Financial Crime Strategy Roadshow
Australia
See it first. See it through.

Know the worth of risk.
www.deloitte.com/au/financial-crime
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message from Ivan Zasarsky</td>
<td>3</td>
</tr>
<tr>
<td>Event overview</td>
<td>4</td>
</tr>
<tr>
<td>The current climate</td>
<td>6</td>
</tr>
<tr>
<td>Industry Panels</td>
<td>10</td>
</tr>
<tr>
<td>Adding analytical value</td>
<td>14</td>
</tr>
<tr>
<td>Organisational structure</td>
<td>16</td>
</tr>
<tr>
<td>Looking ahead</td>
<td>18</td>
</tr>
<tr>
<td>Contact us</td>
<td>19</td>
</tr>
</tbody>
</table>
I am pleased to present the polling responses from our recent financial crime strategy events held in Sydney, Melbourne and Brisbane.

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 is present at different stages in every part of financial services and corporate organisations.

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.

Ivan Zasarsky
Financial Crime Lead
Partner Deloitte, Australia
During May to September 2014, Deloitte held Financial Crime Strategy conferences in Sydney, Melbourne and Brisbane. These were proceeded by conferences held in Singapore, Jakarta and Hong Kong earlier in the year. Delegates were given an overview of the financial crime challenges they face, and the steps needed to successfully deal with those challenges. On the day, delegates listened to presentations and were asked polling questions throughout the day.

The event — chaired by Deloitte Australia’s Lead Financial Crime Partner, Ivan Zasarsky — brought together clients from a range of industries. There were presentations from a number of Deloitte and industry experts on the regulatory environment, industry trends, analytics, technology and strategy. The audience also listened to panel discussions from fraud, and anti-bribery and corruption experts, as well as Deloitte leaders from across Consulting, Risk Services, and Deloitte Analytics.

The panel sessions opened the floor to questions from the audience. This allowed participants to share their views on the main issues they are encountering in financial crime. The below Wordle highlights the key themes discussed at the events.

We are in the midst of an exciting AsOne initiative in Financial Crime spanning service lines and industry in Australia. It’s wonderful to share the success and energy created by the team, our speakers and participants. It is really terrific to see the level of collaboration from across the firm.

Ivan Zasarsky
Financial Crime Lead
Partner Deloitte, Australia
Key Observations:
Delegates clearly recognised 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 organisations
- 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
- Organisations’ financial crime approaches are constantly changing and evolving to deal with new issues
The current climate

The events began with the Ivan Zasarsky noting that financial crime is a well-known and widespread problem that impacts brand value and reputation, goodwill, and revenue of many organisations. 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 in all three cities categorise their financial crime risk exposure through a variety of means. Sydney, Melbourne and Brisbane delegates all agreed that their risk exposure is categorised by “All of the above”. Interestingly, Sydney delegates characterised risk by business type at a higher rate than its Melbourne and Brisbane counterparts.

**Takeaway:** Financial crime risk identification is complex and varied. It is often allocated to ‘siloes’ and can fall through categorisation ‘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.
The top tier results from all three locations were similar. Large numbers of delegates from Sydney, Melbourne and Brisbane concluded that an enterprise-wide process already existed in their organisation.

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

---

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

---

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

Sydney and Melbourne respondents were broadly aligned when assessing financial crime events and threats noting that it usually occurred during business planning or as part of employee training and communication. Interestingly, Brisbane delegates noted that they considered these threats during the internal audit 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.
Brisbane and Melbourne respondents both agreed that a lack of senior management buy-in posed a great financial crime challenge, while Sydney delegates noted that their greatest challenge is related to their organisation’s operational structure. While Melbourne and Brisbane respondents similarly think that increasing regulation is not a huge threat, Sydney respondents noted that increasing regulation is a challenge they face.

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

---

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

![Bar chart showing the distribution of responses from Brisbane, Melbourne, and Sydney respondents.]

Brisbane and Melbourne respondents both agreed that a lack of senior management buy-in posed a great financial crime challenge, while Sydney delegates noted that their greatest challenge is related to their organisation’s operational structure. While Melbourne and Brisbane respondents similarly think that increasing regulation is not a huge threat, Sydney respondents noted that increasing regulation is a challenge they face.

**Takeaway:** Financial crime teams experience a variety of challenges with the organisation’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.**

**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.**

**The current value proposition is too focused on immediate dollar savings.**
The audience listened to panel discussions from fraud, anti-bribery and corruption experts from Coles, Veda, IBM, Corrs, ASIC and the Australian Federal Police.

The fraud industry panelists identified data breaches as a particular issue at the moment - reference was made to a large US retailer which was a victim of a large credit card breach in 2013. Criminals and organised groups are learning how to effectively use technology to make their products more sophisticated. It was noted that the financial services industry in particular faces a daunting task to keep abreast of advances in technology.

The industry panels noted that credit card fraud is becoming increasingly common in the market. Fabricated identities - especially in those industries where electronic verification and online on-boarding is not as sophisticated as other industries - is on the rise. Panelists agreed that the upgrading of infrastructure including technology and intelligence is vital to combating new types of fraud.

Visa fraud - and increasing CV fraud - was also noted as a challenge facing businesses. Examples included student workers working more overtime than permitted and the hiring of friends in to organisations on inappropriate visas. Panelists referred to a number of recent high profile cases where employees have claimed to be members of organisations that either they do not belong to or that do not exist.

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 harmonising with local and international regulations.
The role of an organisation’s Board and their approach to dealing with bribery and corruption risk was discussed. Panelists noted that, in general, Boards within Australian owned companies – in particular those who have no overseas footprint – have a very small appetite for combating this type of risk. Organisations need to constantly assess and update their policies to ensure that specific anti-bribery and corruption policies in place rather than an overall Code of Conduct. While responsibility for bribery and corruption rests with everyone within the organisation, the C-suite must take responsibility for embedding a culture around prioritisation of this risk.

Panelists noted that the effects of allowing bribery and corruption to go undetected in a business is extremely damaging. The impact of not properly protecting a business can result in internal financial cost, shareholder class actions for a publicly listed company, and perhaps most importantly – reputational risk. Ultimately, bribery and corruption in an organisation can affect who you do business with in the future.

I’m concerned that increasingly sophisticated criminals will target my organisation.

The cost of non-compliance is my major motivator.

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

Takeaway: The regulatory network for organisations is likely to get more complicated in the years ahead indicating that an effective and adaptable change management process will be required.
Currently, how are your organisations addressing regulatory change?

Not surprisingly, the majority of respondents noted that their organisation addressed regulatory change in both a tactical and strategic manner. Brisbane organisations appear to possess more of a calculated approach with 32% of respondents advising that they respond strategically.

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

I need to ‘join the dots’ between various organisational programs.

Hyper-connectivity between customers and organisations is increasing.

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

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

In Sydney and Melbourne, Anthony Viel and Justin Guiliano from Deloitte suggested that analytics was the answer to the question of how to deal with financial crime risk. In Brisbane, Ian Blatchford noted that organisations 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 organisation’s financial crime strategy?

Delegates in all locations agreed that analytics would add value in CRA’s, 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 crime program create value for your organisation?

More than half of respondents in each location noted that their financial crime program creates the most value in reducing monetary and reputation losses.

**Takeaway:** An effective financial crime strategy delivers value across a range of areas but organisations 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 organisation collect right data? Am I asking the right questions?**
- **My business needs data for both transactional and analytical purposes.**

- Other
- Competitive advantage
- Increased ability to market to customers
- More profitable customer base
- More profitable products and services
- Reduced losses due to FC incidents (both monetary)
- More efficient operations
- Reduced regulatory penalties

<table>
<thead>
<tr>
<th>Location</th>
<th>Brisbane</th>
<th>Melbourne</th>
<th>Sydney</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced losses due to FC incidents (both monetary)</td>
<td>60%</td>
<td>65%</td>
<td>70%</td>
</tr>
<tr>
<td>More profitable products and services</td>
<td>50%</td>
<td>55%</td>
<td>60%</td>
</tr>
<tr>
<td>More efficient operations</td>
<td>45%</td>
<td>50%</td>
<td>55%</td>
</tr>
<tr>
<td>Increased ability to market to customers</td>
<td>40%</td>
<td>45%</td>
<td>50%</td>
</tr>
<tr>
<td>Competitive advantage</td>
<td>35%</td>
<td>40%</td>
<td>45%</td>
</tr>
<tr>
<td>Other</td>
<td>10%</td>
<td>15%</td>
<td>20%</td>
</tr>
</tbody>
</table>

0 10 20 30 40 50 60 70
Organisational structure

A fragmented approach isn’t enough and neither is a purely reactive one. Maickel Sweekhorst and Arturo Mauleon, Deloitte Consulting, took to the Sydney stage to discuss the importance of an integrated target operating model that can be refined to fit the organisation.

In Melbourne, Stephanie Hudson, Financial Solutions Lead at SAP, suggested that technology tools can give organisations 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 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 organisation begun an Operational Convergence Program to integrate Fraud and Financial Crimes Operational Groups?

Over half of Melbourne and Brisbane respondents and exactly half of Sydney attendees noted that their organisation 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 organisations 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 organisations’ fraud and financial crime operational groups.

I have ever-changing centralised vs decentralised operating models.

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

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 organisation’s cyber planning. Which offering is not a classic cyber security offering?

Almost all of the delegates in Sydney, Melbourne and Brisbane identified that investigative capabilities is not a traditional cyber security offering.

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

- I have conflicting agendas between business and compliance requirements.
- How do you get buy-in from every organisational layer?
- My business has competing priorities for systems/processes/policies and procedures.
Looking ahead

In closing the sessions, Ivan Zasarsky 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 delegates across the three locations expect more organisational changes in the next 24 months, while Brisbane delegates also note that their program is adequate but needs to improve awareness and business culture.

*Takeaway:* Organisations’ 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 organisation.

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 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

Deloitte Hong Kong

Ivan Zasarsky
Partner, Enterprise Risk Services
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
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 globalisation, 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 organisational lifecycle. It risks your organisation’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 organisation to address this challenge in a holistic, effective way.