FINANCIAL CRIME IN THE MIDDLE EAST AND NORTH AFRICA 2017

The Need for Forward Planning

46% indicate a lack of confidence in their financial crime programs

35% indicate a lack of understanding of the regulatory environment

45% believe that justifying overall costs is the biggest challenge of program management

67% say that their technology has increased in sophistication

Deloitte.

the answer company™
THOMSON REUTERS®

TABLE OF CONTENTS

2 INTRODUCTION

4 PRESSURE TO COMPLY INTENSIFIES

7 REGULATORY GAME CHANGER

10 SENIOR LEADERSHIP – MISSING IN ACTION?

12 THE CONTINUED RISE OF TECHNOLOGY

15 SURVEY RESULTS

25 CLOSING THOUGHTS

INTRODUCTION

Welcome to our third annual report in our series of surveys on the subject of financial crime in the Middle East and North Africa (MENA) — a joint initiative between Thomson Reuters and Deloitte. This survey, run in the fourth quarter of every year, allows us to track changing norms, standards and attitudes around compliance and the management of financial crime.

The business of compliance, which in the past was seen by many as a mere tick box exercise, has become incredibly dynamic. It has evolved into a critical, demanding role that challenges executives to stay up-to-date and conversant with regional and global regulatory change and information.

The compliance role has significantly evolved over the past few years, and today's compliance professional requires a repertoire of competencies - agility, the ability to learn quickly and perform under pressure, critical thinking, highly evolved interpersonal ability and the character to manage senior leadership, and have a good head for details. Some will argue that those competencies have always been required for the job, but today more is asked of the compliance executive.

As the role grows increasingly central, they need to be able to understand the business as a whole, not just the task of compliance.

We suspect that these abilities will be rigorously tested in the coming months – while change has always been with us, it seems the compliance industry may be entering a new era of heightened turmoil as political uncertainty impacts the regulatory agenda.

At the same time, new technologies are emerging that have the potential to disrupt how we conduct international trade, on how money will flow across borders and between businesses, and how we communicate and share personal information with each other.

> "We are seeing our industry go through a revolution globally, a perfect storm of economic pressure, political change, new technology and the explosion in financial and regulatory technology – FinTech and RegTech – that is offering both opportunities and threats[1]."
>
> **David W. Craig**
> President, Financial & Risk, Thomson Reuters

This year's survey revealed a number of interesting data points. The typical responder is a compliance executive based in a financial institution that employs 1,000 or more people and has a presence in at least two or more countries.

Money laundering remains their most pressing financial crime issue. While there is a growing awareness around the issue of cyber crime, it is a subject that appears to have been neglected in previous years' studies.

Reputation remains one of the biggest concerns for executives, which has led to a surge in the application of risk assessment processes to measure progress. Although only half of the responders indicated that they obtained assurance using both internal and external parties, too much reliance on internal resources may provide a distorted representation.

We see a continuing frustration with an issue that was apparent in the first two surveys; compliance professionals caught within a conundrum – employed to manage an increasingly complex financial crime and risk compliance program, but seemingly not receiving the support of the **senior leadership** team as much as they should be.

There is a drive to improve the **sophistication** of their compliance program as a way of coping with the increased pressure, but there is a need to be able to justify the sometimes substantial costs.

Training is becoming more important as awareness grows for the need for a specific skillset that will be able to deploy changing technology, ever increasing in terms of sophistication, to its full potential.

Organizations are tackling the compliance challenge with a combination of technology, training and the reorganization of processes.

We identified four specific trends to examine in more detail:

- Pressure to comply intensifies
- Regulatory game changer
- Senior leadership - missing in action?
- The continued rise of technology

83%
HAVE AN AML PROGRAM IN PLACE

[1] *'How the US election will impact the world of financial regulation', Thomson Reuters, 11 November 2016*

PRESSURE TO COMPLY INTENSIFIES

Responses to questions about financial crime programs illustrate the ongoing and ever increasing pressure on organizations to comply with both local and international regulation.

Question 8 and 9, for example, address investment in compliance activity designed to combat financial crime and, as expected, point to a continuing upwards rise of compliance spend. 65% of respondents indicated that their compliance investment had increased over the past 2 years, while 63% indicated that they expected investment to continue to increase over next 2 years; a substantial jump from last year's figures of 52%.

It is interesting to contrast these findings to another recent report – The Cost of Compliance 2016 – that shows a slowing down of compliance spend worldwide, isolating the Middle East and Asia as the only two regions where compliance spend is increasing.

For MENA-based organizations, this may be partly explained by an apparent lack of confidence in programs, revealed by responses to **question 18**: 'How confident are you that your financial crime prevention program is compliant with domestic and international regulatory requirements, and that it prevents illicit activity?' A substantial number of respondents, 44%, indicated a lack of confidence in their programs.

WHERE IS THE MONEY GOING?

As in previous years, participants were asked what financial crime programs their organization had in place. AML programs remain the priority for organizations, with 83% of respondents choosing this program.

We noted a small uptake in fraud programs, which are well represented at 76%. Most regional banks have long established separate functions for management of fraud and AML, and fraud tends to be well supported at a senior management level due to the direct financial impact on the bottom line, rather than the impact of reputational loss. In contrast, the financial impact of an anti bribery and corruption (ABC) or counter-terrorist financing (CFT) program failure can be harder to calculate.

The number of ABC programs has dropped by 4% to below 60%, reflecting relatively low support in comparison to other programs. This may be due to the fact that ABC continues to be seen as a regulation focused on the corporate sector. While some global and regional banks may have separate defined policies on ABC, in many financial services this activity is often rolled up with other compliance activities.

From a systems and processes perspective, many banks are also able to link the technology that supports their AML and fraud programs, but are not able to do this with ABC and CFT programs, mainly because both rely less on technology and more on the human capacity to provide detailed analysis.

There is a slight increase in the number of respondents claiming a sanctions program, in keeping with other research conducted in recent months. Perhaps compliance officers heeded the advice of authorities not to drop their guard following the relaxation of certain sanctions against Iran under the Joint Comprehensive Plan of Action (JCPOA). From past experience we know that when sanctions are about to be lifted, individuals within the country who have exploited the restricted trading environment to their benefit may attempt to transfer their ill-gotten gains outside of the country's borders, in an attempt to hide their inexplicable wealth. It is therefore not a time to decrease compliance procedures — quite the opposite.

It is a complex situation that requires a cautious approach. Should an organization fail to comply with the existing sanctions requirements, they may be subject to sizeable fines and even criminal penalties.

There is also the possibility of a U.S. government 'snapback', triggered by a failure on Iran's part to honour the deal or by a change of direction by the U.S. government. Should a snapback be triggered, organizations that have engaged in trade activities within Iran in the interim will be compelled to take action, albeit over a 180 day wind down period.

Should this occur, any existing trade relationships with Iran that were initiated in the interim will come under pressure, so organizations that have initiated relationships with Iran-based organizations, or that plan to, should have safety measures in their contracts to protect them should the agreement suddenly pose a sanctions breach.

86%

OF RESPONDENTS ARE CONCERNED ABOUT CYBER CRIME

CYBER CRIME SPIKES

We see a growing awareness of the need for increased cyber security, with the number of cyber crime programs spiking by 10% in comparison to last year's results. In last year's report we stated that compliance officers should take very careful precautions to ensure that their customer data is well protected given the surge in the level of cyber crime.

There was concern that not enough attention had been given to the issue, and we are encouraged to see that there is a definite swing towards cyber security in terms of resources, especially in light of a report[2] earlier this year that stated that businesses in the Middle East were experiencing high levels of cyber crime related incidents in comparison to the global average.

[2] *A false sense of security? Cybersecurity in the Middle East, PWC.com, March 2016*

Cyber crime looks set to become an increasingly challenging and critical issue for business leaders; one that will require a cautious and comprehensive approach if its risk is to be effectively mitigated.

As the task of cyber security expands, we expect to see a shift of that responsibility from the IT department to the compliance department.

In particular, cyber crime poses a high threat to business continuity, and a breach of IT security could have significant implications for an organization, including sizeable reputational damage.

Featured Questions: 8, 9 and 18

Full survey results can be found on pages 17 to 26

While reports of cyber attacks continue to increase, cyber security does not appear to be keeping up. There is less of a regulatory incentive compared to other types of financial crime. Cyber crime regulation is difficult to enforce, and because compliance executives are always under such pressure to meet their regulatory obligations, other more pressing financial crimes will be prioritized.

It cannot be ignored for much longer, however, given the rising volume of cyber attacks on organizations in the MENA region, as well as increasing data privacy rules and regulations that will require attention from compliance executives.

While the process of upgrading technology can be costly, it represents a good opportunity to build security features into the system, thus increasing efficiency and the effectiveness of the online protection. Deloitte's 'Tech Trends 2016: Innovating in the digital era[3]' advises on increasing security in three stages:

- 'Secure: Start with tactical steps to create highly virtualized, templated stacks. This establishes a sound, standards-based way to build cyber security into the fabric of the IT environment, with infrastructure automatically inheriting patches, configurations, and cyber-solution elements.
- Vigilant: Build a cohesive monitoring/threat intelligence platform that makes it possible for IT to establish operational baselines. Then, from a cyber security standpoint, determine what "normal" looks like for user behaviour, server loads, data exchange, access, and external connectivity. Understanding what normal is can help IT identify elevated risk situations when they occur and react accordingly.
- Resilient: Is your environment safe enough to restore normal operations following an attack? If the answer is "no," you have a problem. If the answer is "I don't know," you have a bigger problem. Proactively create plans for recovering from various attack scenarios, test them often, and be sure to incorporate lessons learned back into your operational plans to further accelerate detection and reduce impact in the future.'

[3] *Cyber Implications 'Tech Trends 2016: Innovating in the digital era', Deloitte, 2016*

REGULATORY GAME CHANGER

Following decades of steadily integrating regional economies, we are now facing the prospect of 'reverse globalization'. Driven by a desire for protectionism, concerns about data privacy, a rise in economic nationalism and concerns over physical security in the face of a growing refugee crisis, this sudden change of economic direction has taken many people by surprise.

This high level of uncertainty in the global political order affects the regulatory agenda and it is inevitable that there will be an impact on MENA-based organizations.

In the U.S., it is likely that certain leading risk regulatory policies will be revoked, and for the first time since the growth of regulatory compliance in the early 2000's, we may be facing the possibility of a regulatory roll back. At the same time, European governments are trying to understand the consequences of Brexit while facing the prospect of further fragmentation of the EU, as other member states go to the polls this year.

Such is the state of political flux there would be very few brave enough to predict what the regulatory environment will look like in a year's time. What we can say, however, is that it is likely that the regulatory environment will grow even more complex.

Despite election campaign promises, we cannot be sure what U.S. laws will be repealed, if any, and we may find that other laws are upgraded as the war on terror intensifies. While the U.S., along with the UK, has certainly led the regulatory push against corruption and threat financing for many years, other countries have now joined the fray by instituting hard hitting regulations. We therefore do not expect that the volume of regulatory compliance will be on the wane any time soon.

OVERWHELMING FLOW OF REGULATORY UPDATES

In the midst of this regulatory turmoil, the flow of regulatory information has become overwhelming.

> "The increase in regulatory change symbolizes this trend. When we started tracking regulatory changes in financial services, we were collecting 10 changes a day from 100 regulatory bodies; that number is now almost 200 per day from 600 regulatory bodies around the world."
>
> **David W. Craig**
> President, Financial & Risk, Thomson Reuters

We see the impact of regulatory uncertainty, as well as the constant changing flow of regulator information, on compliance executives. Many lack confidence in their processes and, critically, they are unsure if their programs are meeting the requirements of their compliance obligations.

We can see from responses to **question 19**, which asked the main reasons for a lack of confidence in programs, that over a third of respondents indicated their lack of understanding of the regulatory environment was an issue, with 22% pointing to the overwhelming pace and complexity of regulatory updates.

In **question 18**, participants were asked how confident they were that their financial crime prevention program is compliant with domestic and international regulatory requirements, and that it prevents illicit activity. Although we see an improvement on last year's results, a significant number of respondents indicated a lack of confidence in their programs – 44%.

Responses to other questions also indicate a lack of confidence. For example, asked what they believed to be the key concern in terms of financial crime and compliance in **question 13**, a third indicated compliance with international and local regulation to avoid censure.

Question 14 asked what, in their opinion, poses most risk to their organization, 37% indicated a failure to meet regulatory requirements, and another 13% replied failure to take proper action to find risk that is hiding in your database, which reflects a concern about failing to meet regulators' expectations.

STICK TO BASICS

These responses appear to reflect an anxiety among a substantial number of respondents about meeting regulatory obligations, as well as a lack of regulatory insight and guidance. This means that their organization could be exposed to significant risk of a compliance failure.

The compliance role has always been a challenging responsibility, but with the uncertainty of today's global political order and its potential impact on the regulatory environment, it has never been so demanding.

Unfortunately there is little the compliance executive can do to influence the external environment, but what they can do is focus on ensuring that they have the basic building blocks of a best practice compliance program.

There are certain core elements that will serve the compliance function, and the organization at large, regardless of the political and economic storm.

37% BELIEVE THAT FAILING TO MEET REGULATORY REQUIREMENTS IS A MAJOR RISK

Tone at the top — The starting point for any world-class ethics and compliance program is the board and senior management, and the sense of responsibility they share to protect the shareholders' reputational and financial assets.

The board and senior management should do more than pay "lip service" to ethics and compliance. They need to empower and properly resource the individuals who have day-to-day responsibilities to mitigate risks and build organizational trust.

Corporate culture — A culture of integrity is central to any effective ethics and compliance program. Initiatives that do not clearly contribute to a culture of ethical and compliant behaviour may be viewed as perfunctory functions instilling controls that are impediments to driving the "value change" of the enterprise.

Risk assessments — Ethics and compliance risk assessments are not just about process—they are also about understanding the risks that an organization faces. The risk assessment focuses the board and senior management on those risks that are most significant within the organization, and provides the basis for determining the actions necessary to avoid, mitigate, or remediate those risks.

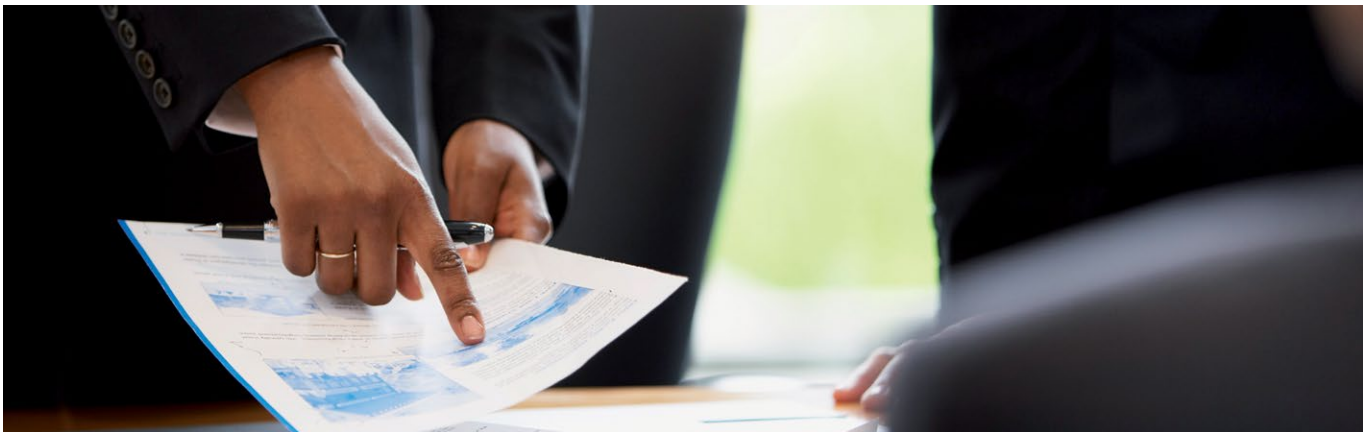
The Chief Compliance Officer (CCO) — The CCO has day-to-day responsibility for overseeing the management of compliance and reputational risks, and is the agent for the board's fiduciary obligations in this regard. A skilled CCO can create a competitive edge for their organization.

Testing and monitoring — A robust testing and monitoring program can help ensure that the control environment is effective. The process begins with implementing appropriate controls, which should be tested and ultimately monitored and audited on a regular basis.

'Building world-class ethics and compliance programs: Making a good program great', Deloitte, 2015

Featured Questions: 13, 14, 18 and 19

Full survey results can be found on pages 17 to 26



SENIOR LEADERSHIP – MISSING IN ACTION?

There has been a recent discussion amongst compliance professionals about how the compliance function had moved from a back office function to the middle office and is now, for the more progressive or mature organization, increasingly seen as a front office function. This shift is being driven in part by recent regulatory updates such as The Markets in Financial Instruments Directive (MiFID) II.

Unfortunately responses to certain questions reveal that many compliance officers are still struggling with what they perceive as a lack of support from senior management. This has been a constant theme since we began this study in 2014.

In **questions 10 and 11** for example, respondents were asked about increased levels of anti-crime and compliance activity and awareness, and to provide a retrospective and prospective view of how it was manifesting within the organization. **Question 10** asked how it had manifested over the past two years, while **question 11** asked about expectations of how it would manifest in the next two years.

In both instances, the option of an increased flow of communication from management to staff, a key element of an appropriate culture of compliance and essential for providing the right tone from the top, was bottom of the list, above only 'there is no difference' or 'don't know'.

It seems that, from replies to both questions, the emphasis in most organizations is firmly on the introduction of new processes as a way of alleviating management pressure.

Other popular options include choosing to increase training levels, as well as redirecting more personnel hours to regulatory compliance and spending more time monitoring regulatory updates and change.

Active communication from senior management with the rest of the staff, as a method of raising awareness of the importance of compliance, seems not to be a priority for many senior managers.

Respondents were asked in **question 19** that where there is a lack of confidence in financial crime programs, what they believe could be the possible causes. Most pointed to a lack of senior management support as their main concern.

When asked, in **question 15**, what they saw as the biggest challenge to managing the various programs of a financial crime and compliance policy, the most commonly chosen answer was 'Justifying the overall costs associated with the program, including technology', again pointing to a perceived lack of support from business leaders. Other commonly chosen answers to that question included 'Securing support from key business leaders'.

THE RIGHT CORPORATE CULTURE IS ESSENTIAL

The need for senior management support for the compliance function is not a message that appears to be filtering through to many business leaders. Perhaps there is a lack of communication or a sense of complacency, or perhaps fewer financial institutions or corporations in MENA have yet to suffer any real sanction for a relatively minor transgression, as their counterparts have in more established financial centres. What we do know, however, is that regulators now expect and look for an appropriate compliance culture when inspecting the governance of an organization, and culture within an organization is driven by leadership. Whilst 'culture' is a subjective term, and may seem unquantifiable to some, there are checks that regulators perform to assess if there has been any meaningful effort to pursue the right level of compliance culture.

In January 2016, America's Financial Industry Regulatory Authority (FINRA) defined what they meant by compliance culture: "set of explicit and implicit norms, practices, and expected behaviours that influence how firm executives, supervisors and employees make and implement decisions in the course of conducting a firm's business."[4]

The regulatory body said that, in assessing institutional compliance, they would look for evidence that compliance and risk are valued within the organization. Specifically, they would look to see if a compliance officer or department had the 'attention of the board or senior management', do they have the budget and staff to do an adequate job, and if there is any evidence of 'clear lines of communication to the very top of firms'.

SENIOR MANAGEMENT SUPPORT IS VITAL

Clear boundaries and regular demonstration of ethical behaviour, as well as visible support for the compliance department, from the top management are essential for the creation of a culture of compliance. Such behaviour very much assists other organizational stakeholders to take their compliance obligations seriously, as well as demonstrating to authorities that an organization is serious about risk control.

Given the complexity of the regulatory environment, as well as the frequency of regulatory updates and the volume of transactions, it is simply not possible to conduct due diligence or monitor each transaction. Hence regulators look to see if the organization has an appropriate response to the compliance challenge. Should there be a compliance failure and there is a lack of evidence of senior management support for compliance, executives may be held individually responsible. A lack of senior level support can also impact the task of attracting and maintaining a sufficient skills base within the organization, especially in a time of growing focus on individual accountability. Due to the extent and velocity of regulatory change, compliance skills require constant development and frequent updating. Senior managers will understand the difficulty of finding people with both the appropriate qualifications and experience.

We are seeing evidence that compliance professionals are increasingly cautious when choosing roles within organizations, and are seeking placements where there is active and visible support for the compliance function. In an era of increasing transparency and individual accountability, compliance personnel are choosing to work for a company where their input will be valued and they are not at risk of losing their positions because they are in constant conflict with senior management. It is the responsibility of the Chief Compliance Officer to educate all members of staff about their compliance responsibilities, including board members and senior management, but should they encounter resistance at this level, it will render the compliance function dysfunctional. It is not surprising, therefore, that an ambitious compliance professional may be very cautious when accepting a new position and will want to know that the senior management team understand the significance of their support.

A lack of experience and skill set within an organization may very well have a cyclical affect, frustrating other talented and capable managers and causing them to seek opportunities elsewhere.

Featured Questions: 10, 11, 15 and 19

Full survey results can be found on pages 17 to 26

[4] *IMPACT ANALYSIS: Defining "culture of compliance" is key to this year's FINRA exams, Jan 14 2016 T Ehret, Regulatory Intelligence*

THE CONTINUED RISE OF TECHNOLOGY

We note the continuing trend in investment in technology as a means of fighting financial crime. While the use of technology to simplify the complexity of the various compliance challenges has long been commonplace, the focus has become the level of sophistication of that technology, with the majority of respondents, 67%, indicating in question 22 that they have increased the level of sophistication of their technology over the past two years.

The sheer volume of information that organizations are required to process, analyse and report on requires a robust and intelligent solution, one that will meet current and future needs if the compliance department is to meet regulators' expectations. A substantial system transformation, however, can be a costly exercise, so before any investment is committed to, a needs assessment conducted by a specialist external agency may be worthwhile to ensure that the analysis is addressing the appropriate issues. Choosing the most expensive and cutting edge technology may not provide the relief that is being sought, it's about the best fit rather than the most sophisticated.

We see, for example, that despite the trend towards increased sophistication in technology in previous reports, there is no corresponding upward trend in reported confidence levels in financial programs or in technology. Asked in **questions 18 and 19** how confident they were that their financial crime programs were achieving their goals and if their technological solutions were operating as required, their responses were almost identical to last year's. It may be that it will take some time for confidence levels in technology solutions to increase based on the quality of output, perhaps additional or new assurance processes are required, or there may be a need for a change of focus.

> "Expanded use of innovative technologies and processes—including cognitive technologies and robotic process automation—can boost effectiveness making it more of a proactive approach, while simultaneously reducing costs."
>
> **Bhavin Shah**
> Partner | Financial Advisory
> Deloitte Corporate Finance Limited

THE NEED FOR BETTER DATA MANAGEMENT

Responses to **question 24** illustrate the desire amongst many senior executives for better data management and analytical capabilities. This is not surprising given the continuous upward regulatory pressure on compliance departments, nor is it confined to executives in MENA. A recent Deloitte UK research report[5] reveals a high number of financial services executives, 65%, believing that data quality is a 'significant problem' for their organizations. This figure rises to 82% when executive commitment to improving data management was viewed to be lacking.

Obtaining 'good quality data' has become an issue of our time – the need to not only produce actionable, credible intelligence from constant streams of information, but to produce the kind of intelligence that instantly builds a picture of risk; one that is easily translated into board and management reports as well as company-wide memorandums, and that brings all stakeholders to the same point of awareness.

In the past, much of the decision making around risk management solutions has tended to be reactive rather than proactive, with the focus on improvements in investigating alerts and reporting systems, or basic KYC/onboarding, screening and monitoring processes. Now that we are in a time of increasing collaboration between international regulatory bodies as well as higher expectations from domestic regulators and substantial fines, we may start to see an investment shift towards a more proactive technological approach to fighting crime and uncovering risk, for example the use of powerful analytics that will profile consumer behaviour and provide an early warning system.

Given the constant upward pressure from regulators and consumer expectations, as well as the increasing digitization of financial services, it is inevitable that technology will play an expanded and central role in compliance. This may, however, necessitate extensive system changes from existing IT infrastructure to facilitate the required level of transparency demanded by both regulators and public sentiment. Although costly, changing systems presents an opportunity to more closely integrate the compliance function with other processes, thus allowing for the streamlining of systems and a more efficient use of resource allocation. It is also an opportunity to uncover organizational and technological vulnerabilities and address any shortfalls before an emergency occurs, such as a technology failure or a cyber attack. It is an exercise, therefore, that is useful in improving business competitiveness and reducing overall risk beyond the compliance function.

89% EXPECT THEIR TECHNOLOGY TO BECOME INCREASINGLY SOPHISTICATED

HAVE WE GOT THE SKILLS TO MATCH?

While the focus is on increasing the level of sophistication, we wondered about the availability of skills. Without the right skillset, returns on investment in technology may not be realised to its full potential. In **question 15**, we noted that respondents were concerned about justifying compliance costs in the future – and given that the biggest obstacle to investment in technology, as revealed by **question 25**, is cost, their existing investment in technology needs to increase the effectiveness and efficiency of output to justify its expense.

Where past survey reports have indicated that investment in skills has lagged behind somewhat, although still not the first choice we see in answers to **questions 10 and 11** a definite uptake in training and skills investment.

[5] *Data quality, reporting and valuation, 'Tackling too-big-to-fail: The resolvability challenge for banks'; Centre For Regulatory Strategy, Deloitte, 2016*

In **question 12**, which asked respondents what they saw as the main focus of investment to meet compliance objectives. Training was rated a close second after technology, an improvement on last year's survey when training was rated third in terms of investment priorities, after technology and processes. This may reflect a growing awareness for the need for a human element in managing financial crime programs and the requirement of sound judgement as a first line of defence. In reply to **question 25** – 'What, in your opinion, is a major disadvantage of using sophisticated technology in a financial crime program?' – the second most favoured response, after cost, was over-reliance on technology.

While it seems that for many sophisticated technology will become more necessity than choice in compliance, it would be a mistake to prioritize technology over human judgement. Technology can be a powerful aid, but when it comes to uncovering risk, it is the interaction between smart technology and human intelligence that delivers best results.

Featured Questions:
10, 11, 12, 15, 18, 19, 22, 23, 24 and 25

Full survey results can be found on pages 17 to 26

The increasing need for IT skills outside of the IT department

Given the demand for technological sophistication and innovation, it may be wise to conduct an audit of IT skills within various departments and at a management level, to understand the current skills base.

It is useful to have key skills at senior management level and not to rely on internal IT specialists to provide an understanding of the various challenges.

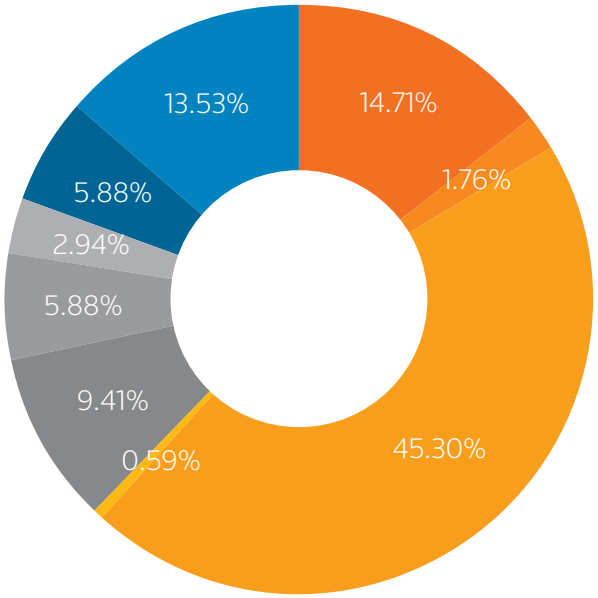
IT skills at a senior management level can be particularly useful in steering the compliance function towards the best fit of technology solution. There is no 'one-size-fits-all' solution to financial crime and compliance, nor is it likely there any 'off the shelf' solutions will be suitable without modification or alignment with existing financial intelligence systems and processes. Management teams will require the skills and capacity to make the most fitting choice according to their organization's unique context, which often may require modification to fit the purpose. Regular assessments also help to ensure that the solution continues to fulfill its mandate, so it is practical to have the necessary skills at a high level.

Senior executives and board members will be well served with a good understanding of the IT skills requirement. We expect that regulators may soon begin to look for this inbuilt capacity at a board level - following a number of systems failures at various banks in 2015. For example, the UK government Treasury Committee published a few suggestions that included ensuring that there is greater IT expertise at board level.

There is little doubt that the trend towards increased sophistication will continue. Close to 90% of respondents in **question 23** indicated that they foresaw the need for increasingly innovative and sophisticated technology to help with the overwhelming task of compliance in the future. For organizations with an existing skills deficit at a senior leadership level, it may be good to begin planning how best to address this.

SURVEY RESULTS

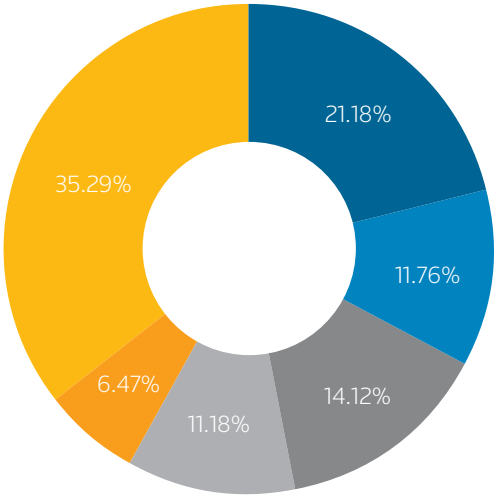
Question 1: To begin, please indicate which of the following best describes your role?



Role descriptions

- Senior management at C-suite level
- Board member
- Risk / AML / compliance / financial crime function
- General counsel
- Internal audit function
- Finance function
- IT function
- External consultant
- Other

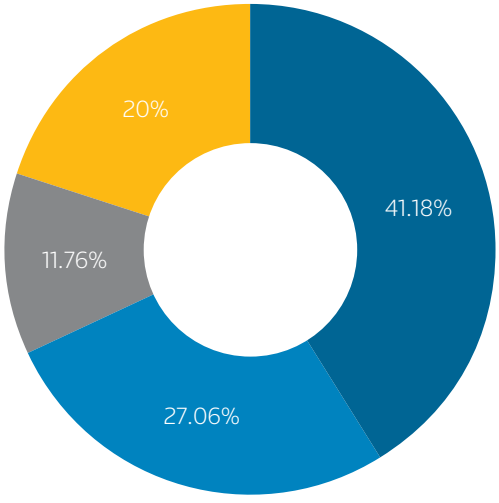
Question 2: Please indicate the number of employees your organization employs within MENA?



Number of employees

- Less than 25
- 25-100
- 101-250
- 251-500
- 501-1000
- 1000+

Question 3: How many countries within MENA does your organization operate?

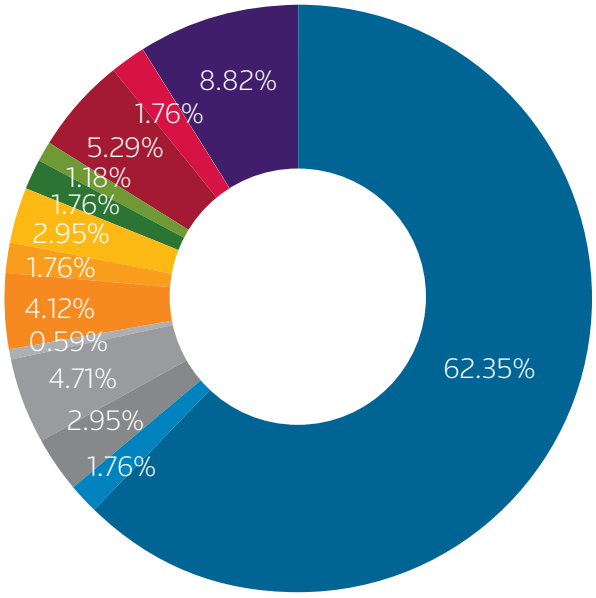


Number of countries

- Has a presence exclusively in one country
- Has a presence in 2–5 countries
- Has a presence in 6–10 countries
- Greater than 10 countries

SURVEY RESULTS (CONTINUED)

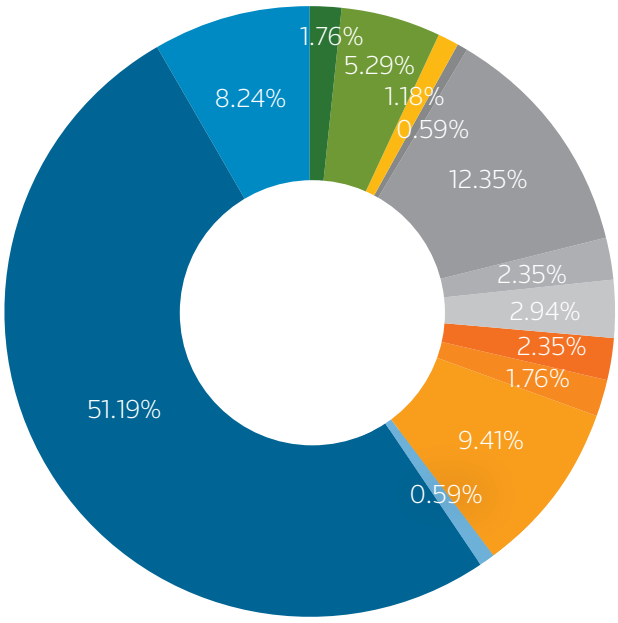
Question 4: Please indicate the primary industry in which you operate.



Primary industry

- Financial Services
- Healthcare
- Retail
- Government
- Charity/Not For Profit
- Oil and Gas/Energy
- Construction/Engineering
- Media
- Transport and logistics
- Legal
- Consultancy
- Manufacturing
- Other

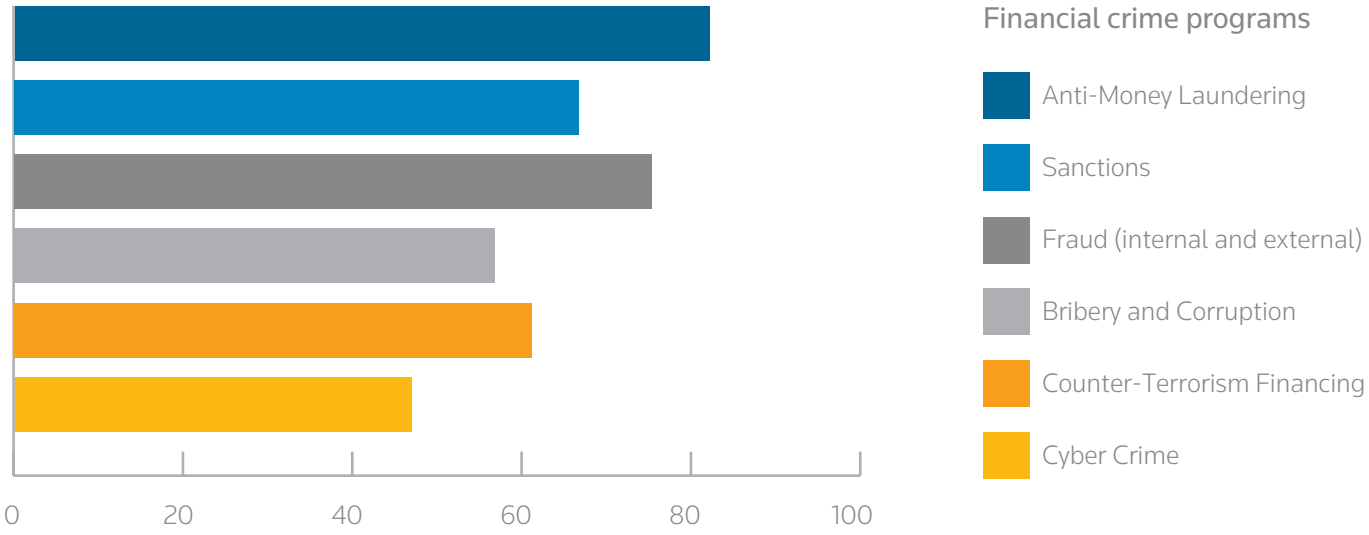
Question 5: In which country are you based?



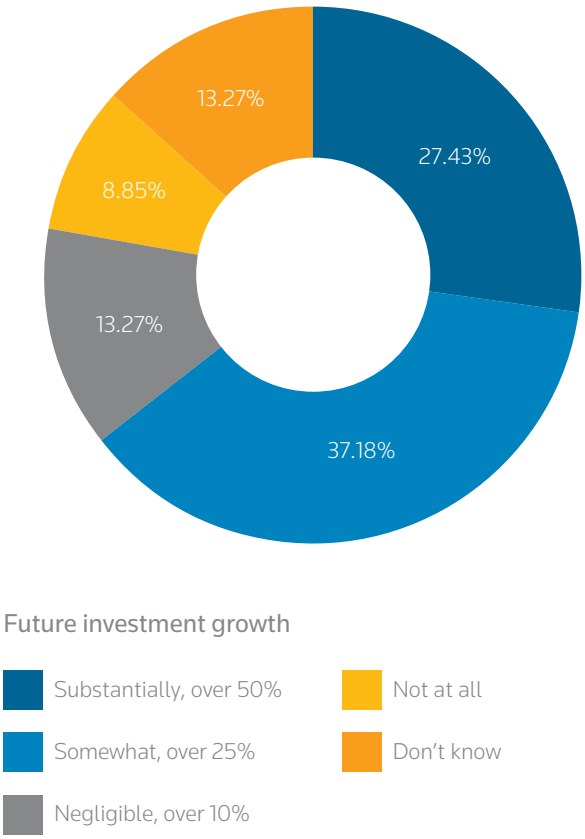
Countries

- Algeria
- Bahrain
- Egypt
- Jordan
- Kingdom of Saudi Arabia
- Kuwait
- Lebanon
- Morocco
- Oman
- Qatar
- Tunisia
- United Arab Emirates
- Other

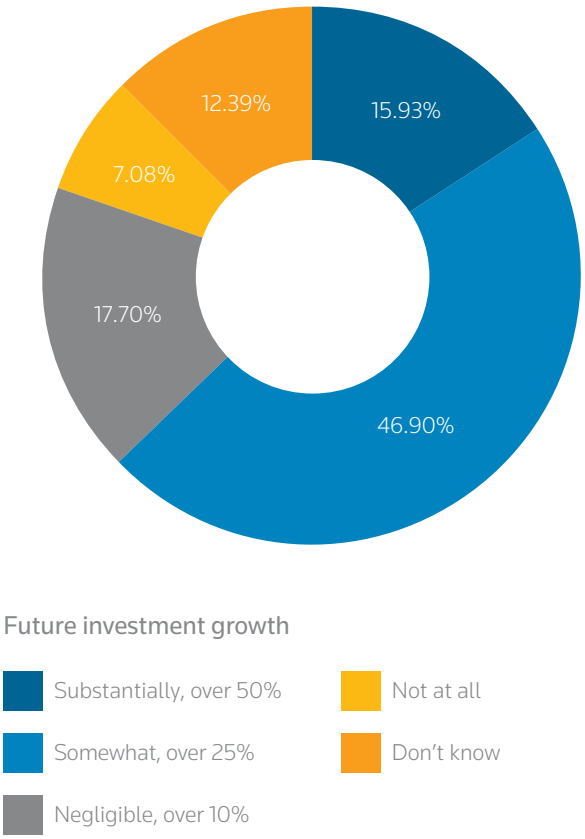
Question 6: Which of the following financial crimes programs does your organization currently have in place?



Question 8: How has your investment in anti-financial crime activity and compliance increased compared to two years ago?

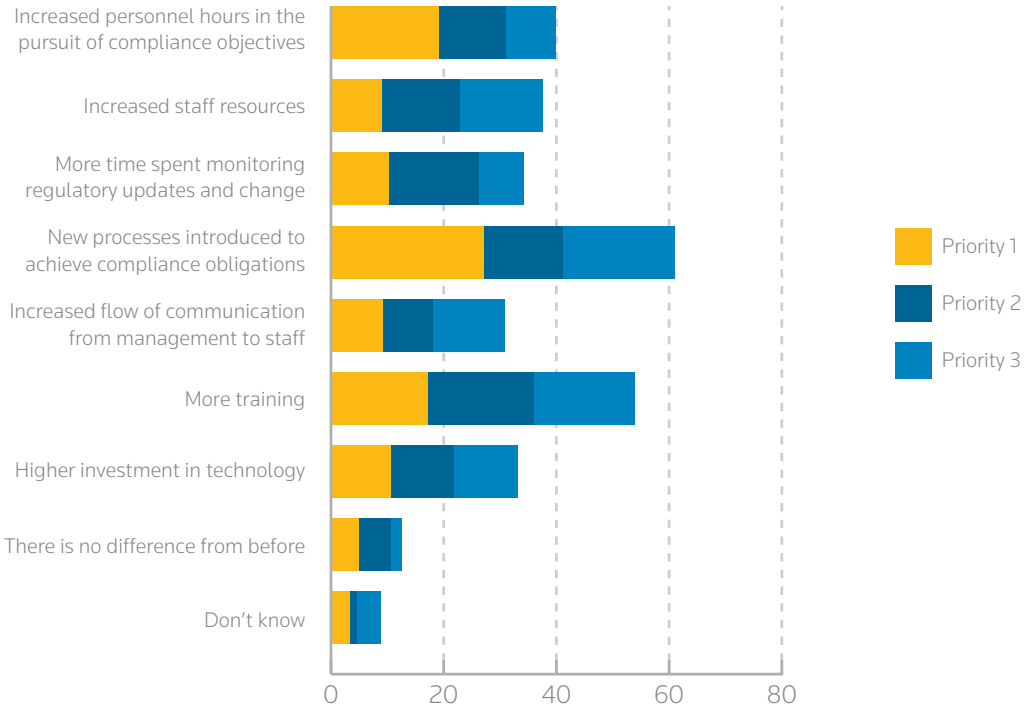


Question 9: Do you anticipate an increase in your anti-financial crime activity and compliance investment over the next two years?

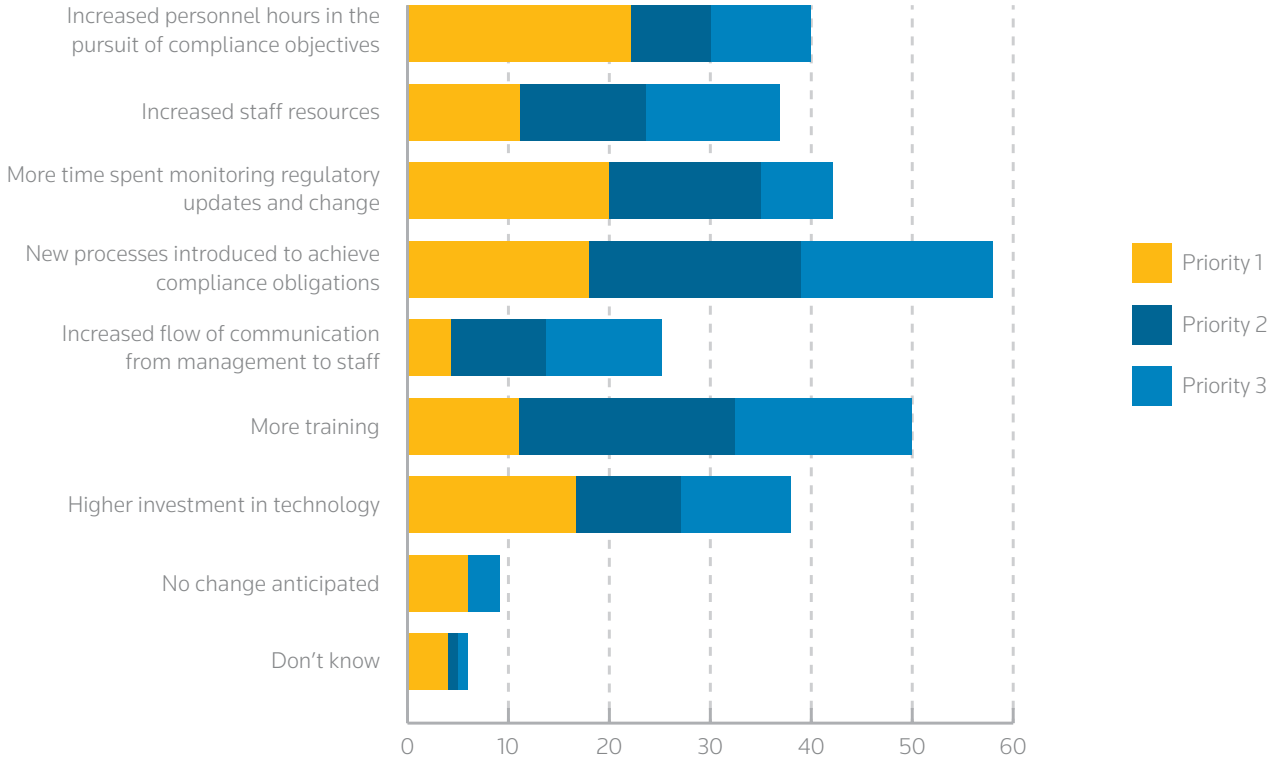


SURVEY RESULTS (CONTINUED)

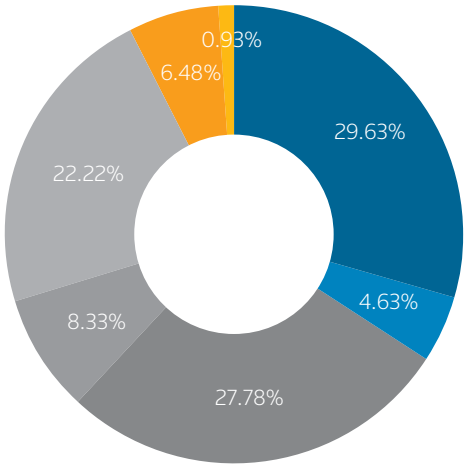
Question 10: How has increased anti-crime and compliance activity and awareness in your organization manifested in the past two years?



Question 11: How do you expect an increase in anti-crime and compliance activity and awareness to impact your organization in the next two years?



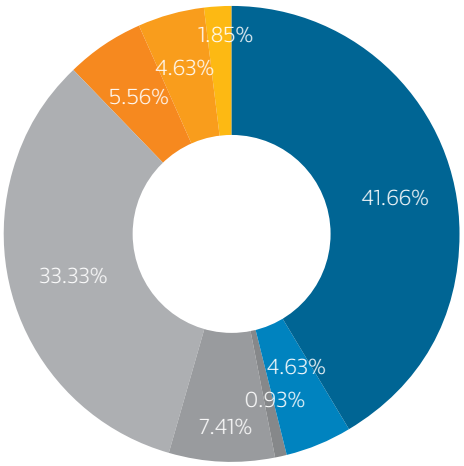
Question 12: Where is the main focus of investment to meet compliance objectives in your organisation?



Investment focus

- Technology
- Outsourcing compliance skills
- Training (compliance department and wider business)
- Regulatory intelligence
- Processes – internal business change and reorganization
- Recruitment
- Other

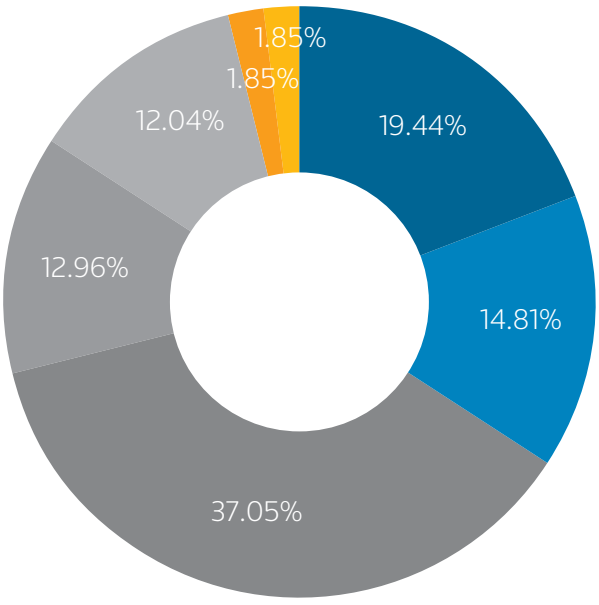
Question 13: In your organization, what do you believe is the key concern in terms of financial crime and compliance?



Investment focus

- Protection of the organization's reputation
- Impact on customer retention
- Slowdown of customer onboarding
- Unwittingly facilitating an illegal act
- Complying with international and local regulation to avoid censure
- Delay in achievement of business goals and objectives
- Meeting customer expectations
- Other

Question 14: What, in your opinion, poses the most risk to your organisation?

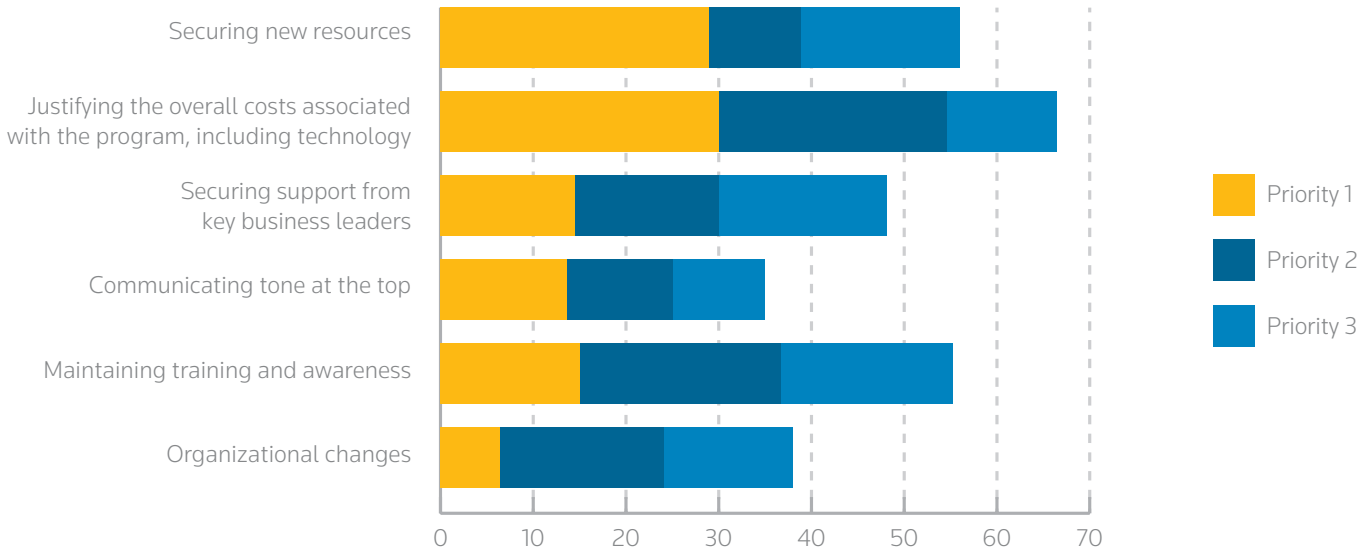


Risk areas

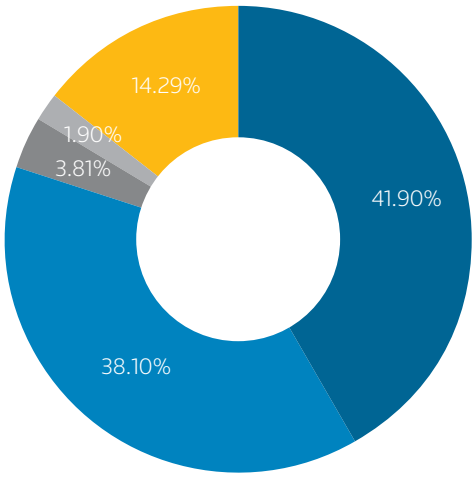
- Failure to reach business objectives
- Failure to live up to customer expectations
- Failure to meet regulatory requirements
- Failure to take proper action to find risk that is hiding in your database
- Unwittingly facilitating an illegal act
- Potential class action
- Other

SURVEY RESULTS (CONTINUED)

Question 15: Over the next two years what do you believe will be the biggest challenge in managing the various programs of your financial crime and compliance policy?



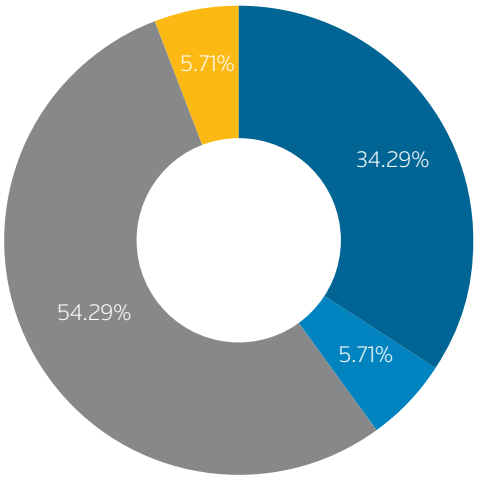
Question 16: How regularly do you assess the risks that financial crime poses to your organization?



Frequency

- Two to four times a year
- Once a year
- Once every two years
- Once every two to five years
- Not on a regular basis

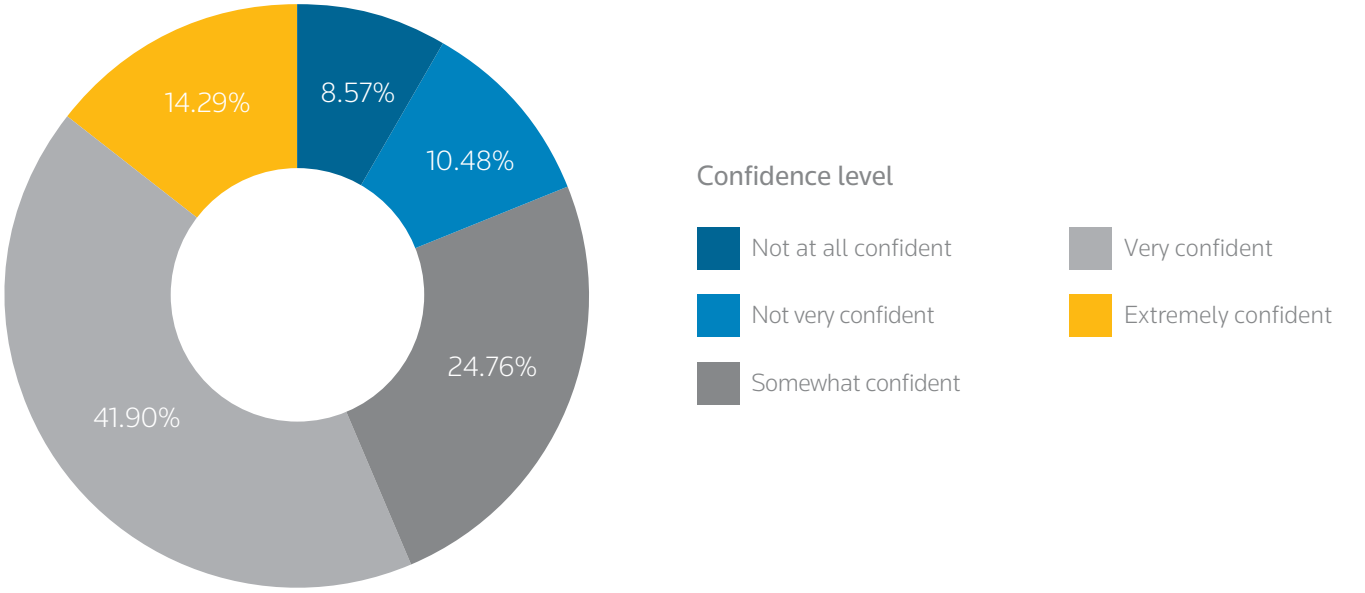
Question 17: How do you monitor and assure your financial crime program?



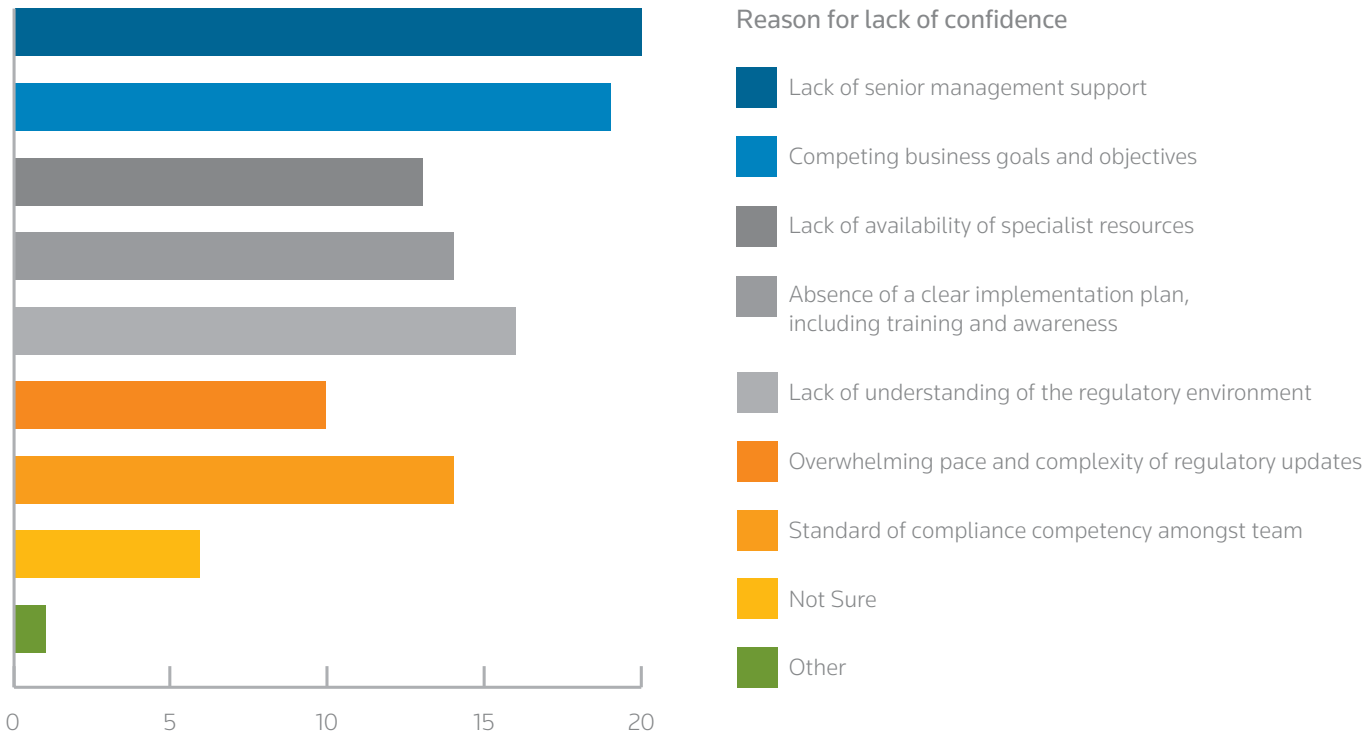
Monitoring processes

- Internal functions, such as internal audit and other internal control functions
- External functions, including external audit and independent consultants
- Combination of internal and external functions
- No formalized assurance process in place

Question 18: How confident are you that your financial crime prevention program is compliant with domestic and international regulatory requirements, and that it prevents illicit activity?

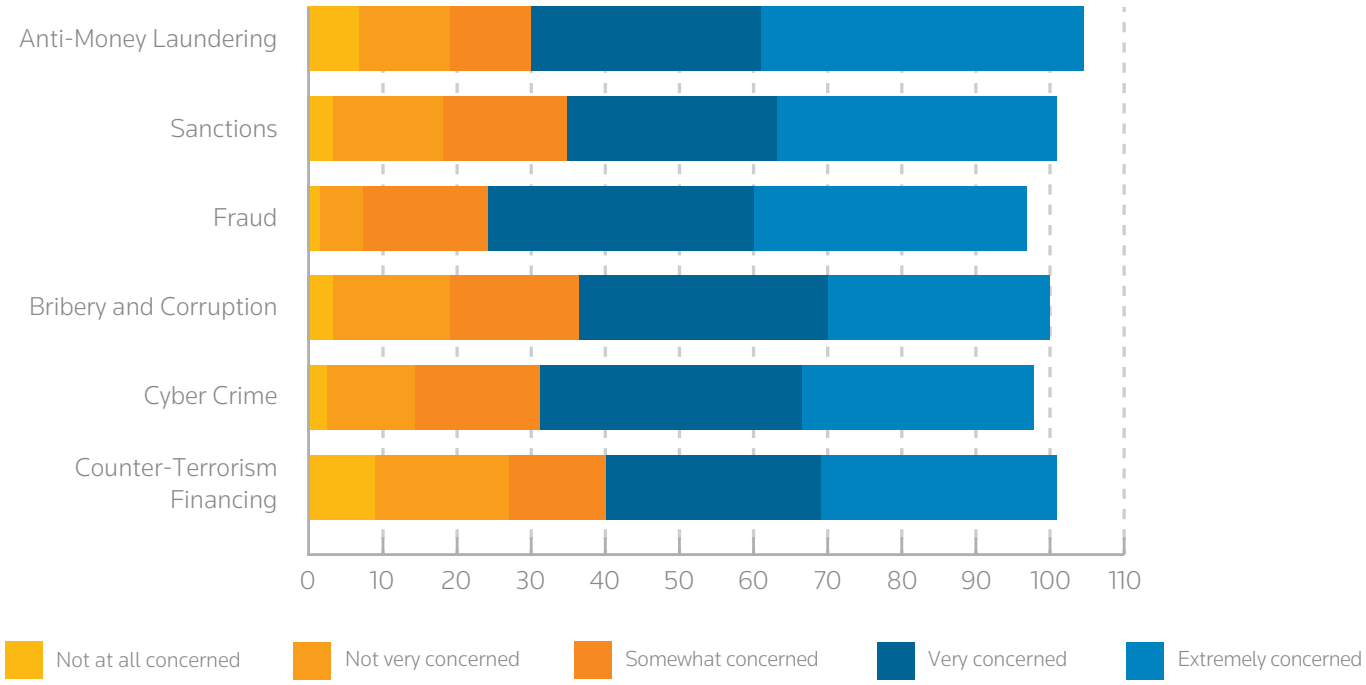


Question 19: Where there is a lack of confidence in your financial crime program, what are the main reasons?

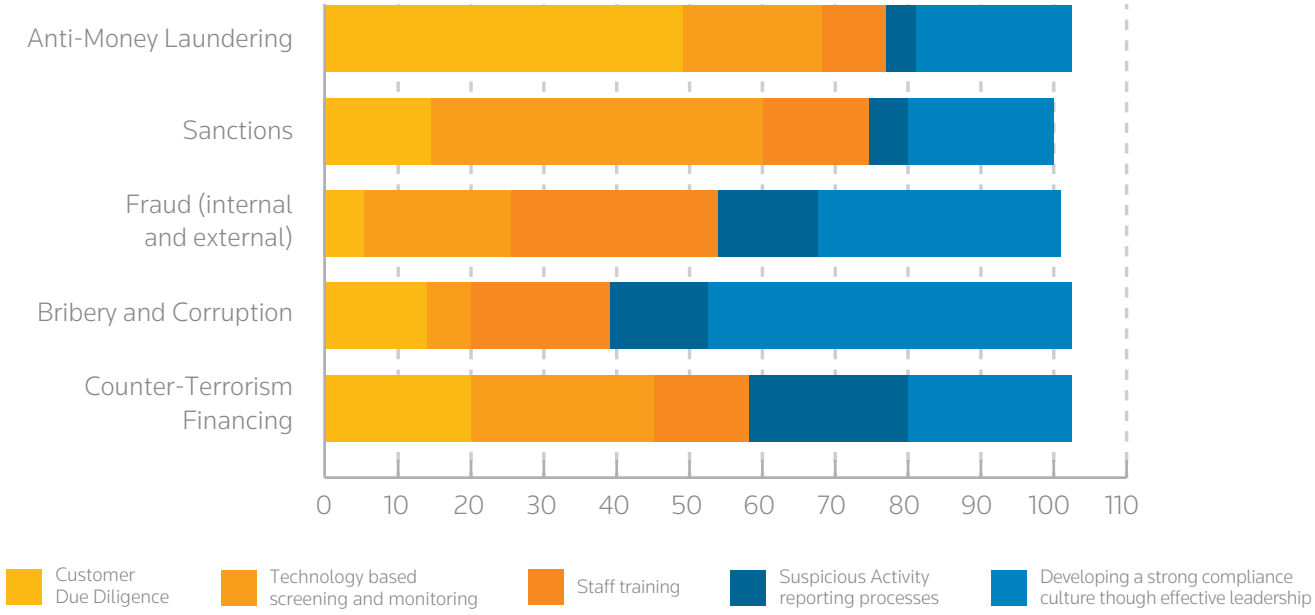


SURVEY RESULTS (CONTINUED)

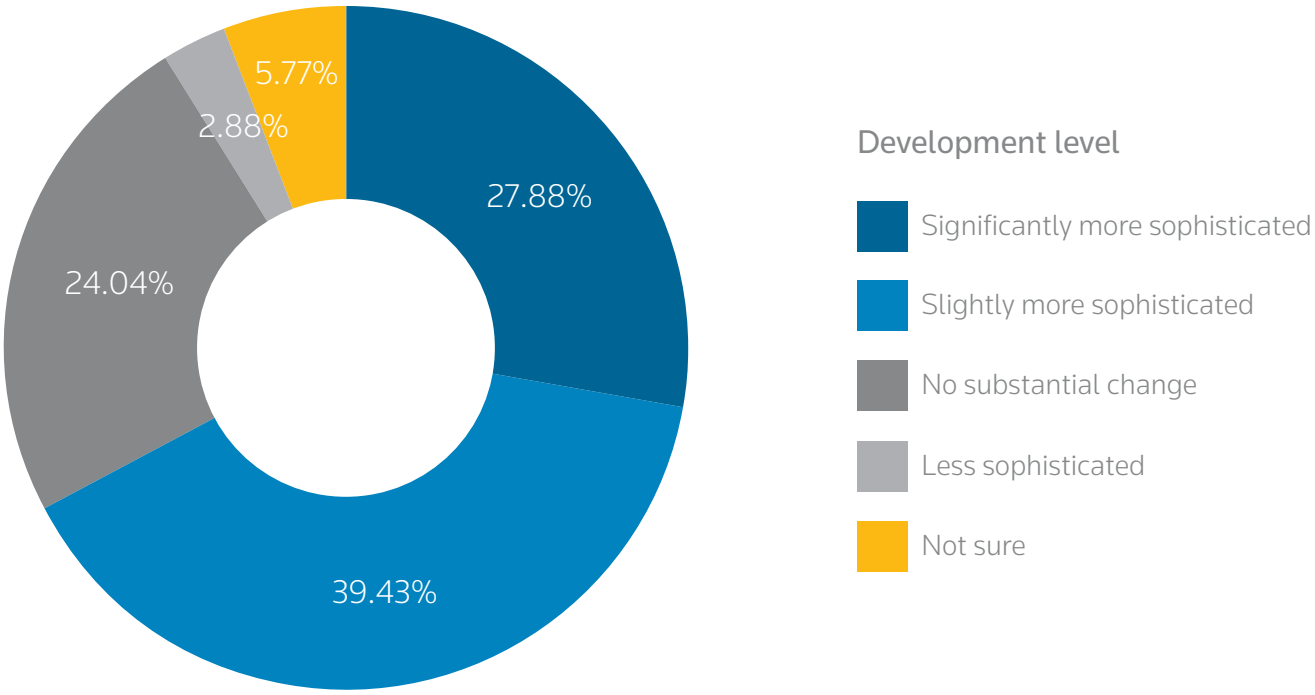
Question 20: How concerned are you with the following financial crime issues?



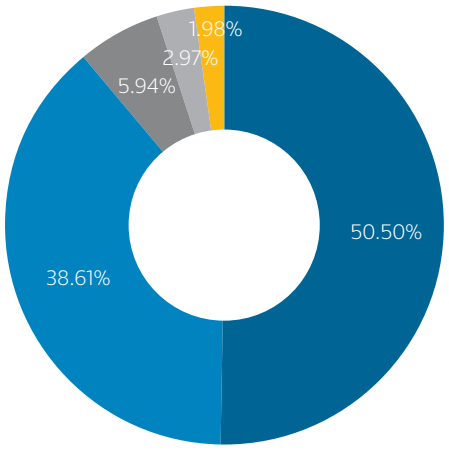
Question 21: For each of the financial crime programs shown below, please indicate which, in your opinion, is the most important tool in managing the prevention and / or detection of crime.

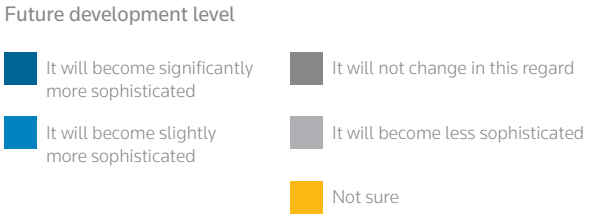


Question 22: The application of technology in the prevention of financial crime has become increasingly sophisticated, for example, the use of data analytics in transaction monitoring. In your opinion, how has your financial crime prevention program developed over the past two years?

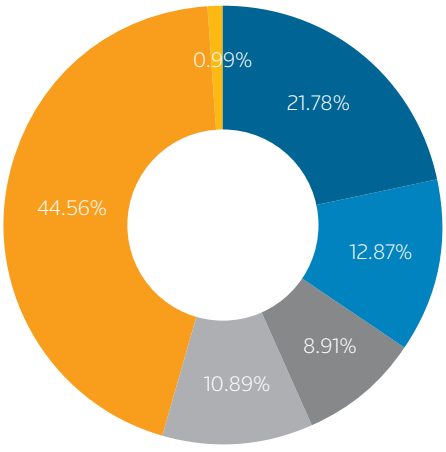


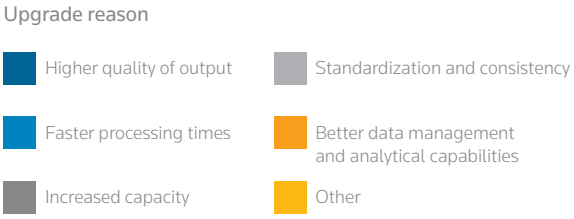
Question 23: How do you expect your technology to change in this regard over the next two years?





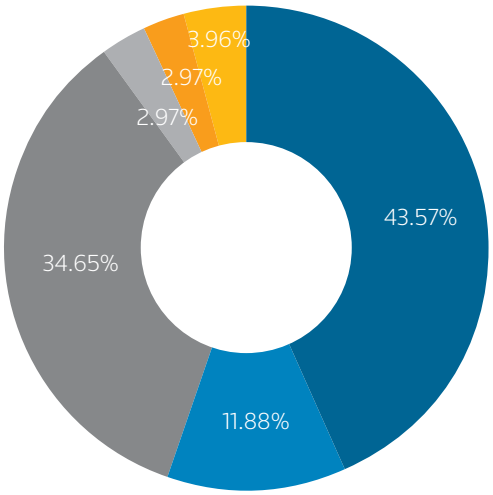
Question 24: What is the main reason you would invest in a technology upgrade?





SURVEY RESULTS (CONTINUED)

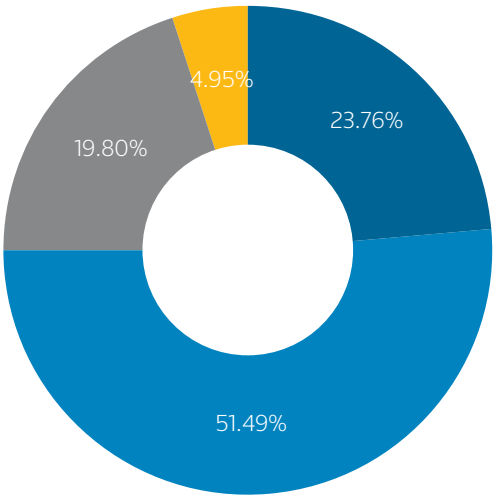
Question 25: What, in your opinion, is a major disadvantage of using sophisticated technology in a financial crime program?



Major disadvantage

- Cost to implement
- Cost of maintenance
- Time to implement
- Wouldn't add value to the current program
- Risk of over-reliance on technology
- Other

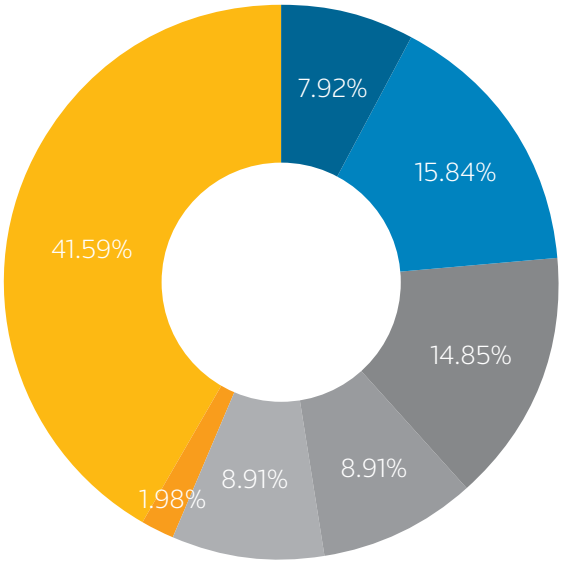
Question 26: How confident are you that your technological financial crime solutions are operating as required and that staff members understand how the solutions operate?



Confidence level

- Very confident
- Limited confidence
- Fairly confident
- Not at all confident

Question 27: If your answer to the previous question is anything other than, 'Very confident' or 'Fairly confident", what are your concerns?



Reason for concern

- You don't fully understand the regulatory environment
- The pace of regulatory updates is overwhelming and challenging to manage
- You doubt the standard of compliance competency amongst staff members
- The implementation training for the technological solution was insufficient
- There is a lack of support from the solution provider
- You don't fully understand the solution and all its uses
- Not sure

CLOSING THOUGHTS

"The financial institutions globally and regionally need to refresh their Financial Crime risk management strategies for how they respond to regulation and how they do business in a regulatory, economic and political environment that could be fundamentally more constraining. Not all institutions will succeed in doing this in the years ahead. Those that do will find ways of making this new environment work for them, capitalizing on their inherent resilience, agility and efficiency."

Bhavin Shah
Partner | Financial Advisory
Deloitte Corporate Finance Limited

Regulatory compliance is on the cusp of dramatic change, about to experience increased automation and new technologies that will change the way we manage data and monitor financial transactions.

This heightened level of change can be disquieting, but we know that change also presents opportunity. Compliance executives, for example, will have access to technology that will be able to automate mundane compliance tasks and help reduce operational risks. It will help to simplify some of the complexities of the compliance challenge and allow for resources to be directed elsewhere.

While the future of regulatory compliance has never been so uncertain, a recent panel discussion by compliance experts held during the Thomson Reuters Pan Asian Regulatory Summit, held in November, highlighted these likely scenarios:

- Compliance will become part of the fabric of business rather than a 'bolt on' function, helping to accelerate time-to-market for new products, minimizing the potential for compliance surprises and helping to reduce operating costs.
- Pre-built compliance frameworks, or end-to-end systems, will be embedded into workflows to automatically maintain compliance and provide an early warning system.
- Ethical behaviour will become a core competence for executives, regularly reinforced by direct line manager behaviours and therefore reducing reliance on training.
- Organizations will adopt smarter compliance analytics to track and evidence compliance to both regulators and internal stakeholders.

It is therefore encouraging to see the emphasis in the responses to this survey on technology and skills investment.

Senior managers may find that if they invest more in improving on visible leadership that it may resolve critical compliance issues not yet realised, thus saving the organization time and money. There is, after all, only so much that technology can achieve.

Thomson Reuters Risk Management Solutions

Risk Management Solutions bring together trusted regulatory, customer and pricing data, intuitive software and expert insight and services – an unrivaled combination in the industry that empowers professionals and enterprises to confidently anticipate and act on risks – and make smarter decisions that accelerate business performance.

For more information, please visit risk.thomsonreuters.com

Deloitte

Deloitte is one of the world's leading professional services organisation which provides audit, consulting, financial advisory, risk management, tax and related services, to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges.

Deloitte's Financial Services Regulatory Advisory ("FSRA") practice addresses regulatory challenges across all levels of an organisation. Our Middle East FSRA team of experts come from multifaceted backgrounds and work closely with Regulators and Financial Intuitions on their current challenges and upcoming regulatory reforms. Key regulatory areas include new laws and regulatory frameworks, prudential risk, conduct risk and financial crime compliance. We use our global network, deep industry experience and advanced analytical technology to understand and resolve issues and deliver the proactive advice clients need to reduce the risk of future problems.

For more information, please visit www.deloitte.com/middleeast