



Australian Government

**Australian Transaction Reports
and Analysis Centre**

Suspicious matter reporting – Market Participants in the securities and derivatives sectors

AUSTRAC survey series – no. 2

November 2010



Disclaimer: The information contained in this document is intended only to provide a summary and general overview on these matters. It is not intended to be comprehensive. It does not constitute, nor should it be treated as, legal advice or opinions. This document may contain statements of policy which reflect AUSTRAC's administration of the legislation in carrying out its statutory functions. The Commonwealth accepts no liability for any loss suffered as a result of reliance on this publication. AUSTRAC recommends that independent professional advice be sought.

The information contained herein is current as at the date of this document.

November 2010

© **Commonwealth of Australia**

Australian Transaction Reports and Analysis Centre (AUSTRAC)
PO Box 5516
West Chatswood NSW 1515

Telephone: 1300 021 037

Facsimile: 02 9950 0071

Website: www.austrac.gov.au

Email: help_desk@austrac.gov.au

Table of contents

| | | |
|----------|---|-----------|
| 1 | Executive summary | 4 |
| 2 | Background, methodology and response | 6 |
| 2.1 | Background and rationale for the survey | 6 |
| 2.2 | Methodology and response | 6 |
| 3 | Risk awareness training programs for staff | 8 |
| 3.1 | Content | 8 |
| 3.2 | Delivery method | 10 |
| 3.3 | Useful resources for developing staff training programs | 11 |
| 4 | Transaction monitoring programs | 13 |
| 4.1 | Type | 13 |
| 4.2 | Ensuring effectiveness | 14 |
| 4.3 | Useful sources for developing transaction monitoring programs | 15 |
| 5 | Suspicious matters | 17 |
| 5.1 | Red flags/triggers | 17 |
| 5.2 | Insider trading and market manipulation | 20 |
| 5.3 | Incidence of identified matters | 21 |
| 5.4 | Diversity of business areas generating suspicious matters | 21 |
| 5.5 | Submission of SMRs to AUSTRAC | 23 |
| 6 | Organisational behaviour post-SMR generation | 24 |
| | Attachment A – AML/CTF Rules referenced in this report | 26 |
| | Attachment B – Item 33 designated service | 28 |
| | Attachment C – Survey of Market Participants | 29 |

1 Executive summary

All reporting entities under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) have obligations to report suspicious matters to AUSTRAC through the submission of suspicious matter reports (SMRs). These reports are a critical source of intelligence in combating serious criminal activity, including organised crime, terrorism financing and tax evasion.

In July 2010 AUSTRAC conducted a survey of reporting entities that are Market Participants¹ in the securities and derivatives sectors. The survey gathered information about how Market Participants have understood and addressed their SMR and related obligations under the AML/CTF Act. The survey included questions about staff training, transaction monitoring and enhanced customer due diligence (ECDD).

This report presents the results of the survey, including aggregated data and analysis. It is a snapshot of organisational capacity and readiness among Market Participants to identify matters that may be reportable to AUSTRAC as SMRs. There are 16 key findings and five areas of 'outlier behaviour' that warrant highlighting. Where the report states that a respondent exhibited 'outlier behaviour', this indicates that the respondent's behaviour diverged from that exhibited by their peers, and that they were yet to develop fully effective AML/CTF programs, systems or processes.

The report's findings will be directly relevant to Market Participants. The findings will also be of interest to the broader regulated population, compliance professionals, industry peak bodies, professional associations and academics.

| Area | Key findings |
|--|--|
| AML/CTF risk awareness training for staff | <ol style="list-style-type: none">1. Respondents covered a diverse range of significant content areas in their AML/CTF risk awareness training programs for staff. Of seven listed content areas, 70% of respondents covered six, or all seven, in their training programs.2. Almost all respondents included the following critical content areas in their staff training programs:<ul style="list-style-type: none">• circumstances that may trigger an obligation to submit an SMR to AUSTRAC (97% of respondents)• how to refer/escalate a potentially suspicious matter within their organisation (97%)• the money laundering or terrorism financing (ML/TF) risks individual staff are likely to face when interacting with customers in their role (90%)• the tipping-off offence in relation to SMRs (90%).<p>Outlier behaviour: Respondents that did not cover a wide range of significant content areas in their staff training programs.</p>3. Formal face-to-face training sessions (delivered by the organisation's staff) were the most common delivery method for risk awareness training programs (82% of respondents).4. Most respondents used a variety of delivery methods to round out their risk awareness training program. Of the 82% of respondents that delivered training via formal face-to- |

¹ Holders of an Australian Financial Services Licence admitted as a Market Participant by the Australian Securities Exchange and permitted to trade for clients. Market Participants that conduct trades for clients have obligations under the AML/CTF Act.

| | |
|--|---|
| | <p>face sessions (delivered by the organisation's staff), around two-thirds also used self-directed learning (e.g. using online information and tests) <i>and</i> on-the job training and mentoring.</p> |
| Transaction monitoring | <p>5. 62% of respondents monitored customer transactions through a combination of manual transaction monitoring conducted by staff and monitoring conducted by computer-based/automated systems.</p> <p>6. A third of respondents relied solely on staff to manually monitor customer transactions, and only 7% relied solely on computer-based/automated systems.</p> <p>7. Most respondents using a computer-based/automated system to monitor customer transactions ensured it was effective by testing triggers/rules (72% of respondents), reviewing triggers/rules (89%), monitoring the volume of alerts (89%) and assessing the quality of alerts (94%).</p> |
| Red flags/triggers for identifying potential suspicious matters | <p>8. 60% of respondents said their organisation would identify 13, or all 14, of the listed categories of potentially suspicious matters. This indicates a very high degree of organisational readiness to identify a diverse range of matters.</p> <p>Outlier behaviour: Respondents that believed their organisation would identify only nine, or even fewer, of the 14 listed categories of potentially suspicious matters.</p> <p>9. Almost all respondents believed their organisation would identify potentially suspicious matters related to doubts about a customer's identity and matters where a customer was located in or the transaction involved a foreign country of interest (e.g. a country that was subject to sanctions or was a tax haven).</p> <p>10. The majority of respondents believed their organisation would identify a range of potentially suspicious matters that would rely, at least to some extent, on staff interaction with a customer. This highlights the critical role played by staff and the importance of having effective staff training programs.</p> <p>Outlier behaviour: Respondents that believed their organisation would <i>not</i> be able to identify potentially suspicious matters relating to unexplained third party involvement in a transaction or where the customer had an unusual company or trust structure.</p> <p>11. Nine out of 10 respondents believe insider trading and market manipulation should either 'sometimes' or 'always' be reportable to AUSTRAC through an SMR.</p> |
| Identified potentially suspicious matters | <p>12. 61% of respondents had identified one or more potentially suspicious matters over a six-month period beginning 1 January 2010. These matters were raised via:</p> <ul style="list-style-type: none"> • front office staff (e.g. traders, advisers, sales staff) • other staff (e.g. back office staff) • computer-based/automated systems. <p>13. Potentially suspicious matters were generated by respondents across all four categories of organisational size, from organisations of less than 20 staff, to those with more than 500 staff.</p> <p>14. Three-quarters of the respondents that had identified potentially suspicious matters identified the matters using two of the three channels listed above.</p> <p>15. Almost a third of the respondents that had identified potentially suspicious matters identified them via all three of the channels listed above.</p> <p>Outlier behaviour: Respondents that did not identify a single potentially suspicious matter over the six month period.</p> |
| Organisational behaviour post-SMR | <p>16. 62% of respondents said their organisation would be likely to carry out eight, or all nine, of the listed categories of ECDD and good practice activities should they determine that an SMR needed to be submitted to AUSTRAC. This indicates a very high degree of organisational readiness to carry out a range of important ongoing due diligence measures.</p> <p>Outlier behaviour: Respondents that would be likely to carry out only five, or fewer, of the nine listed ECDD and good practice activities.</p> |

2 Background, methodology and response

2.1 Background and rationale for the survey

All reporting entities have an obligation to report suspicious matters to AUSTRAC if these matters are connected to the actual or potential provision of a designated service under the AML/CTF Act. This obligation is set out in section 41 of the AML/CTF Act. In summary, an SMR must be submitted to AUSTRAC if the reporting entity forms a suspicion on reasonable grounds that:

- a person (or their agent) is not the person they claim to be, or
- information that the reporting entity has may be:
 - relevant to the investigation or prosecution of a person for
 - an evasion (or attempted evasion) of a tax law (including that of a state or territory), or
 - an offence against a Commonwealth, state or territory law, or
 - of assistance in enforcing
 - the *Proceeds of Crime Act 2002* (or regulations under that Act), or
 - a state or territory law that corresponds to that Act or its regulations, or
- the provision of a designated service may be:
 - preparatory to the commission of an offence related to money laundering or the financing of terrorism, or
 - relevant to the investigation or prosecution of a person for an offence related to money laundering or the financing of terrorism.²

The staff training, transaction monitoring and enhanced customer due diligence (ECDD) obligations set out in the AML/CTF Rules are critical processes that enable reporting entities to identify customer activity and behaviour that may be reportable to AUSTRAC through an SMR (these Rules are reproduced at **Attachment A**). A series of questions in the survey covered these important areas.

The provision of aggregate information in this report is intended to promote greater understanding and compliance with the SMR obligations in the AML/CTF Act and those obligations that enable suspicious matters to be identified. Market Participants will be able to compare the programs, procedures and systems they have in place to meet their SMR and related obligations against those of the wider sector.

2.2 Methodology and response

In July 2010, AUSTRAC invited 83 Market Participants to complete the survey.³ Holders of an Australian Financial Services Licence can apply to the Australian Securities Exchange to be admitted as a Market Participant. The level of admission granted to each Market Participant dictates the types of markets the Market Participant can trade in, and whether

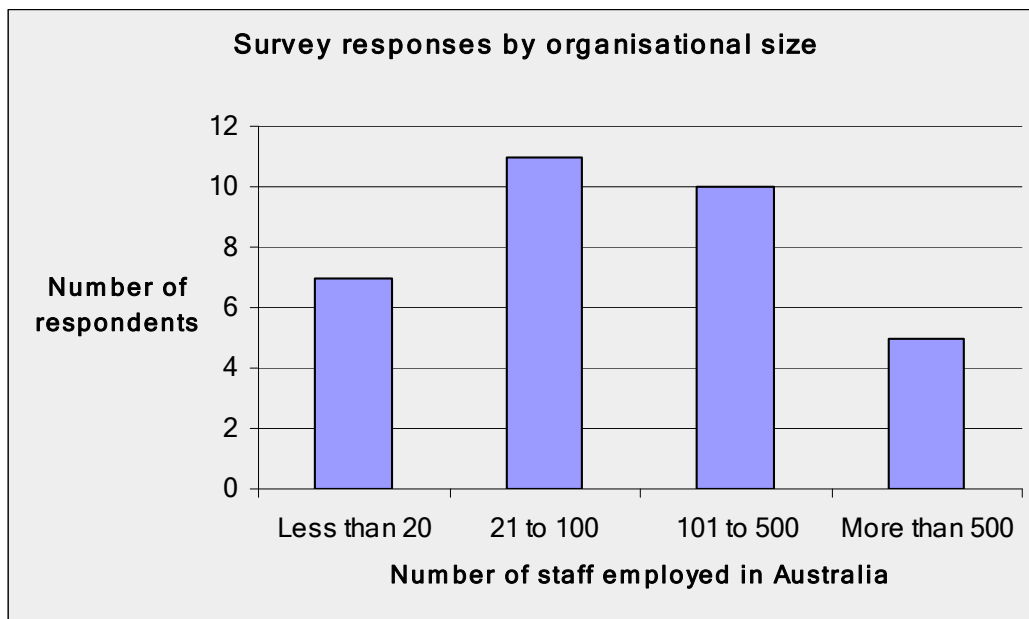
² Further information about the SMR obligation can be found in Chapter 9 of the *AUSTRAC Regulatory Guide* ('Reporting obligations') <http://www.austrac.gov.au/rq_9.html>, and AUSTRAC Public Legal Interpretation 6 ('Suspicious matter and suspect transaction reports') <<http://www.austrac.gov.au/pli.html>>.

³ The survey was open from 21 July to 6 August 2010.

they are permitted to trade for clients. When conducting trades for a customer these Market Participants are likely to be providing an item 33 designated service (under subsection 6(2) of the AML/CTF Act).⁴ Table 1 in subsection 6(2) of the Act describes item 33 designated services, and this section of the table is reproduced at **Attachment B**.

The survey was both anonymous and voluntary. There were no mandatory questions and the survey could only be completed online. It contained sixteen questions spread across five sections: Your organisation, ML/TF risk awareness training for staff, Transaction monitoring program, Red flags/triggers, and Review and submission. The survey can be found at **Attachment C**.

A total of 33 Market Participants completed the survey, producing a response rate of 40%.⁵ As the chart below indicates, responses were received from Market Participants across the four listed categories of organisational size (measured by number of staff employed in Australia).



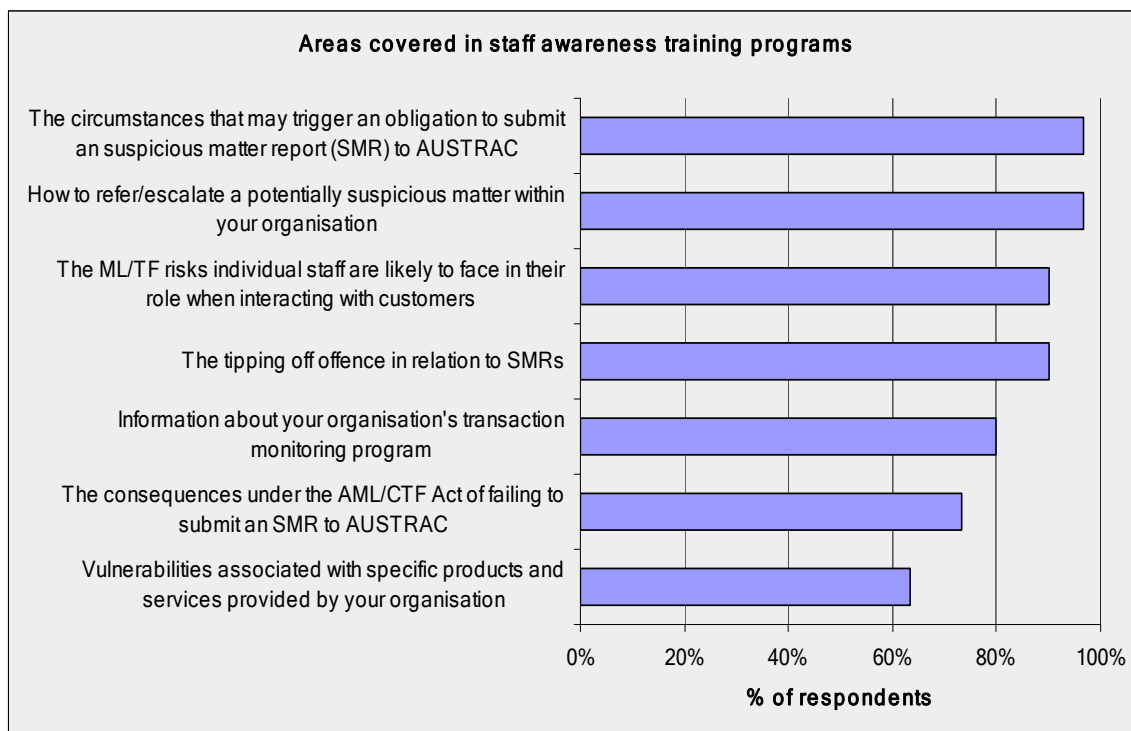
⁴ Market Participants may also provide other designated services to customers.

⁵ Most of these respondents completed almost every question in the survey. For example, 13 of the 16 survey questions were answered by between 26 and 33 respondents. One question was answered by 24 respondents, while Question 9, which was only relevant to those respondents who had a computer-based/automated transaction monitoring program, was answered by 18 respondents. Only 12 respondents answered the last question, 'What are the most significant issues your organisation faces in relation to suspicious matter reporting?' This question required a free text response.

3 Risk awareness training programs for staff

3.1 Content

Survey respondents were asked to select the content areas included in their staff risk awareness training programs. Seven broad content areas were provided and the responses are presented in the chart below.

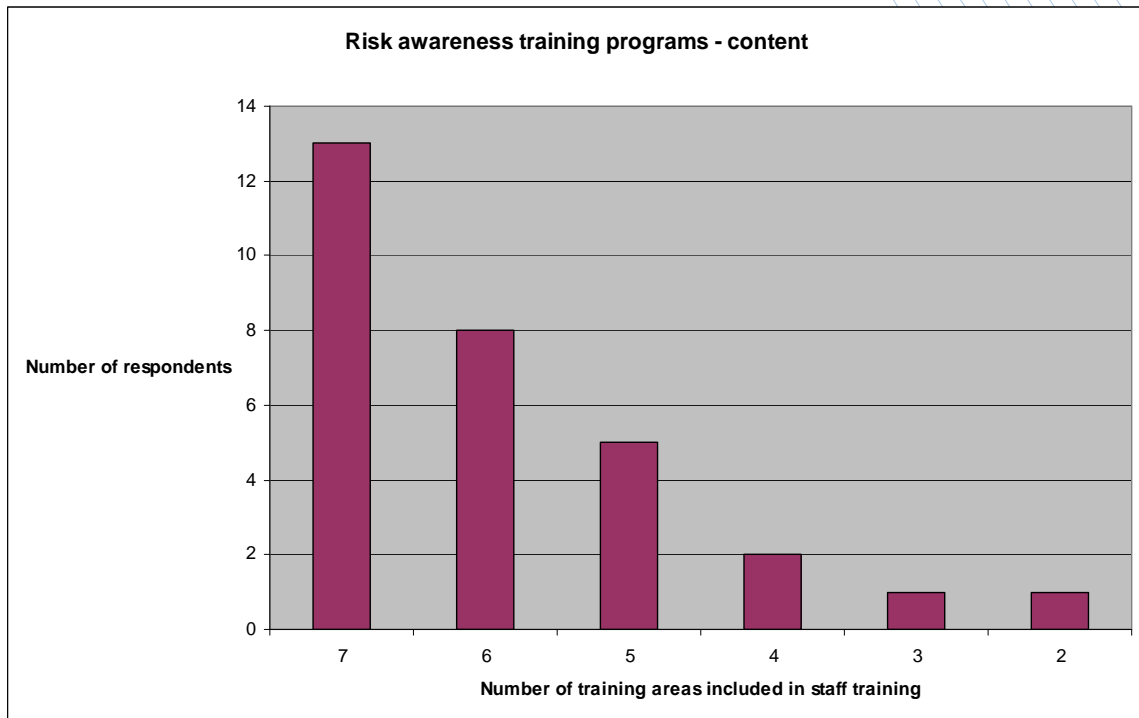


Nearly all respondents (97%) included in their training programs the circumstances that may trigger an obligation to submit a SMR to AUSTRAC and how to refer/escalate potentially suspicious matters within the organisation. Ninety percent of respondents reported that their training programs covered the ML/TF risks individual staff were likely to face in their role when interacting with customers, and 90 percent also covered the tipping-off offence. These are generally encouraging findings. The small number of respondents that did *not* include these items in their training programs exhibited outlier behaviour compared to their peers, and were the exception.

The last content area in the chart ('Vulnerabilities associated with specific products and services provided by your organisation') was included in training by 63% of respondents – less than any other category. AUSTRAC encourages entities to include information about the vulnerabilities associated with specific products and services the entities provide to customers in their risk awareness training programs. This inclusion is unlikely to pose a significant burden on entities – data collected in the 2009 AML/CTF compliance report⁶ indicated that almost all Market Participants have previously assessed the ML/TF risks posed by their designated services. Where possible, the findings from these assessments should be included in staff risk awareness training programs.

⁶ Under section 47 of the AML/CTF Act, reporting entities are required to submit an AML/CTF compliance report to AUSTRAC.

The responses to this question can also be analysed by looking at the number of respondents that included all seven listed areas, those that included six, and so on. The chart below presents the findings of this analysis.



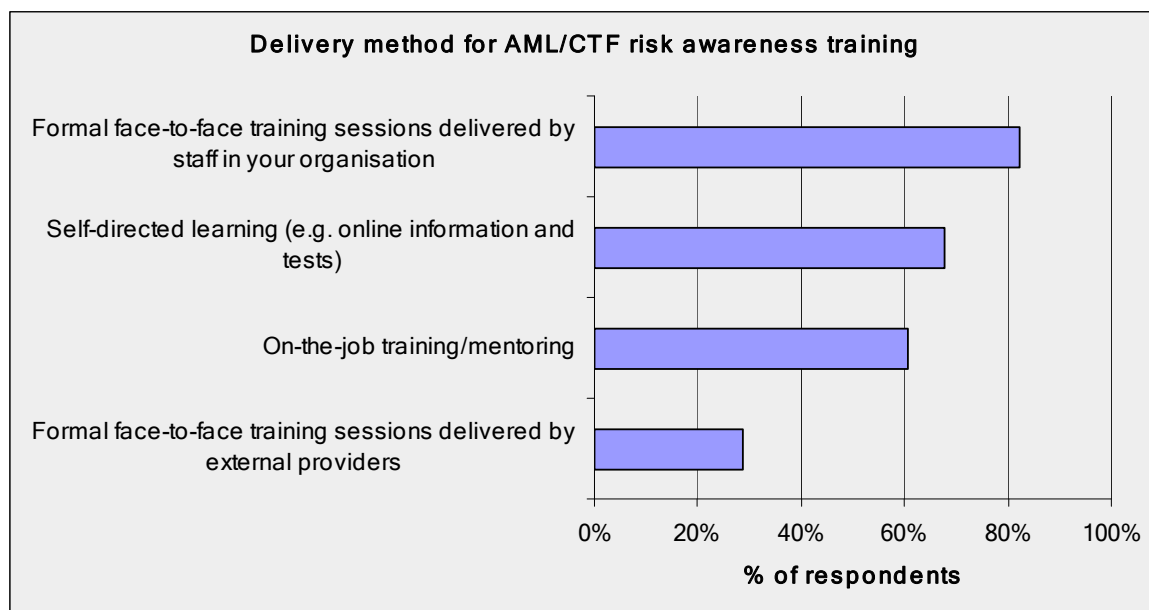
Of the 31 respondents that answered this question, 13 included all seven of the listed content areas in their risk awareness training for staff. A further eight included all but one. These two groups combined accounted for 21 respondents, spanning all four categories of organisational size. Taken together, this indicates that 70% of respondents covered a diverse and significant range of content areas in their programs and is an encouraging finding.

The five respondents that covered five of the listed content areas in their staff training may need to determine how they can further strengthen and broaden their staff training programs. These respondents were spread across all categories of organisational size. There was some commonality among these respondents in terms of the areas which they did *not* include in their training programs – four of the five did not include information about vulnerabilities associated with specific products and services provided by their organisation or information about the consequences under the AML/CTF Act of failing to submit a SMR to AUSTRAC.

The four respondents that covered four or fewer of the seven listed content areas within their staff training exhibited outlier behaviour compared to the majority their peers. In general, respondents in the 'less than 20 staff' category of organisational size tended to include a wider range of content areas within their risk awareness training for staff.

3.2 Delivery method

The chart below indicates that the most common delivery method for staff risk awareness training was through formal face-to-face training sessions delivered by staff in the organisation. On-the-job training/mentoring and self-directed learning were also common delivery methods.

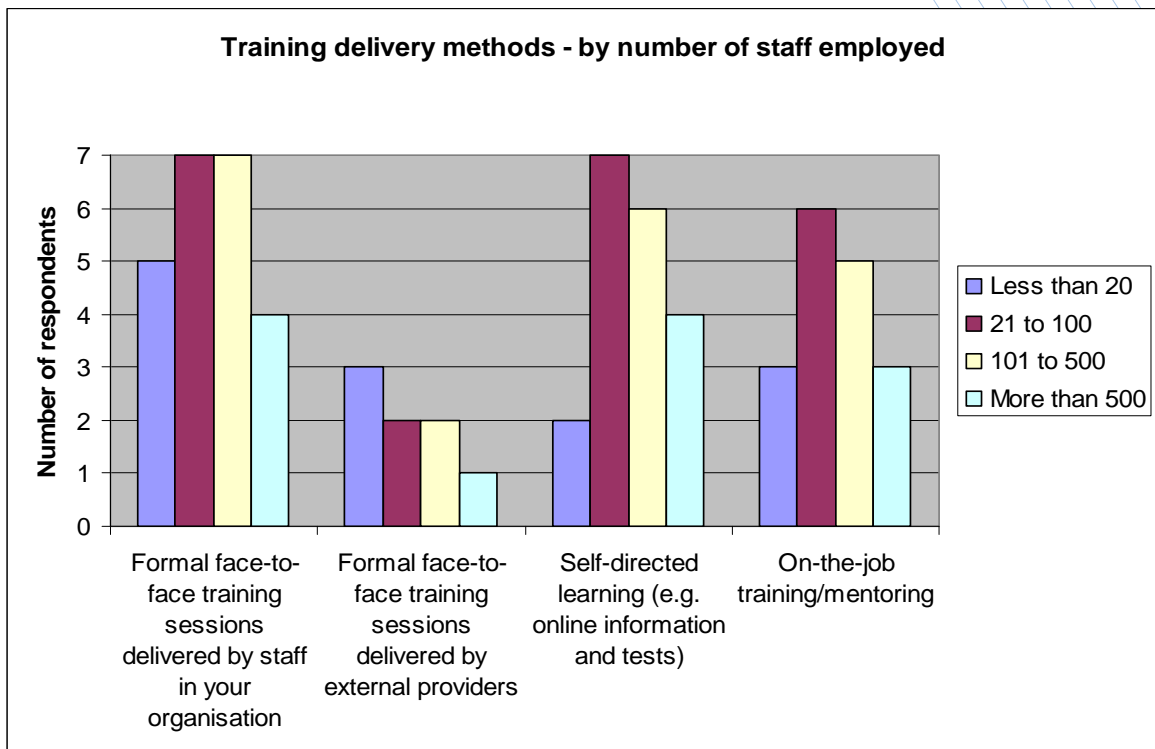


The survey found that respondents generally used a variety of delivery methods to round out their risk awareness training program for staff. This is an encouraging finding. For example, of the 82% of respondents that delivered training via formal face-to-face sessions delivered by the organisation's staff:

- 70% also delivered staff training via self-directed learning (using online information and tests)
- 65% also deliver staff training via on-the-job training and mentoring.

Although a much smaller number of respondents (29%) used external providers to deliver formal face-to-face training, the majority of those that did use external providers also used online information and tests as well as on-the-job training and mentoring to deliver their staff training (63% in both cases).

Respondents were likely to utilise a variety of methods to deliver their risk awareness training programs regardless of the size of their organisation. The chart below shows the extent to which these delivery methods are used by respondents across the four categories of organisational size.



3.3 Useful resources for developing staff training programs

Survey respondents were asked to select the resources that were useful in the development of their staff risk awareness training programs. The survey suggested nine broad content areas, and the responses are presented in the chart below.

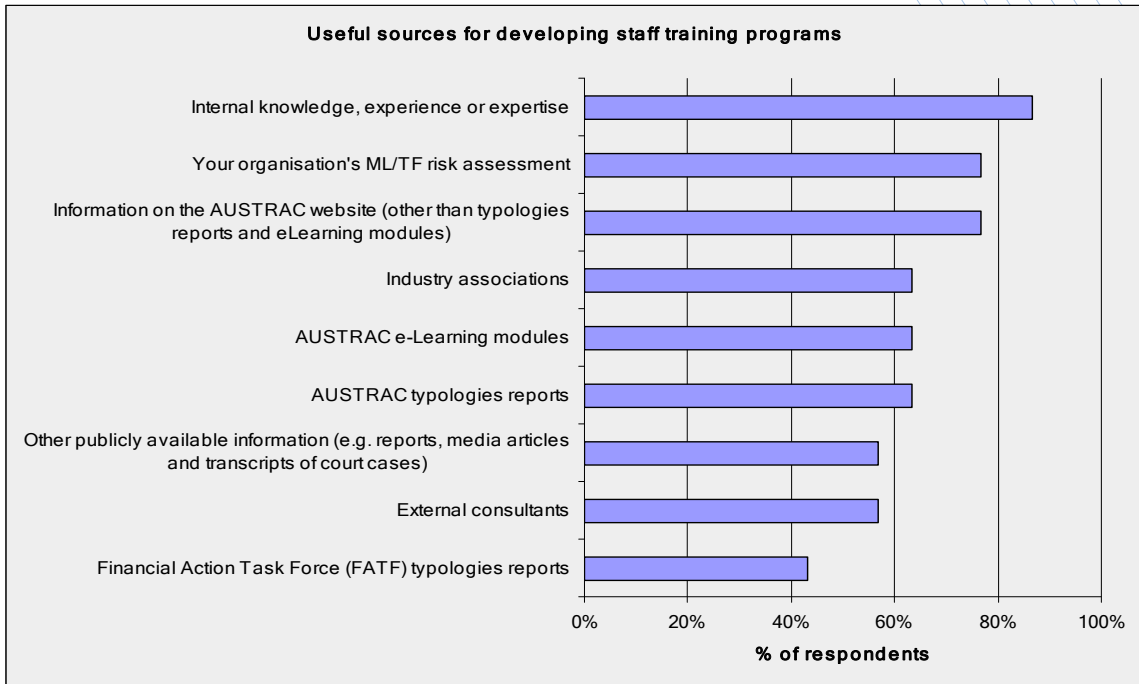
Most respondents (87%) found their own knowledge, experience and expertise to be useful in the development of their ML/TF risk awareness staff training program. The majority (77%) also found their organisation’s ML/TF risk assessment to be useful.

Slightly less than two-thirds of the respondents (63%) found the AUSTRAC e-learning and AUSTRAC typologies reports to be useful in the development of their ML/TF risk awareness training program. Typologies reports were useful for *all* respondents with more than 500 employees, but useful to only 40% of respondents with less than 20 staff.

More than three-quarters of respondents (77%) found information on the AUSTRAC website (other than the typologies reports and the AUSTRAC e-learning modules) to be useful in the development of their staff training programs.

The FATF typologies reports were useful for less than half the respondents (43%), the lowest of any category of resource. This low response is of interest as it suggests that, in particular, the comprehensive October 2009 FATF typologies report on the securities sector is underutilised for training purposes by this sector.⁷

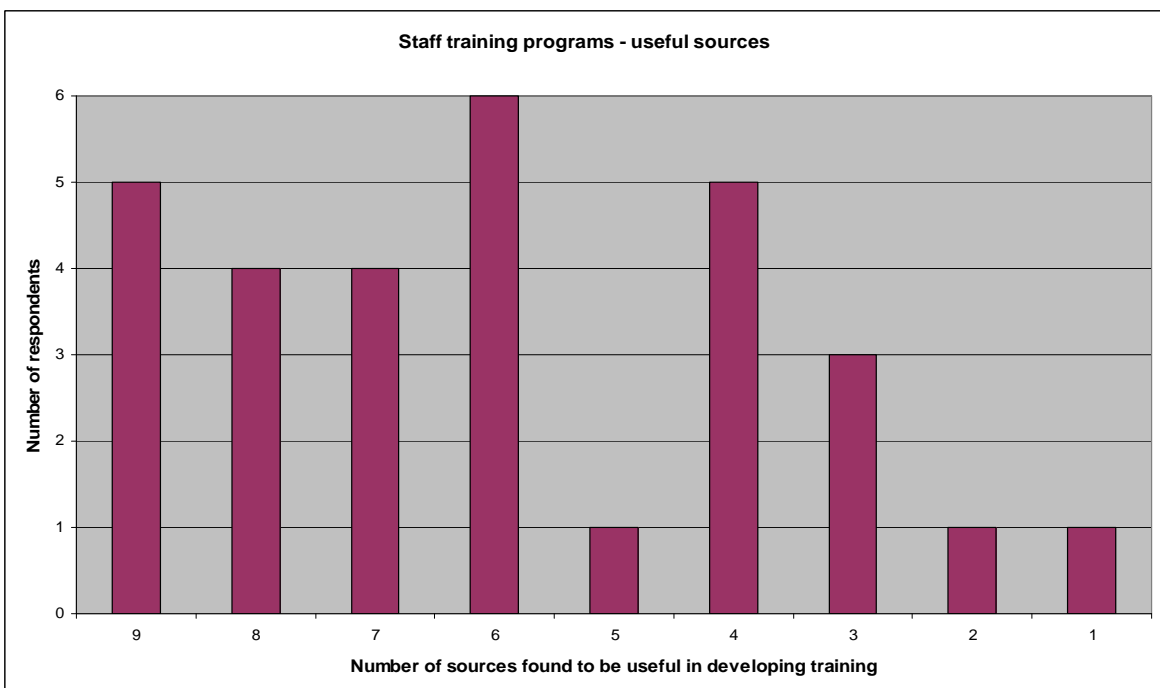
⁷ Financial Action Task Force, *Money Laundering and Terrorist Financing in the Securities Sector*, FATF, Paris, viewed 28 October 2010, <http://www.fatf-gafi.org/document/29/0,3343,en_32250379_32237202_43939933_1_1_1_1,0,0.html>



Of the 30 respondents that completed the question, only five said that all nine listed sources were useful in the development of their risk awareness training program for staff.

A cluster of 19 respondents found six or more of the nine listed sources to be useful in the development of their staff training programs, representing almost two-thirds of all respondents. Respondents from all categories of organisational size are represented in this grouping.

The five respondents that said three or fewer of the listed sources were useful in developing their staff risk awareness training program exhibit outlier behaviour compared to their peers. These respondents all come from the 'less than 20' and the '21-to-100 employees' categories of organisation size. All Market Participants are encouraged to ensure that they draw on the widest possible selection of sources to develop their staff training program.

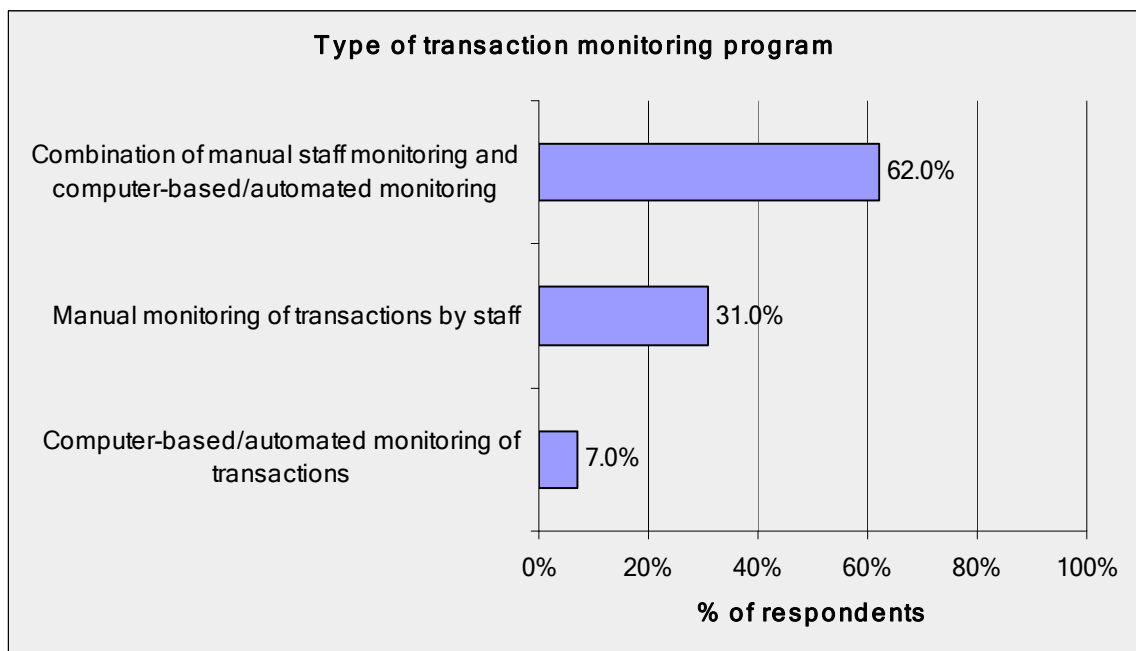


4 Transaction monitoring programs

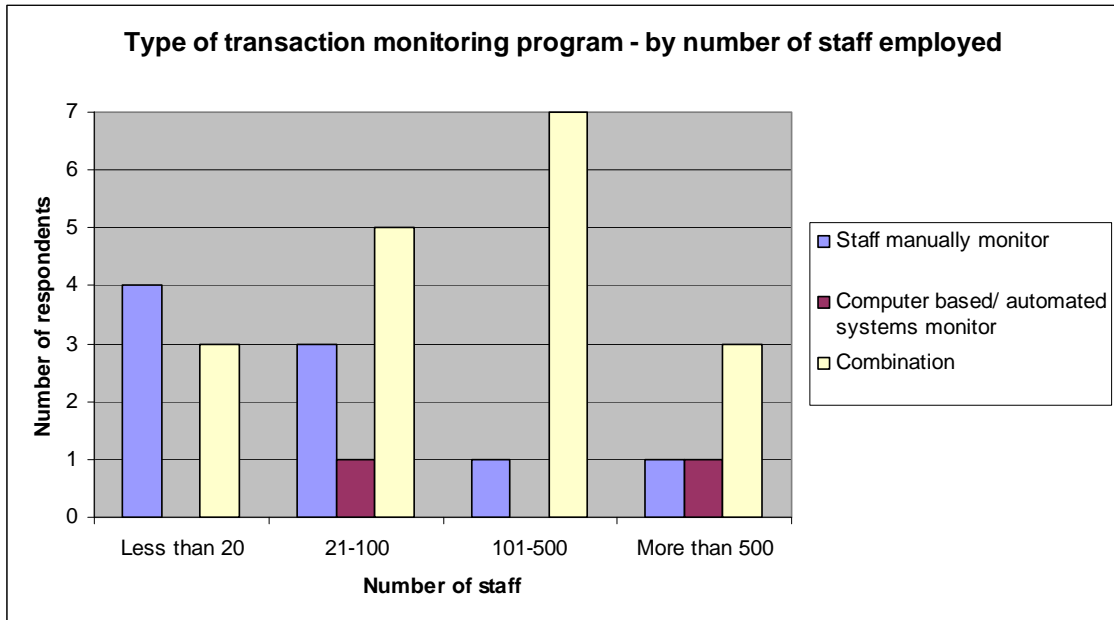
4.1 Type

Survey respondents were asked to select the manner in which they monitor customer transactions. As the chart below indicates, most respondents (62%) monitored customer transactions through a combination of manual transaction monitoring conducted by staff and monitoring conducted by computer-based/automated systems.

Less than a third of respondents (31%) relied solely on staff to manually monitor customer transactions. A much smaller number (7%) relied solely on computer-based/automated systems to monitor customer transactions.



When analysed by organisational size (see below), a combined manual monitoring/computer based automated system is the most common customer transaction monitoring framework across all categories of organisational size, with the exception of organisations with less than 20 staff. Organisations with less than 20 staff are slightly more likely to rely solely on staff to manually monitor customer transactions than to have a combined transaction monitoring framework in place.



4.2 Ensuring effectiveness

Respondents with a computer-based/automated system for monitoring customer transactions were asked a follow up question about the activities they undertake to ensure their system is effective. Most respondents test triggers/rules (72% of respondents), review triggers/rules (89%), monitor the volume of alerts (89%), and assess the quality of alerts (94%). These responses spanned all categories of organisational size. Around half the respondents with computer-based/automated transaction monitoring systems provide feedback to staff about the alerts that are generated.

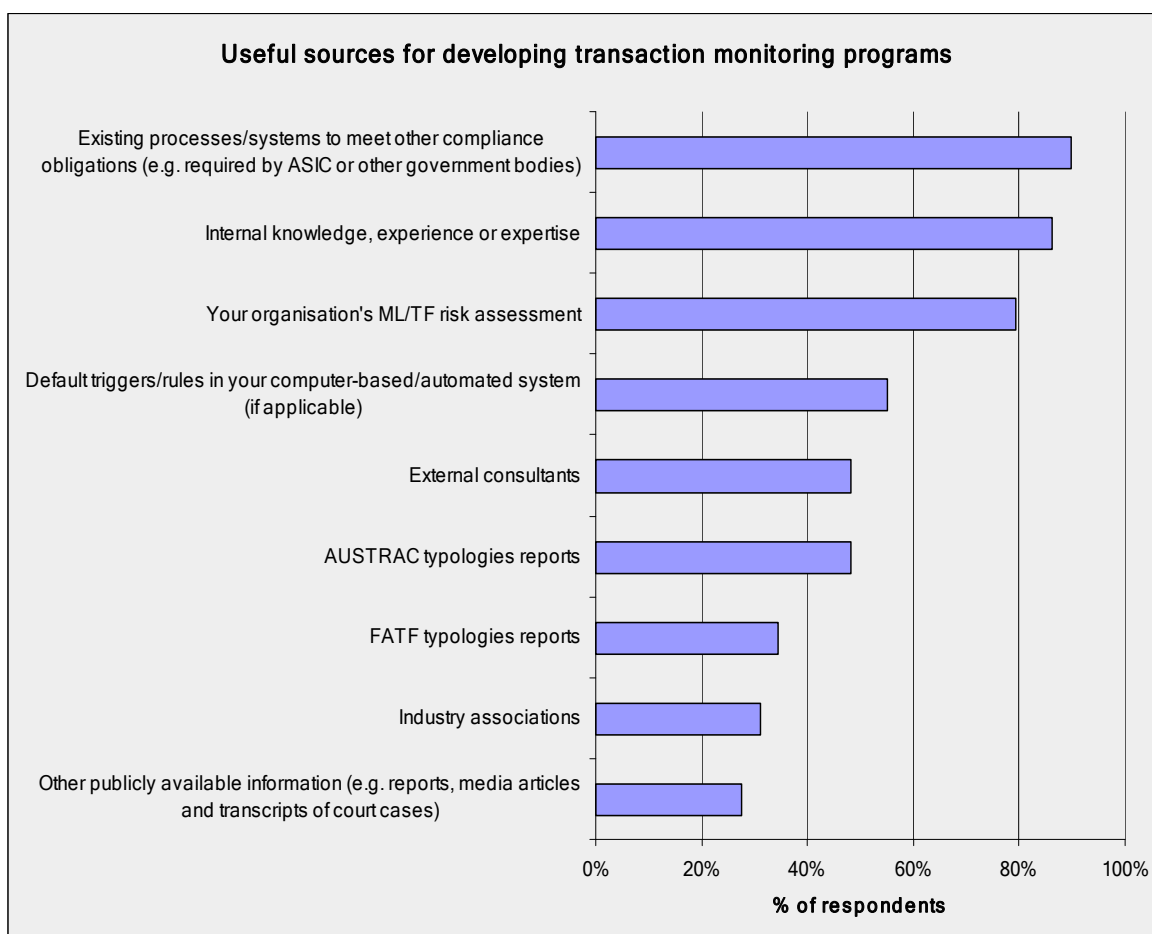
4.3 Useful sources for developing transaction monitoring programs

Survey respondents were asked to select the sources they found useful in the development of their transaction monitoring programs. Nine broad content areas were provided and the responses are presented in the chart below.

Ninety percent of respondents found existing processes/systems that had been established to meet other compliance obligations (for example, for ASIC or other government agencies) to be useful in developing their transaction monitoring program. This is the highest result for all categories and is a significant finding. It indicates that Market Participants have been able to utilise existing processes and systems to meet their AML/CTF transaction monitoring obligations.

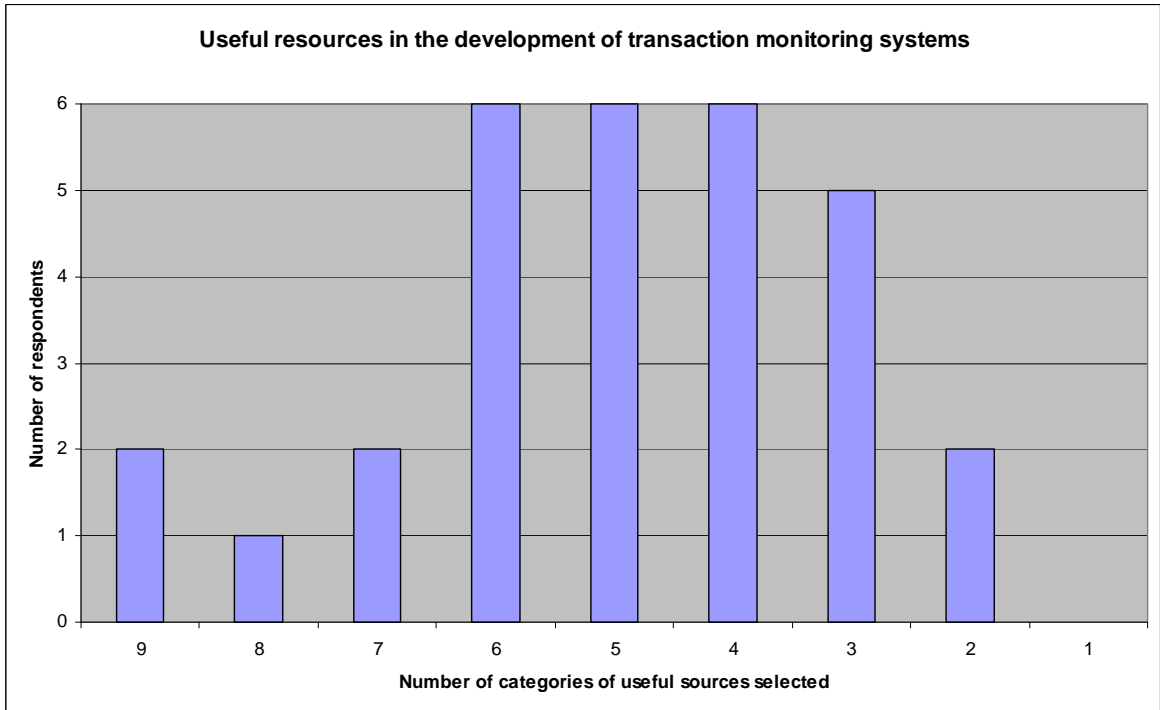
A large number of respondents found their own internal knowledge and expertise (86%) and their ML/TF risk assessment (79%) to be useful in developing their transaction monitoring program.

Slightly less than half (48%) found the AUSTRAC typologies reports useful in developing their transaction monitoring program, while just over a third (35%) found the FATF typologies reports to be useful.



Of the 30 respondents that answered this question, only two reported that all nine listed sources were useful in the development of their transaction monitoring program.

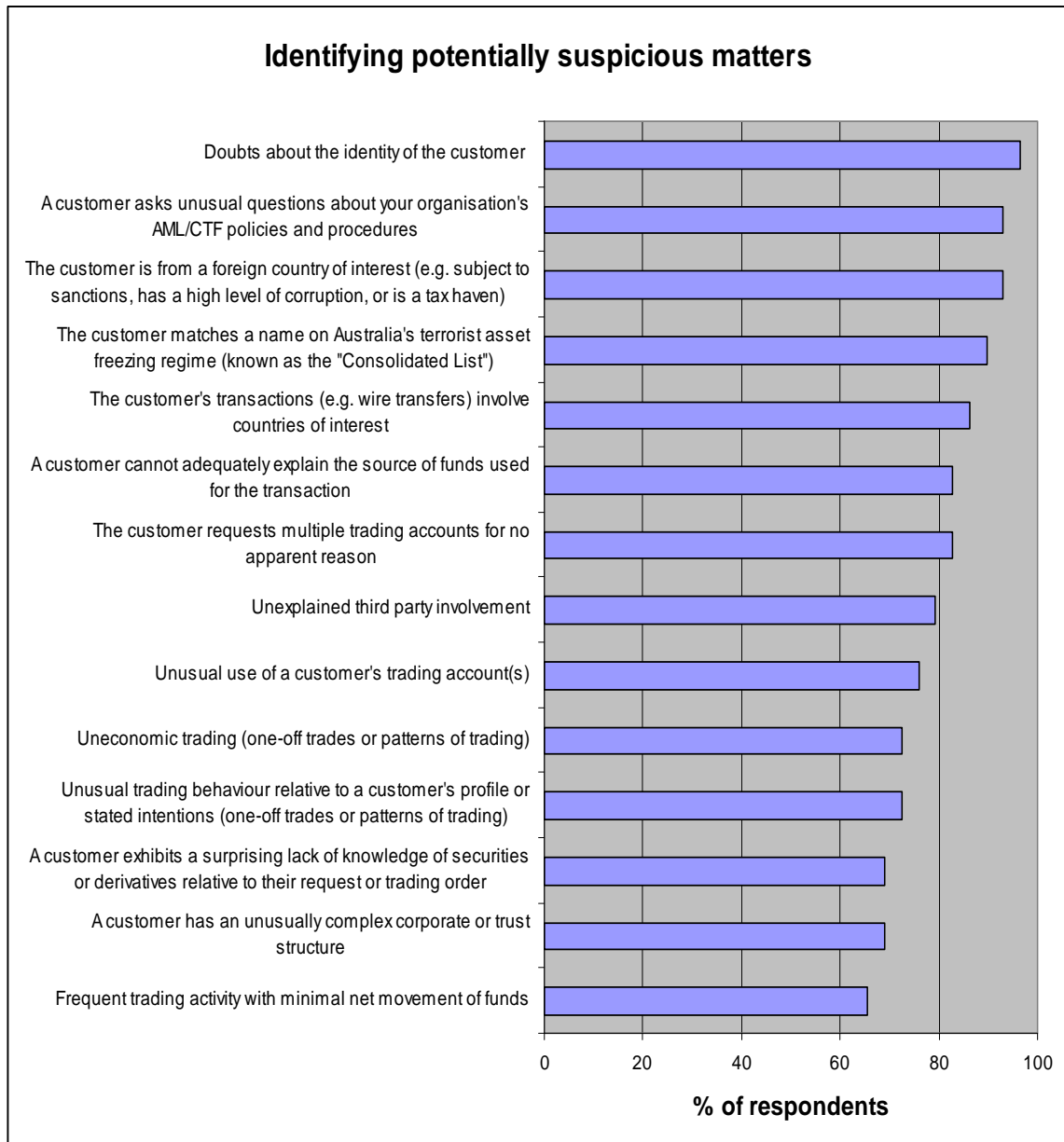
A cluster of 23 respondents (representing 77% of all respondents) found between three and six of the nine listed sources to be useful in the development of their transaction monitoring program.



5 Suspicious matters

5.1 Red flags/triggers

Survey respondents were presented with a list of 14 'potentially suspicious matters' and were asked to indicate which of these their organisation would be able to identify.⁸ The chart below presents the results.



⁸ The term 'potentially suspicious matters' was used in the survey and in this report. It is not, however, a term used in the AML/CTF Act or the AML/CTF Rules. It is intended to capture those matters raised by staff or by computer-based systems that require internal review in order to determine whether they are suspicious within the meaning of section 41 of the AML/CTF Act and are therefore required to be reported to AUSTRAC through the submission of an SMR. These categories are not an exhaustive list of potentially suspicious matters for this sector.

The spread of responses varies significantly across the 14 categories of potentially suspicious matters, and it is clear that some of the categories are more likely to be identified than others. Organisational size (based on employee numbers) did not have a significant impact on a respondent's stated capacity to identify these potentially suspicious matters.

Most respondents believed their organisation would identify potentially suspicious matters related to doubts about a customer's identity (97%), and matters where a customer's location (93%) or the transaction (86%) involved a foreign country of interest (for example, a country that was subject to sanctions or was a tax haven). These are encouraging findings.

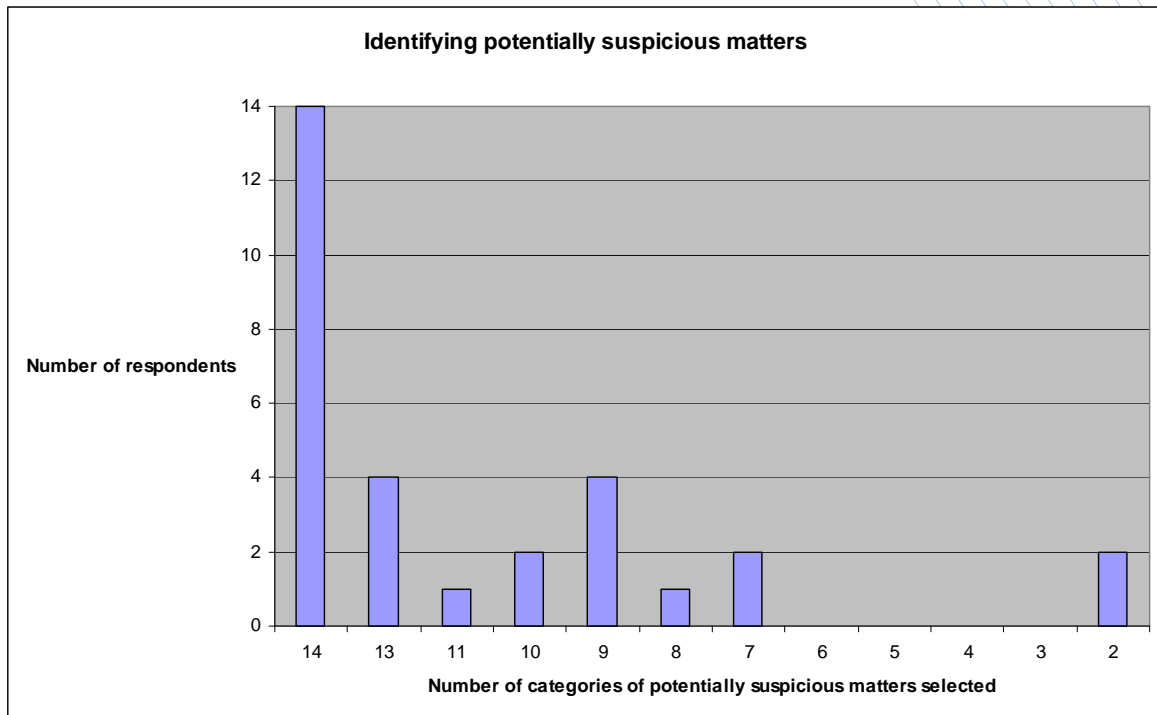
Most respondents also indicated a very high level of engagement with Australia's terrorist asset freezing regime, which applies to all persons and entities included within the 'Consolidated List' maintained by the Department of Foreign Affairs and Trade and included on the department's website. Nine out of ten respondents (90%) believed their organisation would identify when a customer name matches a name on Australia's terrorist asset freezing regime.⁹

Seventy percent or more of respondents believed their organisation would identify potentially suspicious customer behaviour that would rely, at least to some extent, on staff interaction with a customer, highlighting the critical role played by staff and the importance of having effective staff training programs.

Just over 20% of respondents believed their organisation would *not* be able to identify potentially suspicious matters where there was unexplained third party involvement in a transaction. A larger number (31%) said they would not identify potentially suspicious matters where the customer had an unusual company or trust structure. The lack of organisational capacity among these respondents to identify potentially suspicious matters relating to these two important areas suggests that some Market Participants need to further examine their organisational capacity in this area.

⁹ Further information about Australia's terrorist asset freezing regime can be found at: <http://www.dfat.gov.au/globalissues/terrorism.html>

The responses to this question can be further analysed by examining the number of respondents that selected all 14 listed categories of potentially suspicious matters, those that selected 13, and so on. The chart below presents the findings of this analysis.

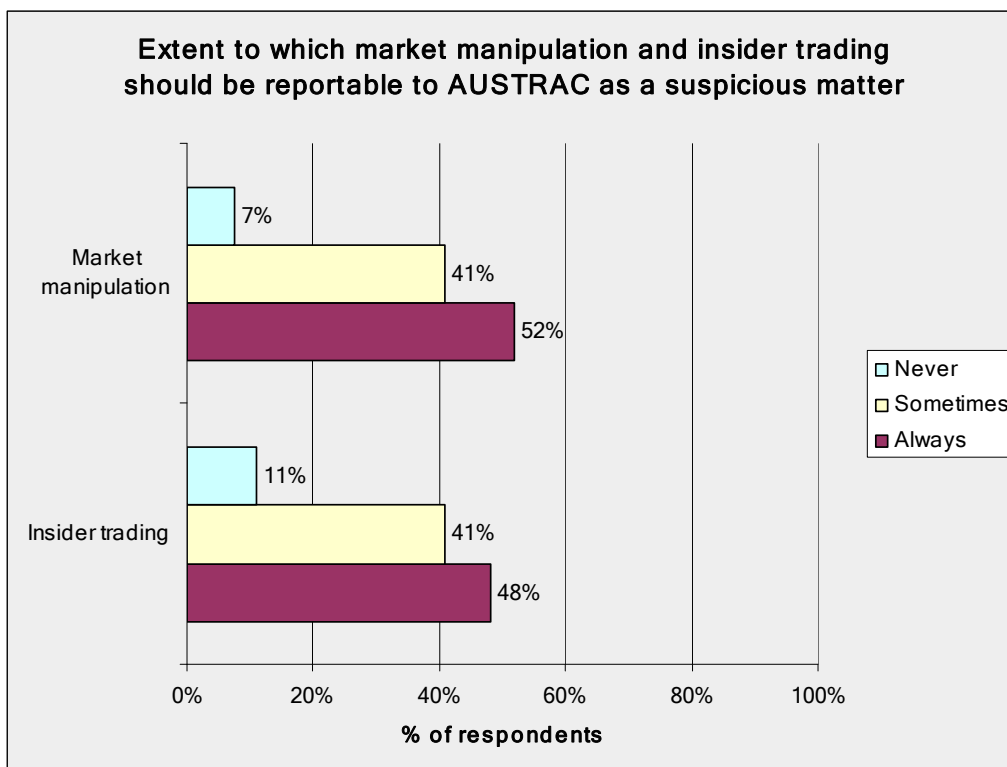


The following observations can be made about the above chart:

- Almost half the respondents (14 of 30) said their organisation would identify *all* fourteen listed categories. Another four respondents said they would identify all but one of the listed categories. This indicates that six out of ten respondents believe they have a very high degree of organisational readiness to identify a diverse range of potentially suspicious matters and is an encouraging result.
- Three respondents believed their organisation would identify either ten or eleven of the listed categories of potentially suspicious matters. There was no clear pattern in relation to the categories of potentially suspicious matters that these organisations would *not* be able to identify.
- A total of seven respondents believed their organisation would identify between seven and nine of the fourteen listed categories of potentially suspicious matters. The organisational readiness of this group of respondents to identify a diverse range of potentially suspicious matters is less developed than their peers.
- Two respondents said their organisation would only identify two of the 14 listed categories of potentially suspicious matters. These respondents are an exception among all respondents and their lack of organisational capacity to identify potentially suspicious matters compared to their peers indicates that further action is required to enhance their organisational readiness in this area.

5.2 Insider trading and market manipulation

The survey included a question to determine how respondents saw the interaction between the SMR obligation in the AML/CTF Act and the breach reporting (insider trading and market manipulation) obligations imposed on Market Participants under the *Corporations Act 2001*. The results are set out in the chart below.



A large majority of respondents believed both insider trading and market manipulation should be reported to AUSTRAC through the submission of an SMR.

- 89% of respondents believed insider trading should 'sometimes' or 'always' be reported to AUSTRAC through an SMR.
- 93% of respondents believed market manipulation should 'sometimes' or 'always' be reported to AUSTRAC through an SMR.

These are encouraging findings and indicate that a large majority of respondents are aware that matters involving these issues fall within the ambit of the SMR obligation in section 41 the AML/CTF Act. The importance of reporting insider trading, in particular, to a national financial intelligence unit was highlighted in the FATF report on money laundering and terrorist financing in the securities sector. The 2009 report noted that:

insider trading is unique to the securities industry and generates illicit assets. As a predicate offence for money laundering, and an offence in its own right, this type of misconduct is reportable on STRs [suspicious transaction reports] and has proven useful in assisting law enforcement and regulators prosecute such misconduct.¹⁰

¹⁰ Financial Action Task Force, *Money Laundering and Terrorist Financing in the Securities Sector*, FATF, Paris, viewed 28 October 2010, <http://www.fatf-gafi.org/document/29/0,3343,en_32250379_32237202_43939933_1_1_1_1,00.html>

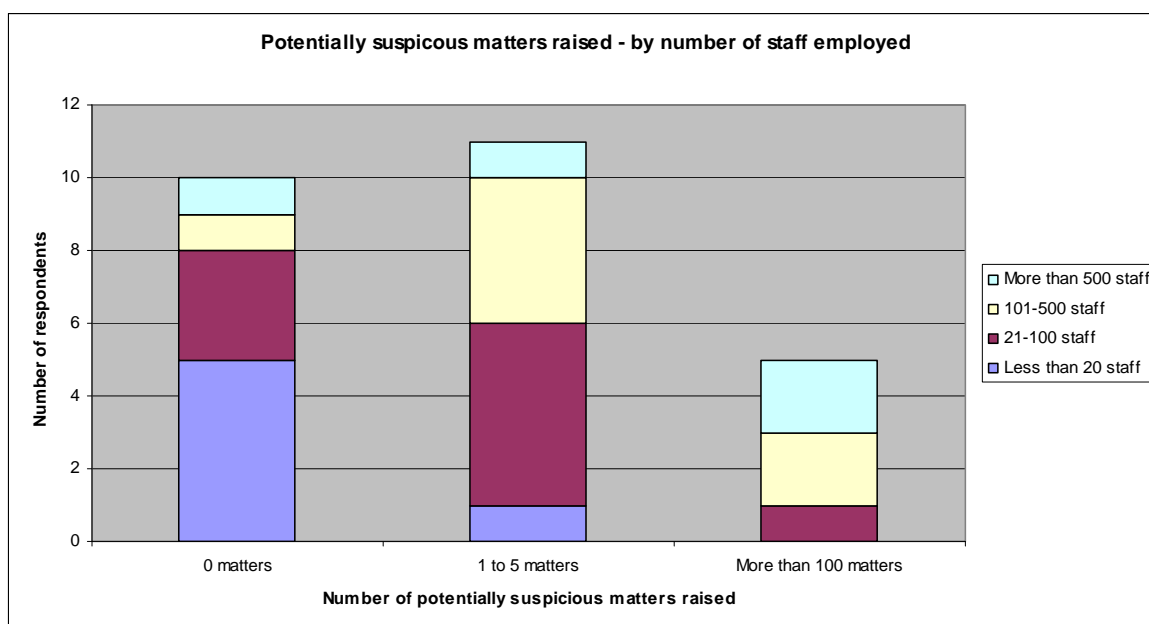
Only a very small minority believed that insider trading (11%) and market manipulation (7%) should ‘never’ be reported to AUSTRAC as an SMR. These views were at variance with those held by their peers.

5.3 Incidence of identified matters

Survey respondents were asked to indicate approximately how many potentially suspicious matters had been raised within their organisations during the first six months of 2010. Organisations were grouped according to how many matters they had raised – that is, zero, 1–5, 6–10, 11–20, 21–50, 51–100, or more than 100 matters. The findings are presented by organisational size in the chart below.

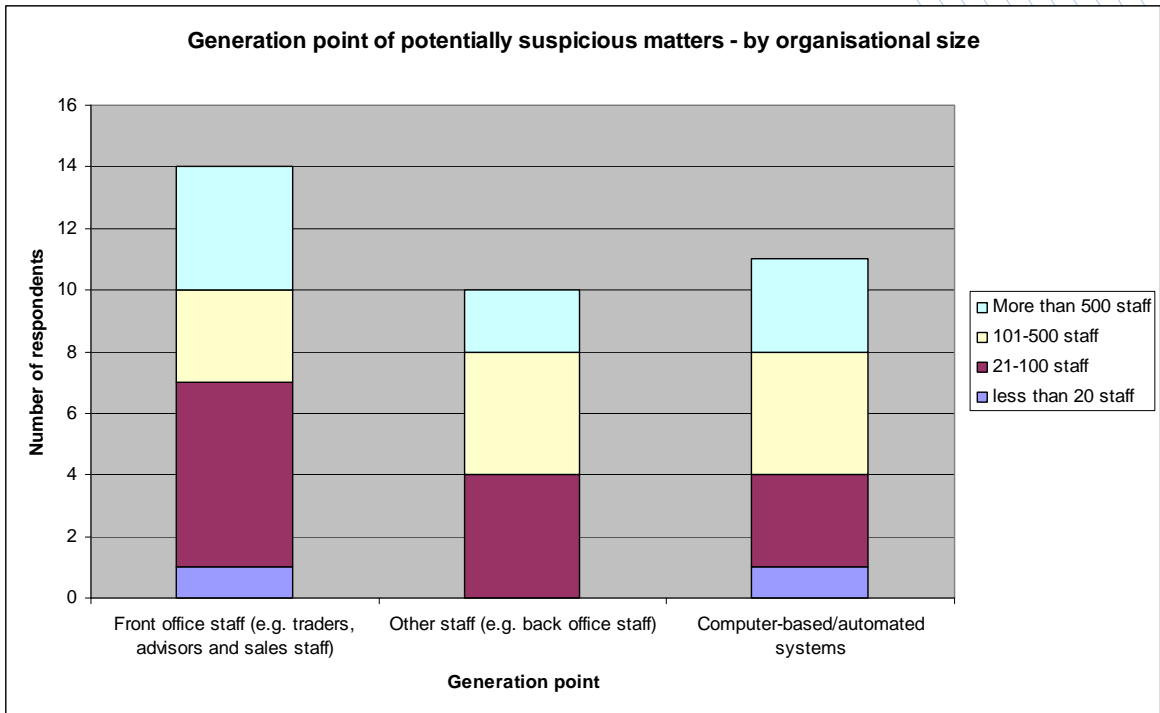
Overall, 16 of the 26 respondents (61%) that answered this question had identified one or more potentially suspicious matters over the six-month period. Other observations include:

- Potentially suspicious matters were generated by respondents across all four categories of organisational size.
- Respondents that had identified potentially suspicious matters fell into just two distinct groups – respondents that had raised 1–5 matters, and those that raised more than 100 matters. It is not clear why all of the respondents that had identified matters were clustered at either end of the ‘number of matters raised’ spectrum.
- Almost four in ten respondents (39%) had *not* generated a single potentially suspicious matter for internal review during the first six months of 2010.



5.4 Diversity of business areas generating suspicious matters

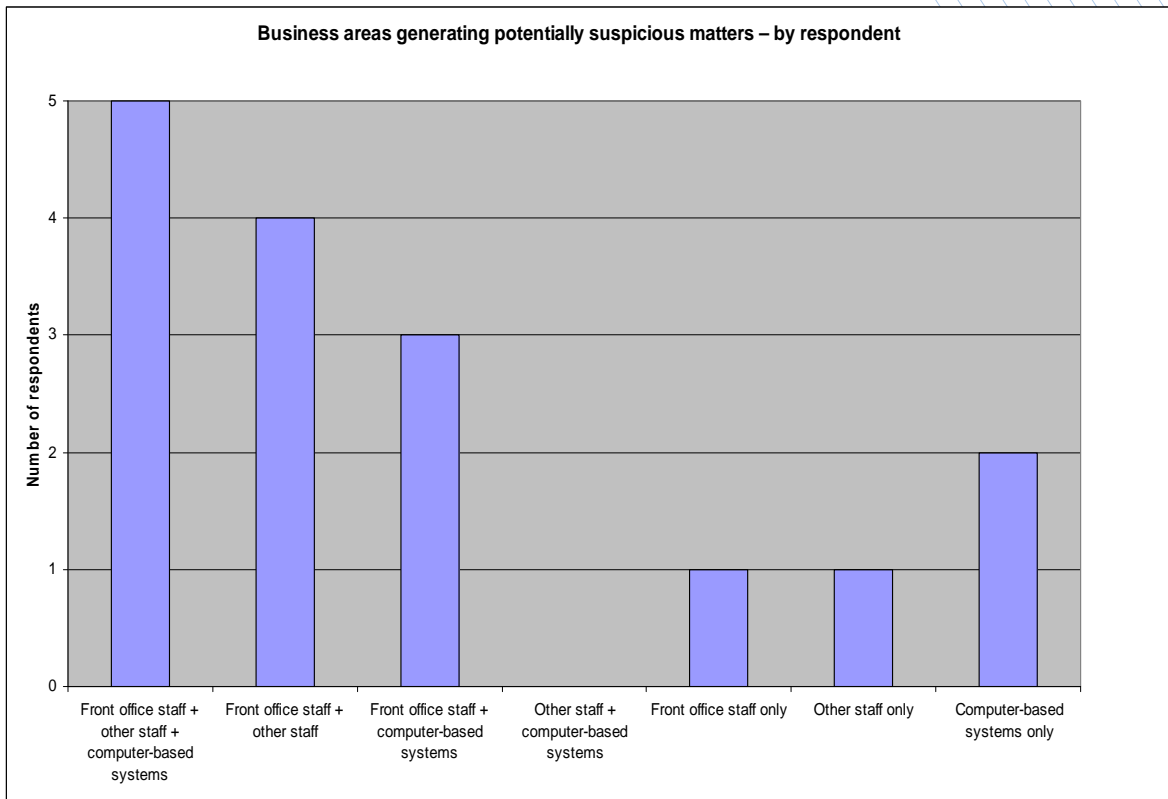
In most organisations, a measure of organisational readiness to identify suspicious matters would be the diversity of business areas and systems from which potentially suspicious matters are generated. The 16 respondents that had identified potentially suspicious matters were also asked to state from where in their organisation these matters were generated (from among three broad response options). The chart below presents the findings by organisational size.



Respondents said potentially suspicious matters were generated across all three of the listed response options, which is an encouraging result. There was a slight bias towards potentially suspicious matters raised via front office staff (for example, traders, advisors, and sales staff) compared to the other two response options. Fourteen of the sixteen respondents that had identified potentially suspicious matters had raised them via their front office staff.

Most of the respondents that had generated potentially suspicious matters over the period had a transaction monitoring program comprising both manual staff monitoring and computer-based/automated systems.

An analysis of individual responses to this question revealed that a significant number of respondents had generated potentially suspicious matters via two or more of these business areas as opposed to just one of the three areas.



Three-quarters of respondents that generated potentially suspicious matters raised them via two of the three areas listed in the chart. Almost a third of respondents (30%) raised these matters via all three areas.

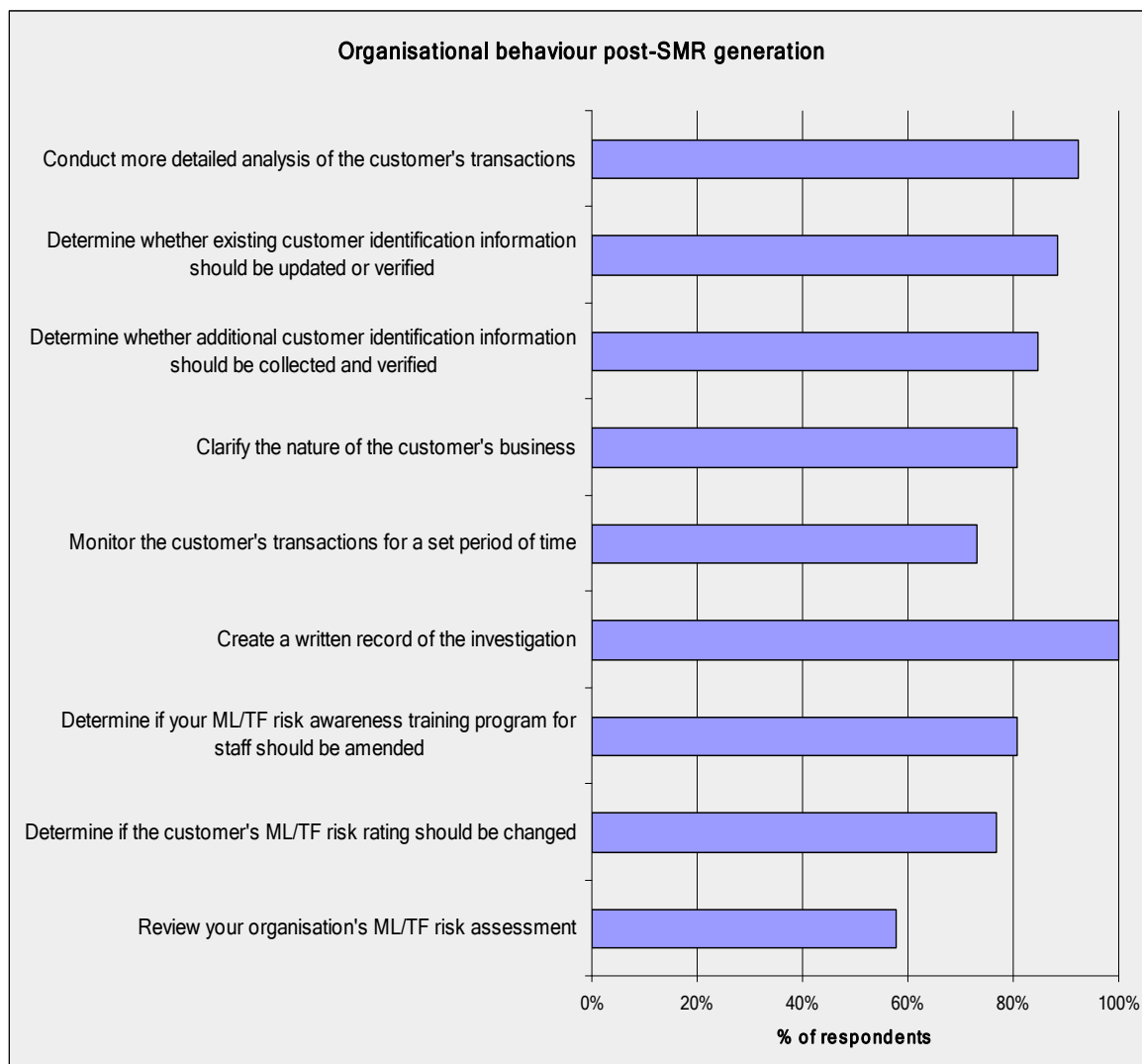
5.5 Submission of SMRs to AUSTRAC

The survey asked respondents to nominate which of the two available methods they would be likely to use to submit SMRs to AUSTRAC.

- 92% of respondents said they would submit SMRs electronically through AUSTRAC Online.
- 8% said they would choose to submit SMRs using a hard copy paper form.

6 Organisational behaviour post-SMR generation

Respondents were asked to state the activities they were likely to carry out *after* their organisation determines that an SMR should be submitted to AUSTRAC. The results are presented in the chart below.



The first five response options in this chart roughly correlate to the enhanced customer due diligence (ECDD) provisions in chapter 15 of the AML/CTF Rules. The last four response options are not listed in the AML/CTF Rules, but are considered by AUSTRAC to be good practice for entities to follow once it has been determined that an SMR should be submitted to AUSTRAC.

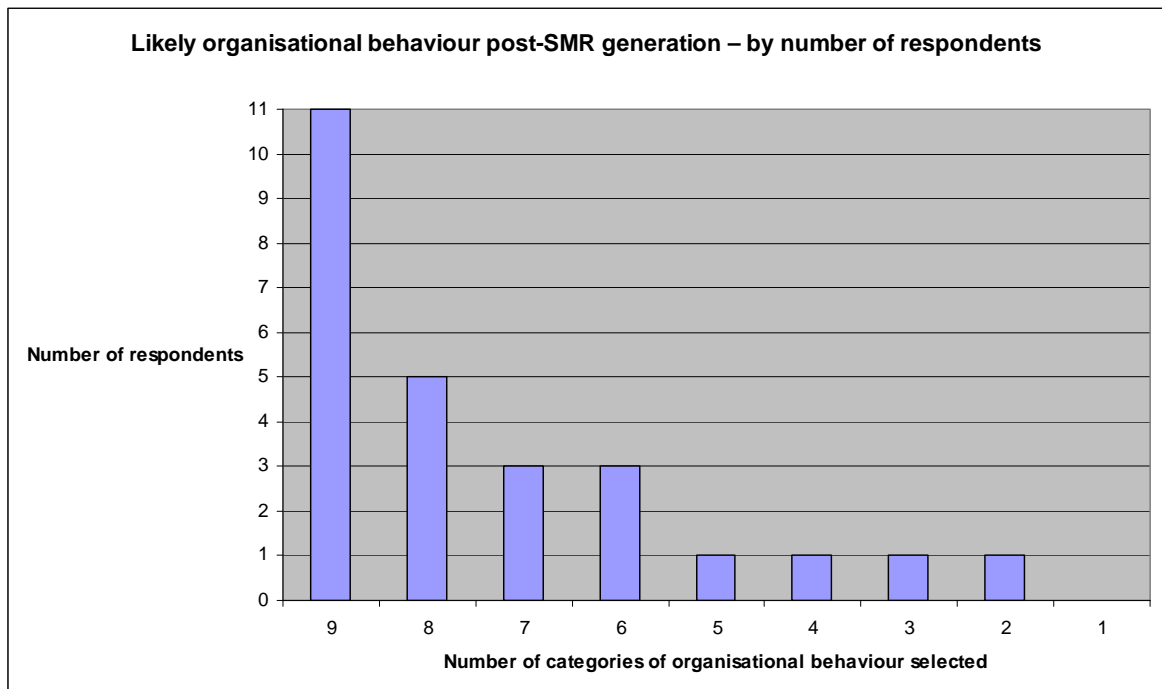
Overall, the responses to this question are encouraging. They indicate that most respondents are likely to undertake the five ECDD measures related to AML/CTF Rules, (73% or more for each response option), and in particular to conduct a detailed analysis of the customer's transactions (92% of respondents, more than any other ECDD category).

More than 50% of respondents said their organisation would be likely to carry out the four activities not listed in the AML/CTF Rules but considered good practice. Of these four, all respondents said they would be likely to create a written record of the investigation but

only slightly more than half (58%) said they would review the organisation's ML/TF risk assessment.

Organisational size as measured by number of staff had little bearing on the way respondents answered this question, with the exception of organisations with less than 20 employees – all respondents with fewer than 20 staff reported that their organisation would be likely to carry out *all* 11 of the listed activities if they determined that an SMR should be submitted to AUSTRAC.

The responses to this question can be further analysed by looking at the number of respondents that selected all 11 listed categories of potentially suspicious matters, those that selected 10, and so on. The chart below presents the findings of this analysis.



As the chart indicates, 16 of the 26 respondents that answered this question said they would be likely to carry out eight or all nine of the listed categories of organisational behaviour after it was determined that an SMR should be submitted to AUSTRAC. This represents some 62% of all respondents and is an encouraging finding. It indicates the majority of respondents have a high degree of organisational readiness to carry out the ECDD and good practice activities should an SMR be submitted to AUSTRAC.

Six respondents said they would be likely to carry out six or seven of the nine listed activities. These respondents should investigate how their organisational readiness could be enhanced after they generate an SMR.

Four respondents said they would be likely to carry out five or fewer of the nine listed activities. These respondents were an exception compared to their peers.

Attachment A – AML/CTF Rules referenced in this report

Part 8.2 AML/CTF risk awareness training program

- 8.2.1 Part A must include an AML/CTF risk awareness training program that meets the requirements of paragraphs 8.2.2 to 8.2.3 below.
- 8.2.2 The AML/CTF risk awareness training program must be designed so that the reporting entity gives its employees appropriate training at appropriate intervals, having regard to ML/TF risk it may reasonably face.
- 8.2.3 The AML/CTF training program must be designed to enable employees to understand:
- (1) the obligations of the reporting entity under the AML/CTF Act and Rules;
 - (2) the consequences of non-compliance with the AML/CTF Act and Rules;
 - (3) the type of ML/TF risk that the reporting entity might face and the potential consequences of such risk; and
 - (4) those processes and procedures provided for by the reporting entity's AML/CTF program that are relevant to the work carried out by the employee.

Chapter 15 Ongoing customer due diligence

Transaction monitoring program

- 15.4 A reporting entity must include a transaction monitoring program in Part A of its AML/CTF program.
- 15.5 The transaction monitoring program must include appropriate risk-based systems and controls to monitor the transactions of customers.
- 15.6 The transaction monitoring program must have the purpose of identifying, having regard to ML/TF risk, any transaction that appears to be suspicious within the terms of section 41 of the AML/CTF Act.
- 15.7 The transaction monitoring program should have regard to complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

Enhanced customer due diligence program¹¹

- 15.8 A reporting entity must include an enhanced customer due diligence program in Part A of its AML/CTF program.

¹¹ At the time of publication, AUSTRAC was considering amendments to the Enhanced Customer Due Diligence Program Rules.

- 15.9 The reporting entity must apply the enhanced customer due diligence program when:
- (1) it determines under its risk-based systems and controls that the ML/TF risk is high; or
 - (2) a suspicion has arisen for the purposes of section 41 of the AML/CTF Act.
- 15.10 The enhanced customer due diligence program must include appropriate risk-based systems and controls so that, in cases where enhanced customer due diligence is applied, a reporting entity gives consideration to whether any one or more of the following applies:
- (1) further information ought to be sought from the customer or from third party sources in order to:
 - (a) clarify or update the customer's KYC information;
 - (b) obtain any further KYC information;
 - (c) clarify the nature of the customer's ongoing business with the reporting entity;
 - (d) consider any suspicion that may have arisen for the purposes of section 41 of the AML/CTF Act;
 - (2) more detailed analysis should be undertaken in respect of the customer's KYC information;
 - (3) KYC information ought to be verified or re-verified in accordance with the customer identification program;
 - (4) more detailed analysis and monitoring should be undertaken in respect of the customer's transactions – both past and future;
 - (5) a suspicious matter report ought to be lodged in accordance with section 41 of the AML/CTF Act.

Attachment B – Item 33 designated service

Item 33 of table 1 in section 6 of the AML/CTF Act:

| Table 1—Financial services | | |
|-----------------------------------|---|---|
| Item | Provision of a designated service | Customer of the designated service |
| 33 | <p>in the capacity of agent of a person, acquiring or disposing of:</p> <ul style="list-style-type: none">(a) a security; or(b) a derivative; or(c) a foreign exchange contract; <p>on behalf of the person, where:</p> <ul style="list-style-type: none">(d) the acquisition or disposal is in the course of carrying on a business of acquiring or disposing of securities, derivatives or foreign exchange contracts in the capacity of agent; and(e) the service is not specified in the AML/CTF Rules | the person |

Attachment C: Survey of Market Participants

1. Your organisation

1. Is your organisation a Market Participant of an exchange (e.g. the ASX or the SFE)?

- Yes
- No (you are not required to complete this survey)

2. As a Market Participant of an exchange, does your organisation conduct trades for customers?

- Yes
- No (you are not required to complete this survey)

3. Approximately how many staff does your organisation employ in Australia?

- Less than 20
- 21 to 100
- 101 to 500
- More than 500

2. ML/TF risk awareness training for staff

4. Which of the following are included in your organisation's money laundering and terrorism financing (ML/TF) risk awareness training? (select all that apply)

- The circumstances that may trigger an obligation to submit a Suspicious Matter Report (SMR) to AUSTRAC
- The ML/TF risks individual staff are likely to face in their role when interacting with customers
- Vulnerabilities associated with specific products and services provided by your organisation
- Information about your organisation's transaction monitoring program
- The tipping off offence in relation to SMRs
- How to refer / escalate a potentially suspicious matter within your organisation
- The consequences under the AML/CTF Act of failing to submit a SMR to AUSTRAC

If you would like to provide additional comments or details, please do so below

5. Which of the following sources were useful in the development of your organisation's ML/TF risk awareness training? (select all that apply)

- Internal knowledge, experience or expertise
- Your organisation's ML/TF risk assessment
- Financial Action Task Force (FATF) typologies reports
- AUSTRAC typologies reports
- AUSTRAC eLearning modules
- Information on the AUSTRAC website (other than typologies reports and eLearning modules)
- External consultants
- Industry associations
- Other publicly available information (e.g. reports, media articles and transcripts of court cases)

If you would like to provide additional comments or details, please do so below

6. How does your organisation deliver its ML/TF risk awareness training? (select all that apply)

Formal face to face training sessions delivered by staff in your organisation

Formal face to face training sessions delivered by external providers

Self directed learning (e.g. online information and tests)

On the job training / mentoring

If you would like to provide additional comments or details, please do so below

3. Transaction monitoring program

7. How does your organisation monitor customer transactions?

- Staff manually monitor customer transactions
- Computer-based / automated systems monitor customer transactions
- Combination of the above two response options

8. Which of the following were useful in the development of your organisation's transaction monitoring program? (select all that apply)

- Internal knowledge, experience or expertise
- Existing processes / systems to meet other compliance obligations (e.g. required by ASIC or other government bodies)
- Your organisation's ML/TF risk assessment
- FATF typologies reports
- AUSTRAC typologies reports
- Default triggers / rules in your computer-based / automated system (if applicable)
- Other publicly available information (e.g. reports, media articles and transcripts of court cases)
- External consultants
- Industry associations

If you would like to provide additional comments or details, please do so below

9. If you have a computer-based / automated system, which of the following activities does your organisation undertake to ensure it is effective? (select all that apply)

- Validate and test triggers / rules
- Regularly review triggers / rules
- Rank alerts according to those most likely to be reported as a SMR to AUSTRAC
- Monitor the volume of alerts generated
- Assess the quality of alerts generated
- Provide feedback to staff on alerts generated

If you would like to provide additional comments or details, please do so below

4. Red flags / triggers

10. Which of the following potentially suspicious matters would be identified by your organisation?

- Doubts about the identity of the customer (e.g. the customer is unwilling to provide identification information or there are discrepancies in the information provided)
- A customer asks unusual questions about your organisation's AML/CTF policies and procedures
- A customer exhibits a surprising lack of knowledge of securities or derivatives relative to their request or trading order
- A customer cannot adequately explain the source of funds used for the transaction
- A customer has an unusually complex corporate or trust structure
- Unusual trading behaviour relative to a customer's profile or stated intentions (one-off trades or patterns of trading)
- Uneconomic trading (one-off trades or patterns of trading)
- Frequent trading activity with minimal net movement of funds
- Unexplained third party involvement
- The customer requests multiple trading accounts for no apparent reason
- Unusual use of a customer's trading account(s)
- The customer is from a foreign country of interest (e.g. subject to sanctions, has a high level of corruption, or is a tax haven)
- The customer's transactions (e.g. wire transfers) involve countries of interest
- The customer matches a name on Australia's terrorist asset freezing regime (known as the "Consolidated List")

For further information about Australia's terrorist asset freezing regime, follow the link on the following webpage:
<http://www.dfat.gov.au/globalissues/terrorism.html>

11. To what extent does your organisation consider the following to be reportable to AUSTRAC as a suspicious matter?

| | Never | Sometimes | Always | Don't know |
|---------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Insider trading | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Market manipulation | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

If you would like to provide additional comments or details, please do so below

5. Review and submission

12. Since January 2010, approximately how many potentially suspicious matters have been generated for internal review as a result of your activities as a Market Participant?

- 0
- 1 to 5
- 6 to 10
- 11 to 20
- 21 to 50
- 51 to 100
- More than 100
- Don't know

If you would like to provide additional comments or details, please do so below

13. From where in your organisation did these potentially suspicious matters originate? (select all that apply)

- Front office staff (e.g. traders, advisors and sales staff)
- Other staff (e.g. back office staff)
- Computer-based / automated systems
- Not applicable (i.e. if you selected '0' or 'don't know' in question 12)

Other (please specify)

14. If your organisation determines that an SMR should be submitted to AUSTRAC, which of the following activities are you likely to carry out? (select all that apply)

- Determine whether existing customer identification information should be updated or verified
- Determine whether additional customer identification information should be collected and verified
- Clarify the nature of the customer's business
- Conduct more detailed analysis of the customer's transactions
- Monitor the customer's transactions for a set period of time
- Determine if the customer's ML/TF risk rating should be changed
- Review your organisation's ML/TF risk assessment
- Create a written record of the investigation
- Determine if your ML/TF risk awareness training program for staff should be amended

15. Which of the following methods would your organisation use to report an SMR to AUSTRAC?

- Electronic format (i.e. through AUSTRAC Online)
- Paper form
- Don't know

16. What are the most significant issues your organisation faces in relation to suspicious matter reporting?