their financial crime program creates the most value in reducing monetary and reputation losses. Eight out of ten Hong Kong respondents agreed that this was a key value creator.

Takeaway: An effective financial crime strategy delivers value across a range of areas but organizations are yet to harness the profitability or know your customer benefits.

My organisation requires a broader perspective on how data can be useful.

I need to use analytics as a tool to deliver strategy.

Does my organization collect right data? Am I asking the right questions?

I want an ability to define 'business as normal'.

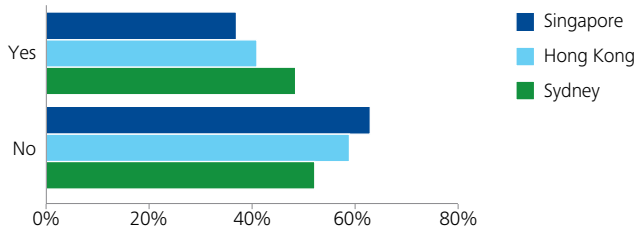
My business needs data for both transactional and analytical purposes.

Organizational structure

A fragmented approach isn't enough and neither is a purely reactive one. Matt Bailey, Deloitte Consulting, took to the Singapore, Jakarta and Hong Kong stages to note that compliance-based approaches addressing particular risks in a siloed or piecemeal fashion are giving way to holistic approaches that look at many types of financial crime risk across the organization. In Sydney, Maickel Sweekhorst and Arturo Mauleon, Deloitte Consulting, discussed the importance of an integrated target operating model that can be refined to fit the organisation.

In Singapore and Hong Kong, Bill Donellan, i2 Executive at IBM, suggested that technology tools can give organizations a more holistic view of their data, highlight potential areas of risk and allow them to be more focused or targeted in their efforts to combat financial crime. In Sydney, Bob Griffin, CEO of i2 and and Vice-President of IBM, noted technology is critical in handling the management and investigation of the origin and cause of the cyber incident.

Has your organization begun an Operational Convergence Program to integrate Fraud and Financial Crimes Operational Groups?



Two thirds of Singapore and Hong Kong respondents and over half of Sydney attendees noted that their organization had yet to begin an operational convergence program to integrate their fraud and financial crime groups despite identifying that operating structure was a barrier to achieving an holistic financial crime approach. Many organizations have not yet taken the operational convergence steps to rectify the gap between fraud and financial crime operational groups.

Takeaway: There may be a gap in many organizations' fraud and financial crime operational groups.

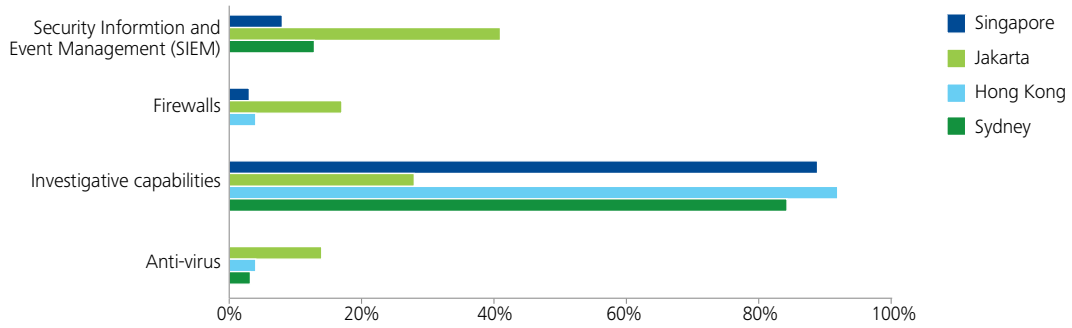
I have ever-changing centralized vs decentralized operating models.

The cost for the right technology and its implementation are significant barriers for my organization.

I have early adopter anxiety where an initiative has never been sanctioned previously.

The lack of a stable IT system raises the risks of my business being a victim of financial crime.

Traditional security offerings address only part of the solution needed for an organization's cyber planning. Which offering is not a classic cyber security offering?



Eight out of ten Singapore, Hong Kong and Sydney respondents identified that investigative capabilities is not a traditional cyber security offering whereas Jakarta responses were varied.

Takeaway: With cybercrime becoming a growing threat, organizations need to adapt their financial crime strategy to include investigative capabilities.

I have conflicting agendas between business and compliance requirements.

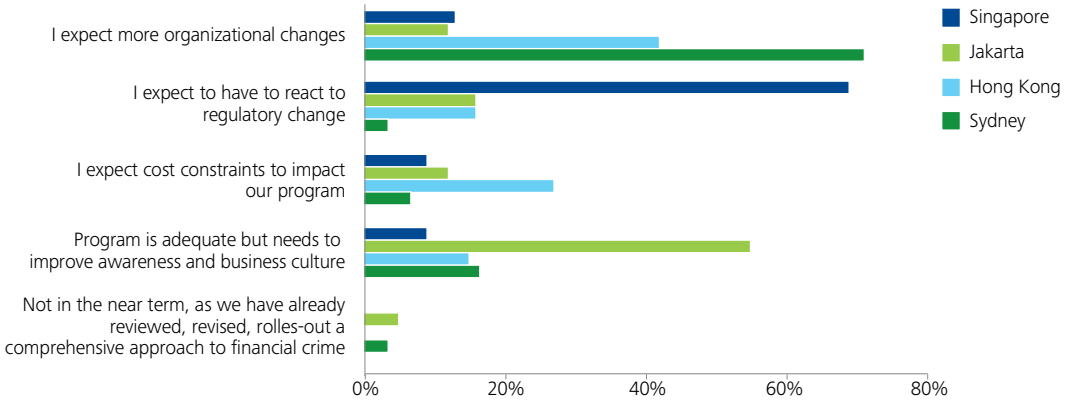
My business has competing priorities for systems / processes / policies and procedures.

How do you get buy-in from every organizational layer?

Looking ahead

In closing the plenary sessions, Chairman noted that it is crucial to implement an integrated approach which enables firms to seek out additional synergies between financial crime intelligence and customer intelligence, thereby creating opportunities to improve customer service and add more business value.

For the next 2 years, is your approach to financial crime stable or evolving?



The vast majority of Sydney delegates expect more organisational changes in the next 24 months while Singapore and Hong Kong delegates also expect regulatory change. Some Jakarta delegates expect their financial crime approach to evolve while the majority believe that their strategy is adequate.

Takeaway: Organizations' financial crime approaches are constantly changing and evolving to deal with new issues yet some resources are slow to evolve.

Data privacy matters are a significant issue for my organization.

I have a lack of senior management support.

Keeping hold of talent – both the quality and quantity – is a real barrier for my business.

Contact us

APAC Financial Crime Leadership Team

Deloitte Singapore

Tim Phillipps
Global Leader, Forensic & Analytics
Singapore and Southeast Asia
+65 6531 5034
tphillipps@deloitte.com

Radish Singh
Partner, Financial Advisory
Singapore and Southeast Asia
+65 6224 8288
radishsingh@deloitte.com

Deloitte Hong Kong

Ivan Zasarsky
Partner, Financial Advisory
Hong Kong
+852 2852 1600
izasarsky@deloitte.com.cn

Chris Fung Yu Cheung
Partner, Financial Advisory
Hong Kong
+852 2238 7205
chrcheung@deloitte.com.hk

Deloitte Australia

Chris Linde
Partner, Risk Advisory
Australia
+61 3 9671 8494
clinde@deloitte.com.au

Lisa Dobbin
Partner, Risk Advisory
Australia
+61 2 9322 3709
ldobbin@deloitte.com.au

Financial Crime.
See it first. See it through.

Bribery, fraud, and cybercrime keep getting more sophisticated. Regulatory agencies demand more accountability. And as business embraces globalization, it encounters nuanced new cultural and legal challenges. A fragmented approach isn't enough. Neither is a purely reactive one.

Financial crime is a constant threat across the entire organizational lifecycle. It risks your organization's money and reputation in more than one way.

Deloitte has the vision, reach, and capability to help you understand, anticipate, and mitigate that threat - in addition to reacting when crimes occur.

Contact our APAC financial crime leadership team to discuss how Deloitte can partner with your organization to address this challenge in a holistic, effective way.

Deloitte.