Financial Crime in the Middle East and North Africa 2018

Deloitte.

The intelligence, technology and human expertise you need to find trusted answers.

the answer company™
THOMSON REUTERS®

TABLE OF CONTENTS

4 EXECUTIVE SUMMARY

6 REGULATORY FATIGUE

10 REGULATORS AND THE TECHNOLOGY REVOLUTION

13 SKILLS AND LEADERSHIP: THE CRISIS DEEPENS

16 TRANSFORMATION OF THE COMPLIANCE FUNCTION: THE SHIFT TO CENTER

18 EMERGING REGULATORY THREATS

24 SURVEY RESULTS

38 CLOSING THOUGHTS

EXECUTIVE SUMMARY

Welcome to our fourth 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, thus allowing compliance practitioners and senior executives the ability to benchmark their services.

As with previous years, the report builds on annual surveys of similar respondents and, where relevant, highlights year-on-year trends and developments.

Our typical respondent is a senior manager in the governance, risk and compliance function, employed in a financial institution with over 1000 employees, with a presence in no more than five countries. Similarly to last year, they are most concerned about money laundering, with a sharp focus on knowing their customer.

In last year's report, we said that 2017 would be a year of heightened turmoil due to political uncertainty and exposure to innovative technology, and this has certainly been true. This turmoil, we believe, may have contributed towards a level of indecision amongst compliance and senior executives, and we see this reflected in a number of responses.

Apart from this apparent indecision, we have noted other trends and have highlighted five in this report.

Regulatory fatigue

For the first time in the life of this longitudinal study, we see a pulling back in compliance spend and activities. For instance, we note a drop in the number of financial crime programs employed across organizations, as well as a drop in the number of people who report that they assess their exposure to risk on a regular basis.

We also note that the rate of investment into technology and resources has flattened for the first time, as has investment into improving the sophistication of technology. However, this trend has been noted globally over the last two years in other surveys.

Transformation of the compliance function

Last year's report noted that the compliance role has evolved significantly, and this is a major theme this year – we believe that there are signs that the transformation of the compliance function will be significant. No longer a backroom operation for some time, it seems that the function has the potential to play a leading role within organizations. This will require a change of focus in terms of skill sets, with an emphasis on managerial and technical skills.

With the compliance function moving into another gear, the ability to stay up-to-date with the kind of technology and regulatory issues that are required to stay compliant, is demanding too much of existing resources and it is challenging to achieve cost efficiencies. We expect, therefore, to see a rise in the use of managed services for specific tasks. Regulatory compliance is beginning to require such detailed reporting that it is becoming very challenging to meet all regulatory obligations without access to a very specialized skill set and software. Not all organizations will have the means to maintain these resources.

Skills & leadership

The emphasis remains firmly on issues around training and communication and the perceived lack of resources to meet organizations' regulatory obligations. There is still a sense of a lack of support from senior management, although this is perhaps slightly less prominent than it has been in the past.

Regulators and the technology revolution

The flattening of investment in technology is interesting, especially as it seems that in the last six months of 2017 there were weekly conferences and debates in financial centers around the world on the subject of innovative technology and how the financial system and its regulation is about to face massive disruption. That may well be the case, but at the moment there seems to be more hype than action. It may be that all the talk of disruption, the coming financial and regulatory technology that is about to change our lives so dramatically, may, in fact, be holding back investment activity in technology. There is as yet no clear direction forward, and we explore this in some detail in the second chapter. Investing in technology is a substantial investment and once a particular system is employed, it is very difficult to undo, as any IT manager struggling to unravel legacy systems can attest to.

There is less investment in increasing the sophistication of technology, but a desire for better data management and better quality of output – are decision makers waiting for direction from regulators before they invest in innovative technology? There is an explosion in choice, service providers and information on regtech/fintech. Given this, how do organizations make a major investment decision that could have ramifications for years in the future, especially as the regulatory environment is so dynamic? 'Cost to implement' is stated as the main obstacle to investing in technology.

Emerging regulatory threats

Responses to some of the questions point to potential weaknesses in compliance defenses for issues such as cyber crime and sanctions which we examine in detail in the section on emerging regulatory threats. While cyber crime and sanctions have been an ongoing issue for some years now, we are also expecting to see regulation about other issues, such as whistleblower protection and trade based money laundering, that we believe will have an impact on MENA-based organizations in the short term.

REGULATORY FATIGUE

For the first time since the longitudinal study began, we note a tapering off regarding investment into technology. While technology is still the focus of much of the investment in compliance, there is a noticeable decline, a trend that has been noted over two years in other survey results - the Thomson Reuters Cost of Compliance reports of 2016[1] and 2017[2].

There has also been a drop off in the number of respondents reporting on financial crime programs that they employ, as well as reports of how often risk is assessed. There was a notable drop across all financial crime programs in responses to **question 6**, which asks which programs are in place within the respondent's organization.

The most noticeable drop was in the number of reported sanctions and fraud programs, and this is despite a 5% spike in organizations reporting financial fraud in the region in 2016 compared to 2015[3].

The status of international sanctions is fluid and volatile and it is difficult to predict with any certainty how the situation may develop over the next six, if not three, months. With the potential for the dynamic to pivot suddenly at any time, organizations are advised to assess their risk in this context and to systematically reassess it at frequent intervals. Also, the easing and lifting of sanctions, especially long standing sanctions, can result in heightened risk which calls for increased vigilance. It is advisable therefore to review their sanctions programs and not be tempted to allow them to lapse in any way.

The most popular choice in financial crime programs are Anti-Money Laundering (AML) and Know Your Customer (KYC), with two thirds of respondents claiming to have these programs in place, although the percentage of respondents claiming to have both these programs dipped slightly..

This year we added a few programs to the list – transaction monitoring, whistleblowing protection and trade based money laundering - as we were curious to see the level of awareness for these programs and the extent of their implementation.

All three programs have relatively low uptake, with 55% of respondents claiming to have implemented a transaction monitoring program, 51% of respondents claiming to have a whistleblower protection program and only 36% of respondents claiming to have a specific program for trade based money laundering.

Only around 50% of respondents have programs against bribery and corruption,

and nearly 60% of respondents have instituted a threat financing program.

[1] Cost of Compliance Report 2016, Thomson Reuters

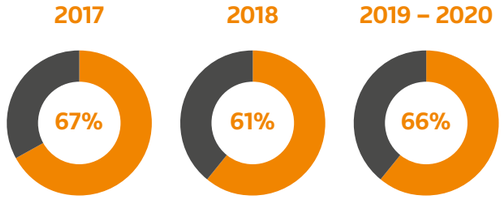
[2] Cost of Compliance Report 2017, Thomson Reuters

[3] 'Economic Crime in the Arab World 2016' PwC

"The fundamental challenge of financial crime compliance is that critical portions of the requirements are risk-based, which presents challenges to both the regulators and banking industry as they seek to determine what preventive actions are sufficient given the risks posed within individual institutions and across industries."

Bhavin Shah, Partner,
Financial Services Regulatory Advisory, Deloitte

Percentage of people who expected an increase in technology sophistication



Questions 8 and 9 address investment into anti-financial crime activity and compliance, **question 8** examines the issue retrospectively while **question 9** looks at projected investment.

Just over 40% replied that their investment has increased substantially or somewhat over the past two years and 49% expect substantial or somewhat increase in investment in the short term. Compared to last year's study, these figures represent about a 20% drop in both retrospective and projected investment.

This flattening of compliance spend is in line with global survey findings however, and while we did expect this trend to appear at some stage, the extent of the drop was surprising.

In the Thomson Reuters Cost of Compliance Report 2017, which is a global survey of compliance practitioners, it was noted that budgets were moderating with 53% of firms expecting the total compliance budget to be slightly or significantly more over 12 months, a similar period to this survey, and 42% expecting the budget to grow in the following year.

Similarly, when asked in **questions 22 and 23** about the increasing sophistication of technology, another drop in investment was noted from an otherwise upward trajectory in previous years. In this year's survey, 61% expected their technology to become more sophisticated, as compared to 67% last year, and over the next two years, 66% respondents expect their technology to become more sophisticated, a substantial drop from the nearly 90% of respondents last year that expected increased sophistication.

"Make no mistake. The need for KYC checking is not diminishing. If anything it is growing in importance. It has never been more important for the financial sector to ensure it denies access to the banking system to people involved in crime."

David Craig, President Thomson Reuters
Financial & Risk

These responses give a sense that the foot has been taken off of the pedal somewhat, in sharp contrast to the increasing volume and complexity of the regulatory environment. The flow of regulatory updates continues to wash over organizations at an increasing pace. In 2008, when Thomson Reuters first began to track regulatory updates, they numbered around 10 a day, today that figure is closer to 200 updates daily, with no sign of slowing down. Apart from the increased volume, the compliance function is now required to deliver a higher level of detail by incoming regulations such as the Markets in Financial Instruments Directive II (MiFID II), a directive which demands increased market transparency.

At the same time enforcement activity has been stepped up, with greater focus on the individual rather than corporate responsibility. Regulators, including the Financial Conduct Authority (FCA), Dubai Financial Services Authority (DFSA) and U.S. Securities and Exchange Commission, are pursuing strategies that target executives using tools such as the Senior Managers and Certification Regime (SMR). Organizations are being issued with eye-watering penalties, for example, the major U.S. investment firm that was fined GBP 34.5 million by the FCA in October 2017 for compliance failures associated with the European Market Infrastructure Regulation (EMIR).

Not only have fines increased dramatically, so has the personal risk to executives. In this environment, you would expect that compliance spend would continue to increase.

So why would there be a pulling back at this stage?

It appears that senior management are often overwhelmed with a growing avalanche of regulatory information. We note in the Thomson Reuters Cost of Compliance report of 2015 that executives expressed fatigue and overload in the face of the regulatory avalanche of information and board members revealed in the survey that regulatory matters were consuming a disproportionate amount of time. It seemed that regulators were aware of fatigue levels, however, when the then acting chief executive of the UK's Financial Conduct Authority, Tracey McDermott, remarked on the potential adverse effects of the increasing compliance burden on companies and warned that it was not sustainable.

Ms McDermott also pointed out the danger of regulatory overload, noting that it may "crowd out the creativity, innovation and competition which should present the opportunities for growth in the future."

After some years it may be understandable if there is a degree of fatigue or complacency. Cost cutting in a challenging economic and political environment is a natural response and has been going on for some time; the difference is that this is the first time it appears to be impacting the compliance function at a time when there is a need for greater vigilance.

"We have seen an ongoing rise in compliance leaders expressing regulatory fatigue as they are being held to increased accountability amidst an ever-escalating volume of regulation, the expectation of being knowledgeable, and the added pressure of being exposed to record fines for non-compliance. With heightened scrutiny and accountability, it has never been more vital for boards to continue to support the compliance function and senior leadership with the budget, resources and tools to help ensure a culture of transparency, trust and adaptive-change in behaviors throughout firms."

Phil Cotter, Managing Director of Thomson Reuters Risk business

Featured questions:
6, 8, 9, 22, 23

Full survey results can be found on pages 24-37

REGULATORS AND THE TECHNOLOGY REVOLUTION

It has become apparent throughout the years of our study that many compliance executives are constantly seeking more – more support, more resources, more skills, and more analysis – in a bid to relieve some of the stress of the compliance function.

When asked in **question 15** what will be the biggest challenge in managing financial crime and compliance programs, the top three answers were 'Securing new resources'; 'Communicating tone at the top'; and 'Attracting and retaining key skills'. Asked for reasons for a lack of confidence in their programs in **question 19**, most responses point to a lack of senior management support, as they did in the previous study.

It is understandable, therefore, that there is a desire for greater sophistication in software – lacking support from senior management and concerned about an apparent skills deficit in their teams, compliance executives are tasked with frequent decision making that often has critical outcomes and can carry considerable personal and corporate risk. Many seek increasingly sophisticated software to help with some of the heavy lifting of their role, as we see in the responses to **question 24** – when asked for reasons for investing in a technology upgrade, the two most popular responses were 'Better data management & analytical capabilities', and 'Higher quality of output', consistent with responses from the previous year's study.

Despite this search for increased sophistication and greater data management capabilities, there is a notable drop in expected investment compared to last year's study, revealed by responses to **questions 8 and 9 .**

If we look for reasons why there is this slow down in current and expected investment, cost is definitely a factor - when asked about the disadvantage of an advanced technological solution, the majority of responses cited 'cost to implement'. At the same time, there appears to be a growing awareness of coming change – if anything, 2017 has been the year that fintech and regtech stepped out of the sidelines and became one of the leading topics of conversation.

> "Fintech is looking at innovative solutions typically for consumers in the little gaps left by financial services organizations, the bigger banks, the bigger insurance businesses … Regtech is looking at really a very different area, some of the technology is similar but the solution is different. Here we're looking at how institutions, banks, insurance companies and other regulated entities can comply with regulation and do that in a better and more efficient way."
>
> **Andrew Yuille, Head of Risk Business Solutions at Thomson Reuters, 2017**

While the technology that underpins both fintech and regtech holds much promise, it seems that many people may have high expectations of what the new technology will be able to deliver in the short term, and its impact on their daily working lives and bottom lines.

Vitalik Buterin, the founder of Ethereum, one of the world's most popular cryptocurrencies, refers to the situation as 'peak hype'.

Take blockchain as an example - despite expectations, it has yet to deliver any mainstream solutions yet commentators continue to speculate on a tipping point for its use, as well as pontificate on its numerous uses.

We suspect that this hype may be impacting on compliance spend as decisions makers are bombarded by a confusion of information about different solutions, unfamiliar terms, and warnings of coming disruption. Given the level of commitment required to invest in new technology, and to disinvest from current systems, we believe that there is a strong possibility that decision makers may be holding back on further investment until there is clear regulatory guidance in the market.

They may not have long to wait - in MENA, we have seen the regulators attempt to catch up to the lead set by their peers in Europe and Asia with the establishment of fintech bays', hive's and hubs and numerous 'sandboxes' appearing throughout the year.

A recent Deloitte report[4] on global fintech hubs reveal that European and Asian hubs are benefitting from government support.

Research shows that new European hubs enjoy good access to talent, although they also reported regulatory barriers were holding them back. The UK, Netherlands, Russia, Switzerland and Norway have committed to a regulatory sandbox to help solve the issue of regulatory strangulation, while the UK, French and Swiss regulators have signed fintech cooperation agreements with other regulators elsewhere.

Asian Pacific Hubs are setting the pace, however. Seven regulators have either set up or are committed to setting up regulatory sandboxes. A number of them – China, South Korea, Hong Kong, Japan, Singapore, Australia and India – have been proactive in signing cooperation agreements with regulators outside of their region, and one of them, Singapore, has the most fintech co-operation agreements than any other Hub.

In contrast, two Hubs from the Gulf region claim excellent government and regulator support for fintech, for example, Abu Dhabi has the RegLab and Dubai has the FinTech Hive and 2020 blockchain ambition, Bahrain benefits from fintech work driven by the Economic Development Board.

The aim for regional regulators has very much been on trying to replicate the environment achieved within the UK, which now has a fintech economy valued at 7bn GBP annually[5].

The expectations are that fintech will bring unprecedented change to the financial sector, and that regtech will need to keep pace if growth is to be achieved as regulators strive to shape the new environment.

At this stage, when there is much talk but not enough practical application, it is interesting to watch trends develop. While many are expecting fintech to disrupt the established frameworks of financial institutions, the reality is that the major advances are being made by operators in the traditionally less fashionable and less profitable areas of the financial services industry, such as the lower end of the retail banking market.

The ability of fintech companies to bring low cost solutions to the low value, but high volume markets, has seen a revolution in areas such as the remittance and payments markets.

One such market entrant in the payments space, India's Paytm, is said to have attracted over USD 1.4 bn of funding recently, which is not surprising when you look at their figures. The company states that it has signed up over 500,000 taxi and rickshaw drivers to its mobile payment platform and is adding around 10,000 shop merchants a day. By 2020, they aim to have signed over 500 million customers[6]. Given that the government is working hard to stop people using cash in a bid to stem the circulation of black money, they are well placed to rapidly grow their market share.

[4] A tale of 44 cities: Connecting Global FinTech: Interim Hub Review 2017, Deloitte April 2017

[5] Fintech is now worth £7 billion to Britain's economy and employs 60,000 people, Business Insider, April 12 2017

[6] 'Mobile Wallet Paytm Hits Pay Dirt Amid India's Cash Crackdown', 4-traders.com, May 2017

These numbers are staggering, but interestingly, Paytm was until relatively recently unregulated and operating in a space that the traditional banks had little interest and no profitable model to serve. The emergence of fintech's servicing the so called 'un-bankable' elements of society is one of the more positive trends to establish itself in this new market but we wait to see how potential regulation may impact the sector.

Undoubtedly the area that has gripped the imagination of the public the most in recent months has been the subject of cryptocurrency. 2017 has seen governments establishing plans for their own virtual currencies, as in Japan, or outlawing cryptocurrency activity, as in China.

All this against the backdrop of the Bitcoin hysteria that saw the value of a single Bitcoin in the past twelve months shoot up from less than USD1,000 to over USD19,000 at the time of writing, December 2017. Love it or hate it, this huge upsurge in the value has coincided with a shift in awareness and understanding of cryptocurrencies, as well as a shift in attitude by some governments towards more progressive and open minded strategies about the future of virtual currencies in the global economy.

This presents a major challenge for the governments and regulators. As we go into 2018, we are still very much in a sandbox or testing environment for so many of the emerging technologies. There is for many, however, a realization that the pace of exploration can change dramatically at any given time.

> "Regulators are realizing they're going to have to develop new tools. They can't keep up. Old ways of regulating are completely mismatched with the challenges emerging in this fast-changing environment. They are going to have to create new models of regulation and regulatory collaboration or they're going to have huge failures."
>
> **Jo Ann Barefoot, CEO Barefoot Innovation Group**

Governments are faced with the task of creating a favorable environment that will allow them to profit from the massive benefits that could accrue from the new technology while at the same time minimizing their exposure to risk. It should be remembered, however, that the current regulatory environment was shaped to respond to the aftermath of the 2008 crisis with the focus on propping up some of the major banks. Regulators have to develop a completely new mindset and approach, and awareness of this is apparent in a recent fintech/regtech survey[7]. Respondents reported a substantial drop in compliance monitoring, which was their top priority in 2016, to regulatory change and reporting in 2017.

We are still in the early adoption phase of the new technologies that are already in the market, with experts stating that blockchain will be widely adopted and integral to the capital markets ecosystem by 2025[8]. Governments keen to compete as a fintech hub should be thinking of preparing a roadmap, that will support innovation and technology development for the next decade.

[7] Fintech, Regtech and the Role of Compliance in 2017, Thomson Reuters

[8] How the laws & regulation affecting blockchain technology can impact its adoption, Business Insider, October 2017

Featured questions:
8, 9, 15, 19, 24

Full survey results can be found on pages 24-37

SKILLS AND LEADERSHIP: THE CRISIS DEEPENS

From the beginning of this longitudinal study, there has been one trend that has remained steadfastly prominent – a crisis of confidence in GRC abilities, competencies and programs. This year, this trend was more noticeable.

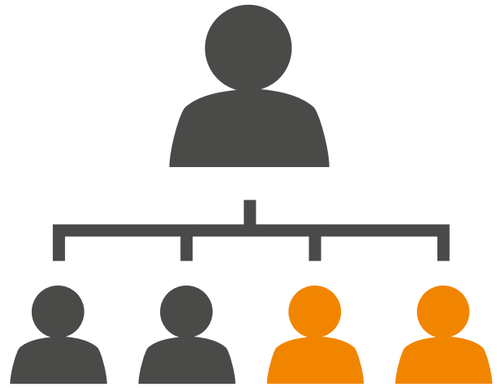
In **question 26**, when asked how confident they were that their technological financial crime solutions were operating as required and that staff members understood how the solutions operated, there was a spike in responses citing a lack of confidence in their solutions. Over a third of respondents to this question reported limited or no confidence in solutions, a jump from last year's response rate from a quarter of respondents reporting limited or no confidence.

When asked why in **question 27**, nearly a quarter of respondents replied that they doubted the standard of compliance competency of their staff members.

Question 18 probes confidence levels in financial crime prevention programs and their compliance with regulations – nearly a quarter of respondents reported a lack of confidence, up from 19% last year. Asked for reasons for a lack of confidence in **question 19**, close to half of the respondents cited a lack of senior management support, also the most popular choice in last year's study.

What is notable here is that there has been a substantial investment in compliance programs over the years. Since this longitudinal study began, we have noted an increase in positive responses when asked about investment into compliance year-on-year, until this year when there was a drop. It is also notable in the responses to **questions 10, 11 and 15** that skills and training is a priority.

Asked in **question 10** how increased anti-crime and compliance activity and awareness has manifested itself across the organization, emphasis on training and increased staff resources were top priorities.



47% cite lack of management support for their lack of confidence

Asked in **question 11** what the expectation was for increased awareness to manifest itself, the focus continued to be on training and staff.

Question 15 examined the challenges involved in the management of various financial crime and compliance solutions; top issues reported included 'attracting and retaining key skills' and 'maintaining training and awareness'.

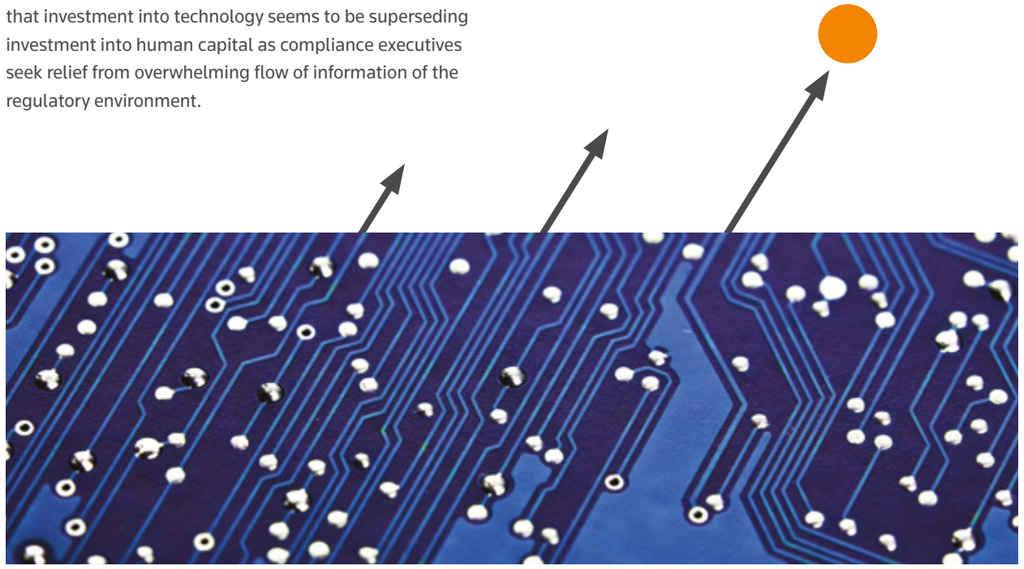
The impact, of course, of a confidence crisis is that it can paralyze action, delay decision making and impede the progress of the compliance function. It, therefore, poses a risk to the health of the organization. It is, however, perhaps a feature of transition, which will be addressed more fully in the next section, when uncertainty is a constant.

Finding a remedy may not be straightforward, the skills deficit has been an issue for some years, perhaps not surprising given the dynamic nature of the compliance function, and its changing profile and norms.

This year we believe an added stressor is the increasing noise around a potential digital disruptor, expected to have a major impact on contractual processes and financial flows, which contributes to a sense of uncertainty. We note that investment into technology seems to be superseding investment into human capital as compliance executives seek relief from overwhelming flow of information of the regulatory environment.

"Analytics is becoming essential to effectiveness. With the growth of electronic transactions and the explosion in the amount of information available to organizations, advanced data management and analysis is becoming both the weapon of choice for fighting financial crime and the glue binding enterprise-wide approaches together. An important factor is that the combination of analytics and big data is allowing financial institutions to spot potential problems and relationships between parties."

Nipun Srivastava, Director, Financial Services Regulatory Advisory, Deloitte



The shift towards technology is apparent in **question 12** - asked where the main focus of investment to meet compliance objectives, technology has been the main focus for last two years of the study - in **question 22** which reveals a general upward trend in the sophistication of technology - in **question 23** where two thirds of respondents say that they expect their technology to become more sophisticated over the next two years - in **question 24** where most respondents say they are searching for better data management and analytical capabilities when investing in a technology upgrade.

This move towards higher levels of analysis and sound decision making through the use of sophisticated technology, including enhanced analytics visualization tools, will no doubt heighten expectations for the compliance function to proactively identify, manage and report a broader spectrum of risk. Hopefully it helps to quell any rising anxiety about meeting regulatory obligations, as we see reflected in responses to **question 14** which asked what poses the most risk to their organizations - the most common response was "Failure to meet regulatory requirements".

However, a quarter of respondents voiced concern about over reliance on technology – best practice compliance has always been a balanced interaction between technology and human interaction, but as we see investment increasingly tipping in favour of technology to the detriment of skills, some are raising a red flag. While there is an increasing tendency to outsource compliance tasks there is still a need to retain appropriate skill sets.

There is an essential skill set at the core of effective compliance that is not impacted by software. While there is a sense of waiting for events to run their course, as well as waiting for regulators to provide guidance on the new normal, the compliance function may be well served by a focus on this core skill set.

Managed services to strengthen the compliance function

The functional knowledge base for many compliance areas has had to expand and deepen at a rapid rate, and this high velocity of change reduces the capacity of an organization to obtain and maintain a high level of institutional knowledge.

In this environment, there is a strong case for the use of managed services to supplement organizational capacity. It is simply too important a task, too large a load and increasingly too specialized a function to cope with in-house, to the required degree of competency. In question 12a, we see that, when asked for reasons for a lack of confidence in their programs, a third of respondents pointed to 'Lack of availability of specialist resources'.

With it becoming increasingly challenging – and costly - to locate appropriate skills in the market place, organizations can proactively limit enterprise risk and strengthen compliance by using well designed managed services to address deficiencies in internal talent, improve process quality and adopt technologies and to supplement internal processes. And with technology developing as rapidly as it is, it is highly likely that the skills deficit will widen. While key skills will always be a requirement in-house, managed services will greatly help to bridge the skills deficit.

Featured questions:
10, 11, 12, 14, 15, 18, 19, 22, 23, 24, 26, and 27

Full survey results can be found on pages 24-37

TRANSFORMATION OF THE COMPLIANCE FUNCTION:

The shift to center

The compliance function appears to be undergoing a transformation which could see it become the strategic center of the organization.

Indeed, some would argue that there is a pressing need for the compliance function to become more integrated, more pervasive, and to lead from the front – despite the growth in regulatory volume and complexity, we are still often dismayed by further revelations in the media of private and public malfeasance.

The trend appears to be towards a broader risk-based approach with a shared responsibility between management, staff, the board and internal audit.

We see evidence of integration in responses to **question 17** that show a level of integration with the audit function, or the third line of defense - when asked how they monitor and assure financial crime programs, responses show that most use a combination of external and internal functions.

Historically Compliance functions' primary focus has been to define the rules and framework for an organization to achieve compliance with relevant laws and regulations. While this will remain at the core of Compliance functions' remits, we expect to see a continuation in the evolution of the Compliance function in 2020 and beyond. We expect to see an increasing focus on ethics, culture and principles, and progress towards functions which are enabling change, acting in an advisory capacity to the business and (although hard to measure), providing a source of competitive advantage, with many functions rebranding as Compliance and Ethics.

New horizons: Compliance 2020 and beyond 2016

> "In the 21st century, money crosses borders more easily - and with less oversight - than people."
>
> **The Paradise Papers, OCCRP.org**

There is already a level of integration with the first line of defense, the operational defense, apart from an oversight role, the compliance function provides a systematic process that assists in alerting front line employees to red flags.

Having a robust 'three lines of defense' approach is not always a guarantee of success however. It requires careful monitoring and support to ensure that all three lines are working effectively together. Also helpful is a strong emphasis on ethics and culture in leadership with a place at the top table for the leading compliance executive.

The original compliance model served as a simple tick box exercise for the legal function and after the 2008 financial crisis, the model expanded to include conduct rules and have a larger emphasis on management accountability. Today, overwhelmed by a constant barrage of regulatory updates and demands, increased business expectations and the management of daily operations that increase in complexity every year, compliance executives are looking to leverage all available resources in a bid to meet their obligations.

As the compliance functions transforms and moves away from a 'standard' AML and CFT approach, we see the function moving into a more pivotal role within the organization. While much of the current focus is on innovative technology that will have an impact on the compliance function, we believe the real shift will occur in mindset and approach. The role of compliance is broadening into something very different from the original model, and we expect to see the function increasingly move towards a strategic, advisory role.

Such a transformation and change in approach should assist in identifying and mitigating a broader spectrum of risk and should therefore achieve greater efficiencies in a time of flattening budgets. To achieve this transformation requires a formal, focused change management effort to support the integration of compliance across key governance functions - legal, risk management, internal audit – all of which play a role in the 'three lines of defense'.

> "The role and function of the compliance and risk team has been revolutionized over the past decade beyond recognition. There's a greater focus on personal liability, with regulator focus moving from rules-based compliance to culture and conduct."
>
> **David Craig, President of Financial and Risk at Thomson Reuters**

This will require investment into senior managerial capacity, although we note from the survey responses a general shift towards investing in technology over human capacity, with certain tasks passed to managed services with the specialized skillsets and resources required to cope with the various complexities of remediating risk. Integration into the greater risk framework will require a greater sharing of knowledge and co-ordination between teams if the necessary synergy is to be achieved.

With the compliance function in a state of flux, this is a good time to step back and reflect on trends and consider what will be required from the function, now and in the future - what role can the compliance function fulfil that it is not doing now? It is time to move away from fire-fighting and create a road map that will develop a next generation compliance function. With support from sophisticated analytics, there is scope for the function to become a strategic advisor to senior management as well as a control function, and to be able to lead from the front.

Future of compliance

By 2025, we anticipate compliance to catalyse the shift towards a cultural change and an insights-driven organization.

As the Executive of a financial services institution pushes the transformational mandate, compliance will be a driver of cultural change. Being compliant will be the responsibility of all employees and ultimately become a natural and integral part of an institution's DNA. Moreover, enabled by redesigned processes, enhanced technology and an evolved workforce, compliance will be one of the key drivers of an insights-driven transition.

The compliance function of the future will be part of a service centric compliance eco-system where software vendors, data providers, start-ups and financial services institutions engage in deeper and more efficient collaborative models.

Compliance 2025: DNA evolution in the Financial Services Industry, August 2017, Deloitte

Featured question:
17

Full survey results can be found on pages 24-37

EMERGING REGULATORY THREATS

The regulatory environment is always described as fluid, dynamic, challenging, and often times it must feel for many compliance executives that they are only just getting to grips with the current regulatory dynamic before a new challenge asserts itself. This is especially true in the current scenario. Faced with incoming regulatory monoliths such as Markets in Financial Instruments Directive II (MiFID II) and General Data Protection Regulation (GDPR), compliance executives will be subsumed with gearing existing systems to accommodate a much higher level of detail and transparency that is demanded by these regulations.

As well as these new regulatory demands, some MENA governments are preparing for upcoming 2019 MENAFATF mutual evaluations. The GCC is a member of (Financial Action Task Force) FATF and although individual member countries do not belong to the organization, they are subject to mutual evaluations conducted jointly by the regional AML/CFT body for MENA, which is MENAFATF.

The FATF calls upon all countries to implement the necessary measures that will align their national systems for combating money laundering, terrorist financing and the financing of proliferation of WMD with revised FATF Recommendations. As the nature of financial crime evolves, regulators are required to ensure that their approach remains current and update their regulations accordingly, and the pressure is passed onto those within organizations with responsibility for compliance.

It is necessary, therefore, for compliance executives to not only stay current but to also keep their eyes on the horizon for several regulatory threats looming large. We see concern for this responsibility in responses to **question 13**, when asked what they believe is the key concern in terms of financial crime and compliance, the majority of responders chose 'Complying with international and local regulation to avoid censure', and nearly a quarter of respondents revealed low levels of confidence in their programs being compliant with domestic and international regulations in **question 18**.

According to some of the survey responses, we think that compliance executives should be monitoring their programs that relate to cyber crime, sanctions, trade based money laundering and whistleblowing.

> "Financial Institutes 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 firms will succeed in doing this in the year ahead. Those that do will find ways of making this new environment work for them, capitalising on their inherent resilience, agility and efficiency."
>
> **Bhavin Shah, Partner, Financial Services Regulatory Advisory, Deloitte**

If we look at the number of respondents in question 6 reporting a cyber crime program for example, we see that, as with other programs this year, there has been a drop. Indeed, the percentage of respondents to this question over the years has never risen over 50%, starting at a low of 33% in the first year of the study and climbing to a peak of 47% in last year's study. This year, it has dropped to 43%, which is remarkably low considering that there seems to be a high, and spiking, level of concern around cyber crime. Last year 68% of respondents reported high levels of concern, this year 73% of respondents reported that they were very or extremely concerned about cyber crime.

This means that while levels of concern are rising, work on remediating the risk is falling, and we wondered why. A recent Deloitte report[9] offers interesting insights. It seems that many financial institutions report that they are struggling to keep up with cyber security issues, despite generous budgets and several years available to prepare a good defense against the crime. In fact a 2016 survey report showed that only 42% of respondents believe that their organization is 'extremely effective' or 'very effective' in managing cyber exposure.

[9] Taking cyber risk management to the next level, Deloitte Insights, June 22 2016

The report also offers a few reasons why organizations may be struggling with cyber security

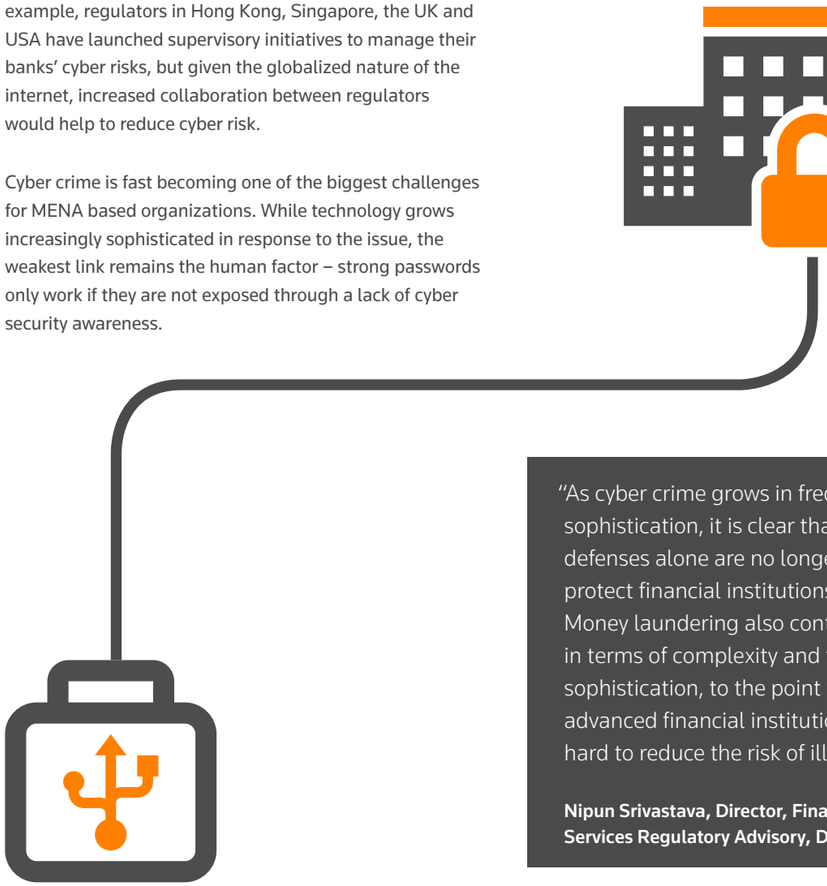
- **Competing priorities** the role of the information officer has grown increasingly complex over the years, and today they are faced with a range of issues, all of which are equally pressing. Their core function, of course, is maintaining health of the IT infrastructure, ensuring that downtime is minimized and that everyone is kept connected and functional, in itself a mammoth undertaking. Recently, innovation is pushing everyone onto a massive learning curve, and the sense of the coming disruption is slowing down decision making. With online threats changing so quickly, to be effective, cybersecurity policies have to be reviewed and updated frequently, a difficult challenge in this situation. Information officers are simply overwhelmed by the task of staying relevant.

- **Skills scarcity** the implementation of effective cyber risk management policies requires skills that go far beyond the technical. It needs a business mind-set and a strategic approach, a combination that is hard to find.

- **Cyber risk and data management** in an increasingly data rich and complex environment, information officers often struggle to analyse and interpret data in a meaningful way so that it is relevant and actionable.

A lack of co-ordination of a regulatory response between regulators is also a contributing factor – we see a growing effort by regulators to provide controls for this issue, for example, regulators in Hong Kong, Singapore, the UK and USA have launched supervisory initiatives to manage their banks' cyber risks, but given the globalized nature of the internet, increased collaboration between regulators would help to reduce cyber risk.

Cyber crime is fast becoming one of the biggest challenges for MENA based organizations. While technology grows increasingly sophisticated in response to the issue, the weakest link remains the human factor – strong passwords only work if they are not exposed through a lack of cyber security awareness.



"As cyber crime grows in frequency, size and sophistication, it is clear that technological defenses alone are no longer sufficient to protect financial institutions from attacks. Money laundering also continues to evolve in terms of complexity and technological sophistication, to the point that even advanced financial institutions are finding it hard to reduce the risk of illicit activity."

Nipun Srivastava, Director, Financial Services Regulatory Advisory, Deloitte

Business leaders cannot afford to be complacent as the issue of cyber crime poses a serious risk to the longevity and success of their organization.

There is also a notable drop in respondents reporting a dedicated sanctions program. Last year 67% of respondents reported having a sanctions program, this year this number dropped to 57%. This is despite more than two thirds of respondents reporting that they are either very or extremely concerned about the issue of sanctions, a slightly higher number than last year.

Since the Trump administration took office January 2017, there has been a strong possibility of increased sanctions, so this is not a time to be complacent and organizations are advised to continue to apply rigorous checks to ensure that there is no unwitting transgression of international sanctions.

To circumvent sanctions, for example, many affected organizations have developed complicated mechanisms to conceal their transactions. The use of shell companies, obscure bank ownership structures and third parties have made the detection of high risk relationships increasingly complex.

Both the US and EU explicitly require that financial institutions understand the ownership structure of their clients. Ultimate beneficial ownership (UBO) has become a regulatory focus in recent years, and organizations are expected to take all reasonable steps to clarify the true ownership of organizations in the value chain, not only the organizations that they deal with directly, but also those they to which they are indirectly linked.

Indeed, entering into any type of contract with a company without taking all reasonable steps to establish UBO may expose an organization to significant risk. It can be challenging due to various layers of ownership, working across different jurisdictions, difficulty in sourcing physical documentation and a lack of skilled resources to conduct the search.

"Growing sophistication in the cyber crime community", where criminal groups band together to deliver "cyber crime services", is becoming the major engine of growth in online crime undertaken for illegal profit."

Europol director Rob Wainwright, September 2017

The consequences of non-compliance with a sanctions order can be significant and there have been substantial financial penalties imposed by OFAC in recent years. Apart from financial penalties, the other consequences of sanctions breaches include being shut off from trade with the U.S., designated as a Specially Designated National, reputational degradation and even a prison sentence.

Coming up: two regulatory issues fast gaining prominence is that of whistleblower protection and trade based money laundering.

The subject of whistleblower protection is increasingly in the sights of the regulator, and thus we thought it important to introduce the subject into the longitudinal study. Results of the survey revealed that only half of the respondents claim to have a whistleblower policy in place. Asked for reasons for the lack of policy, the most commonly chosen answer was the lack of awareness for the need for one, followed by the lack of available resources, including skills, and lack of senior management support.

The risk of not having a policy in place is that potential whistleblowers are discouraged from approaching management with a potential problem. This means, of course, that organizations could be potentially supporting systemic or isolated cases of financial crime, with a blissfully unaware senior management team at the helm, at high risk of being held personally responsible.

Should wrongdoing be uncovered and reported by an external stakeholder, or picked up by an enforcement agency, the consequences could be dire.

While having a whistleblower protection policy does not offer iron clad security, there are studies that illustrate that the practice of whistleblowing can be very effective at uncovering financial mismanagement. Several research reports produced by the Association of Certified Fraud Examiners (ACFE) highlight the effectiveness of whistleblowing as a method of uncovering financial crime[10].

It is not surprising therefore that regulation enforcing whistleblowing protection is growing around the world. We are in no doubt that this trend will impact business in the MENA region in the short term. As certain centers within the region work to increase their competitive edge against the traditional financial hubs for business, they are very likely to align their financial regulation. Centers such as Dubai, Doha, Cairo, Casablanca, Riyadh and Tunis are increasingly competing on a global stage for recognition and of this list, only two – Dubai and Tunis – are actively addressing whistleblower protection, giving them an edge against their regional associates. In November 2017, the Saudi Shoura Council announced plans to discuss a proposal for whistleblower protection.

Unfortunately, whistleblowers are often penalized for stepping forward even when the regulatory environment offers protection. It is one thing to have a solid policy on paper; it is another to execute it effectively, as a recent case study illustrates. A serious error of judgement by the most senior executive of a major bank illustrates the risk posed by inappropriate application of a sound whistleblower protection policy.

As regulation in this area increases, organizations can prepare by publishing a carefully considered whistleblower protection policy, and also:

- Regularly communicating on the subject within the organization
- Offering training and workshops on a regular basis
- Providing a safe and secure space for whistleblowing purposes
- Guaranteeing anonymity

Providing a safe space for whistleblowers to come forward and voice their concerns is a complicated business and an area where many have misstepped. It requires skilfull handling and absolute iron tight guarantees, but the payoff could be the difference between success and longevity or destruction and bankruptcy for some. The onus is on the senior leadership team to know what is happening in their business before anyone else does, and this can be particularly challenging in today's dynamic business environment when challenged by a constant flow of competitive and regulatory information, and where everyone has a camera on their phone and the means to disseminate information instantly. Leaders should ensure that whistleblowers feel safe and welcome to approach them, it can save not only the company but their own career.

[10] The Case For Whistleblower Protection', Thomson Reuters, 2017

Of all the financial crime programs listed in the survey, trade based money laundering was the least employed, with just over a third of respondents claiming to have an established program at their company.

This is despite over half of respondents claiming that they were either very or extremely concerned about this issue.

The profile of TBML has risen over the past ten years, just as the regulatory environment has tightened considerably and enforcement activity has forced many organizations to review and align their compliance processes. This regulatory activity has targeted the more common money laundering methods, therefore shutting down various routes to transfer money into the financial system. It is now estimated that hundreds of billions of dollars are transferred through trade mechanisms each year, and developing economies are particularly vulnerable. It is estimated that as much as 80% of illicit financial flows through developing countries are routed through trade[11].

We should not be surprised at the scale, given that the volume of trade has grown so rapidly, with so many governments actively seeking to integrate their economy with regional and global economies. Regulators are now looking for ways to subdue the practice.

The FATF and U.S. government agencies have highlighted TBML as a significant issue. The FATF has issued reports and best practice guides that address the issue. Several government agencies around the world, including agencies in MENA, are exploring possible collaborations against TBML and we can expect regulation on this topic to expand shortly.

As the name suggests, TBML uses trade to transfer funds around the world. An example of a TBML scheme is the shipping of a consignment of goods from one port to another with trade papers that grossly inflates the consignment's value. It is time consuming and arduous for customs officials to follow the paper trail to investigate the true value of a consignment, and superficial checking would not normally raise any red flags.

Moving funds in such a way can also be complicated by moving the consignment several times, through several ports, with each customs clearance adding a veneer of respectability, thus helping to obfuscate the value of the goods.

As trade grows between MENA-based organizations and business located elsewhere, so does the opportunity for TBML. With many economies in the region dependant on trade for growth, there is an interest in meeting international best practice standards of compliance, and this requires transparency, robust management and consistency in reporting and supply chain management. Without such, there is a higher risk of TBML, and long term growth plans may be in jeopardy.

Asked what the important tools are in managing TBML, the most popular choice was transaction monitoring, followed by staff training and technology based screening and monitoring. It is also really important to establish beneficial ownership of any company involved in the trade, that the location of the transaction is established, that the country of origin of traded goods is established, as well as any ports that were involved during the trip, and as far as possible determine the value of the goods.

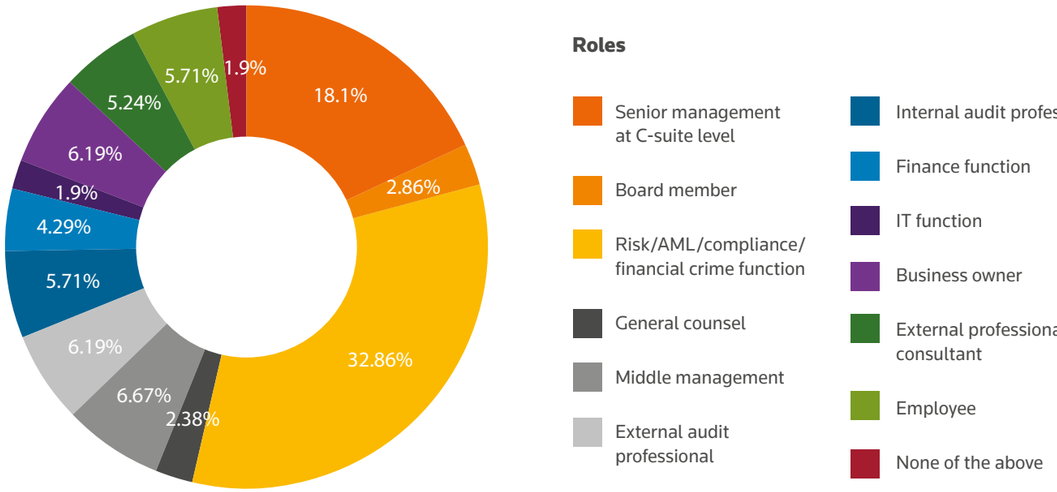
[11] http://www.gfintegrity.org/

Featured questions:
6, 13 and 18

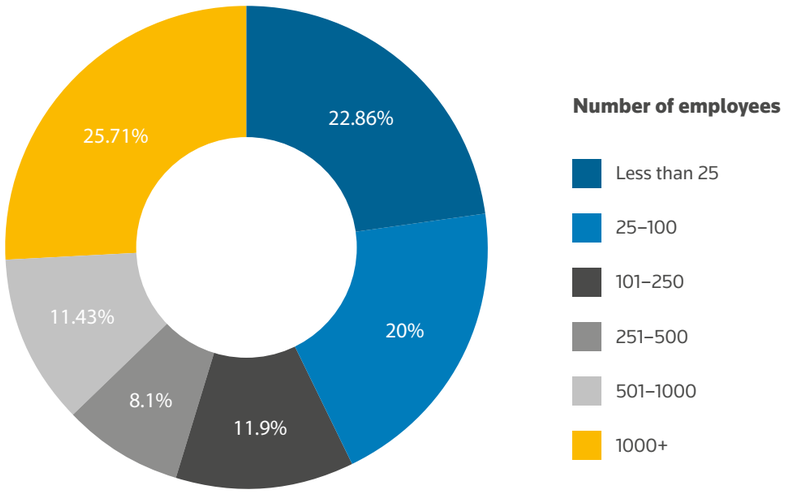
Full survey results can be found on pages 24-37

SURVEY RESULTS

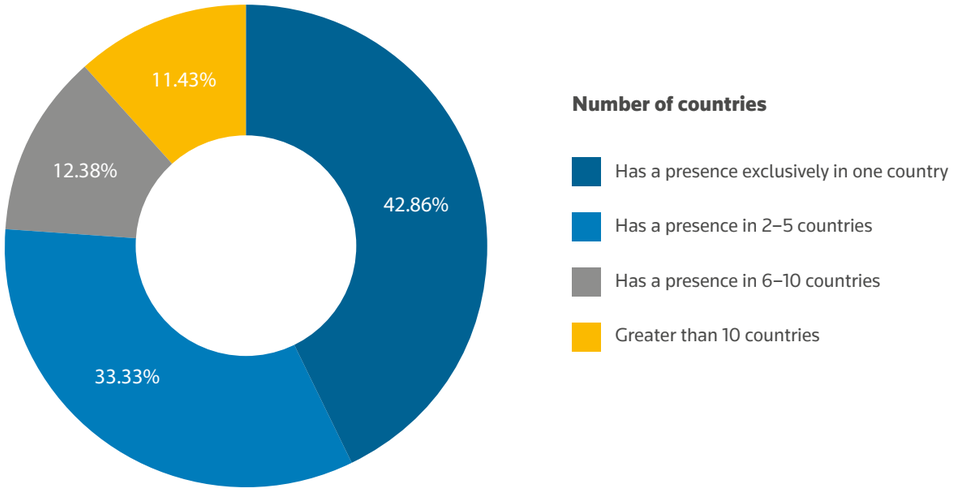
Question 1: Please choose the option that is the closet fit to your role.



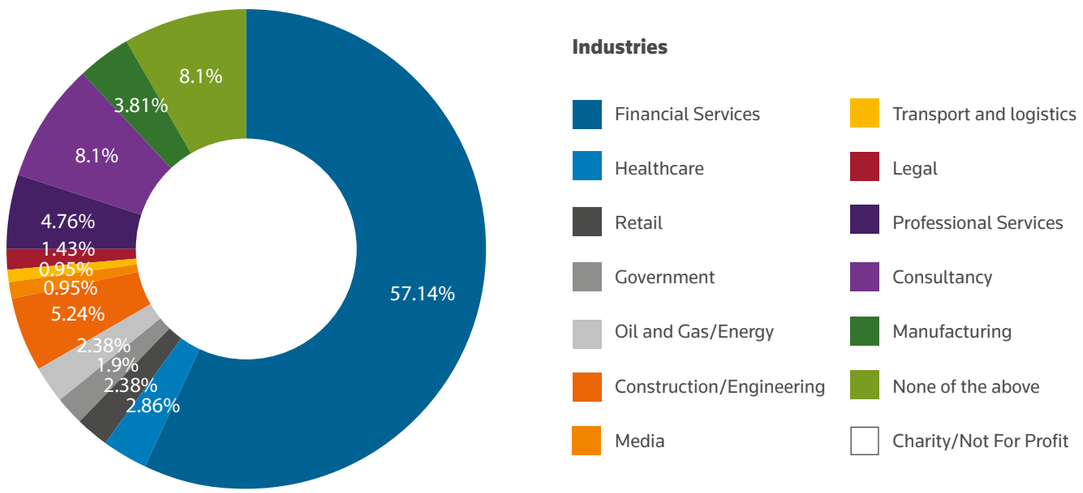
Question 2: Please indicate the number of employees your organization employs within MENA.



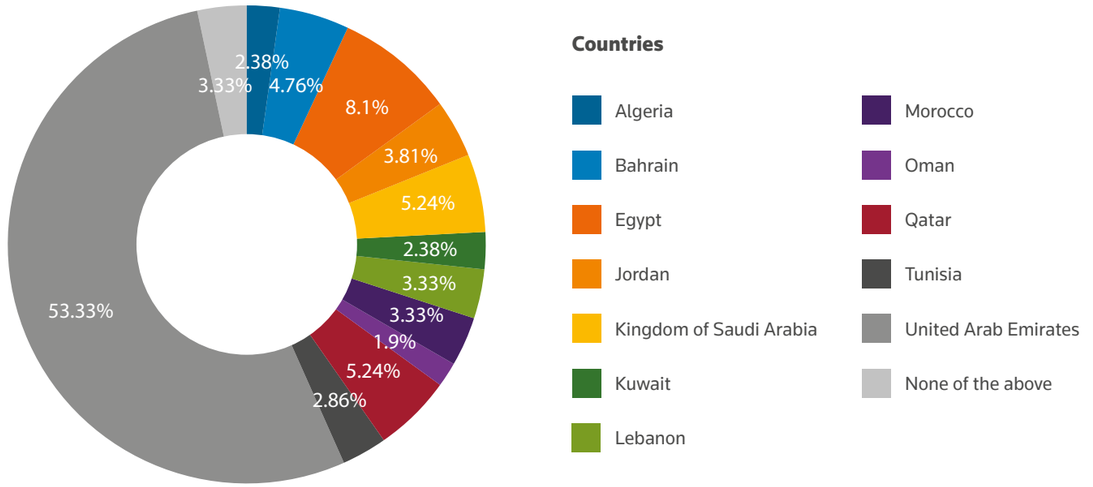
Question 3: In how many countries within MENA does your organization operate?



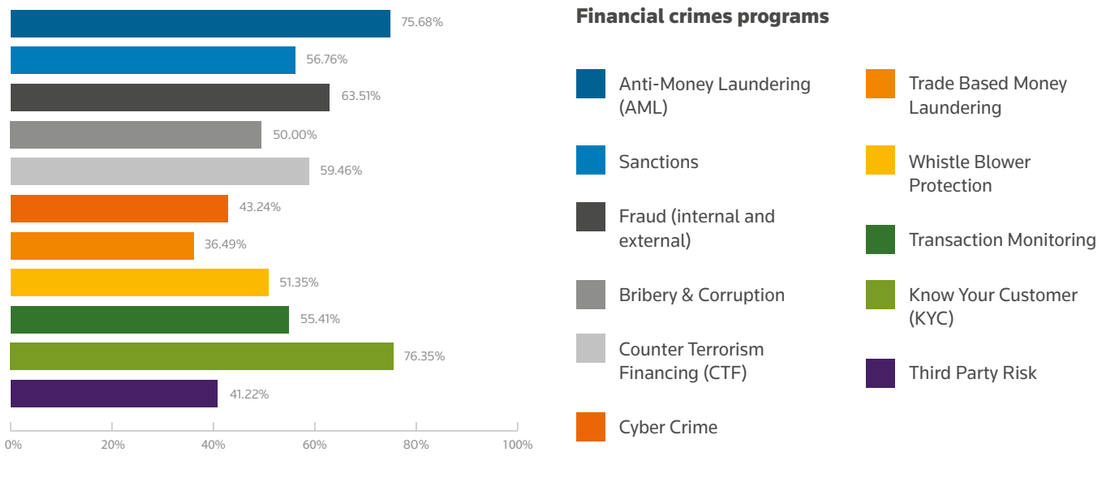
Question 4: Please indicate the primary industry in which you operate.



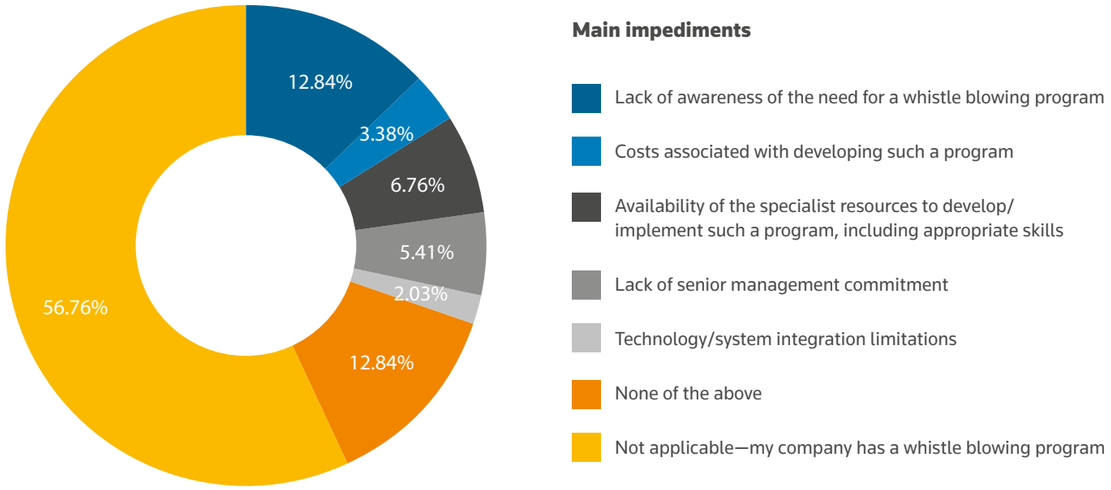
Question 5: In which country are you based?



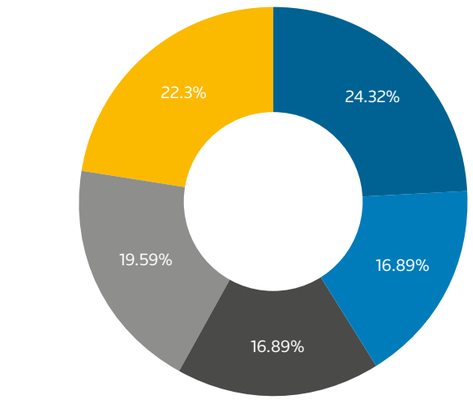
Question 6: Which of the following financial crimes programs does your organization currently have in place? Please select all that apply.



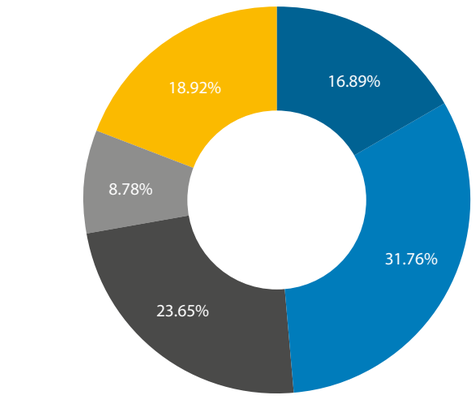
Question 7: If your company does not have a whistle blowing program, what is the main impediments for implementing it?



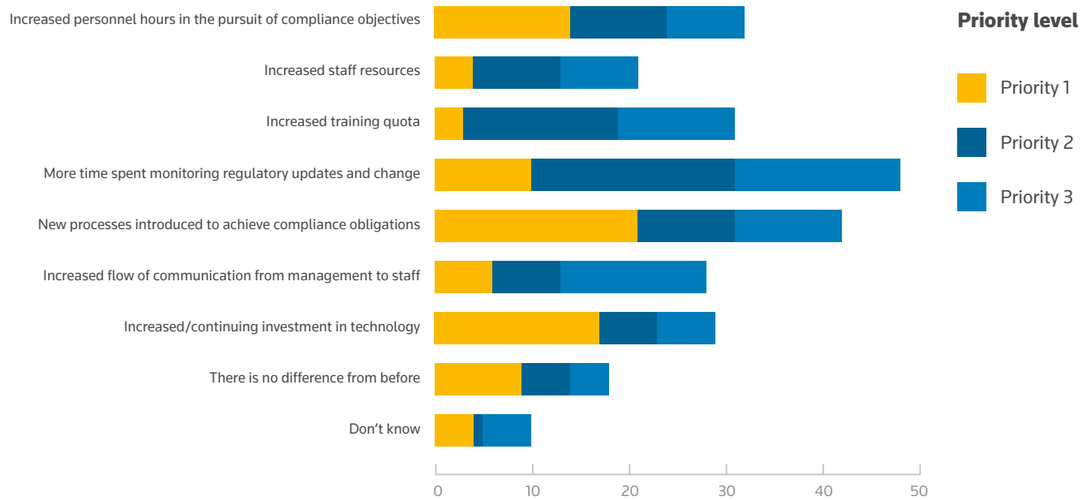
Question 8: How has your investment in anti-financial crime activity and compliance increased compared to two years ago?



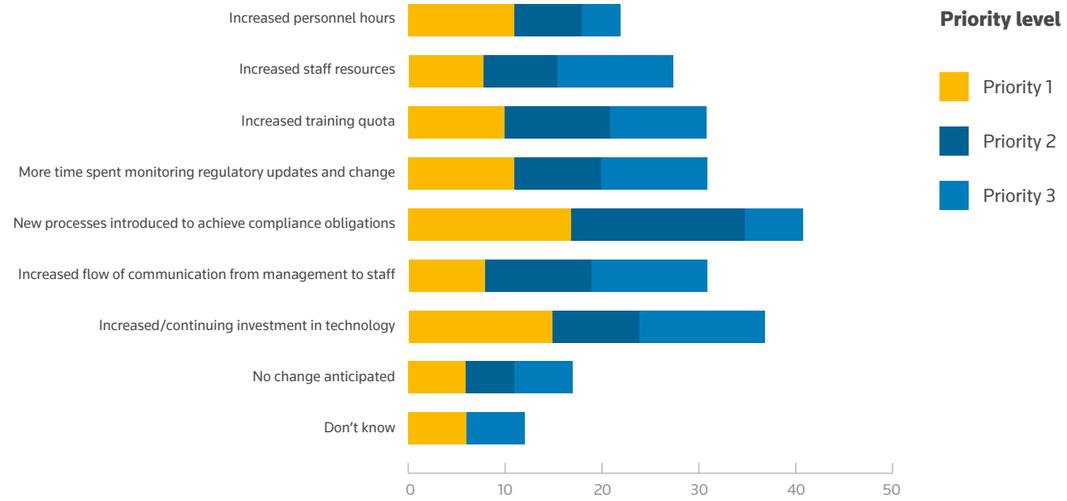
Question 9: What do you anticipate the increase in your anti-financial crime activity and compliance investment will be over the next two years?



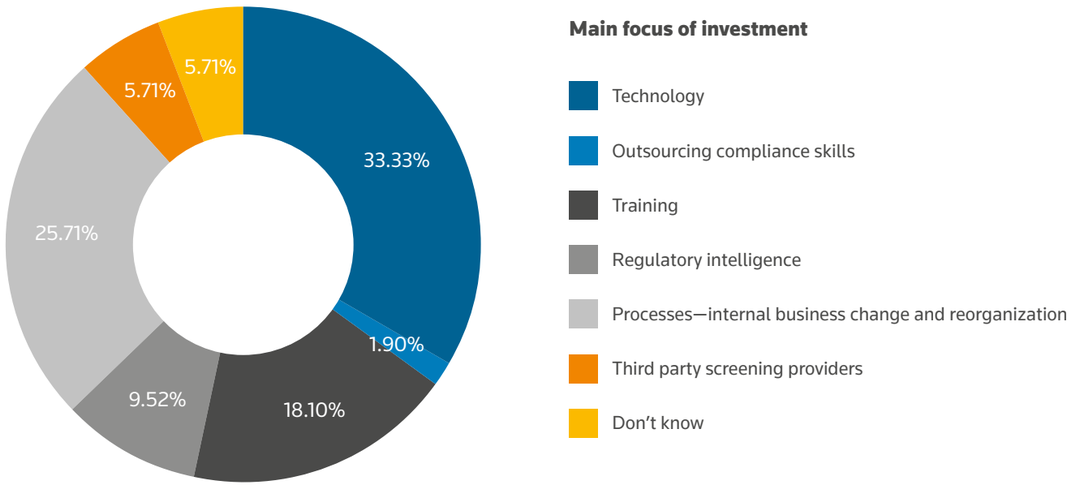
Question 10: How has increased anti-crime and compliance activity and awareness in your organization manifested in the past two years?



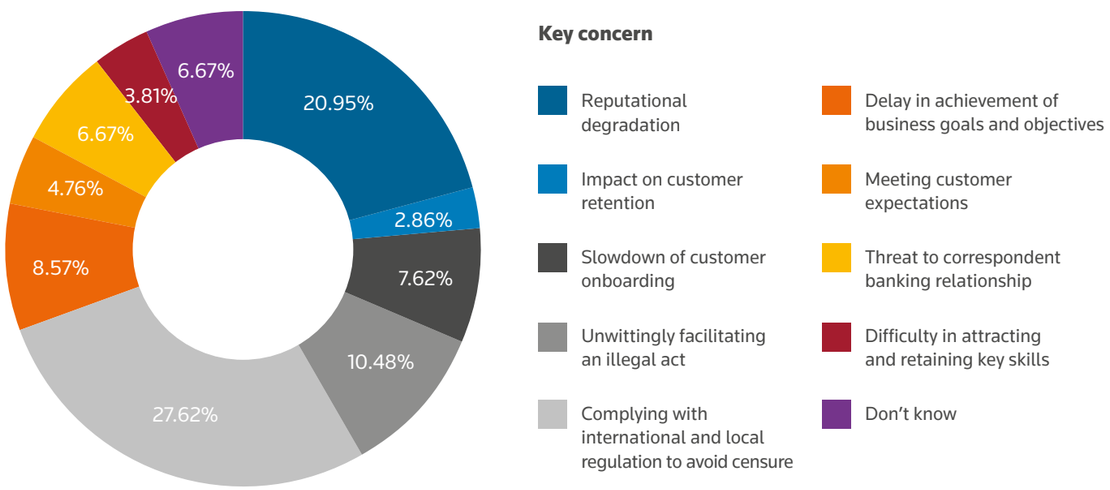
Question 11: Where and how do you expect an increase in anti-crime and compliance activity and awareness to impact your organization in the next two years?



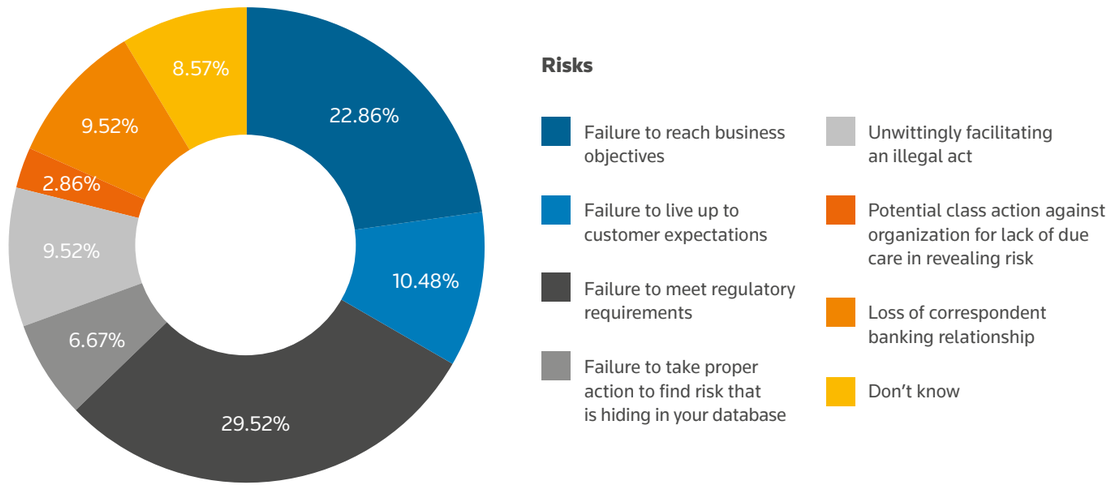
Question 12: Where is the main focus of investment to meet compliance objectives in your organization?



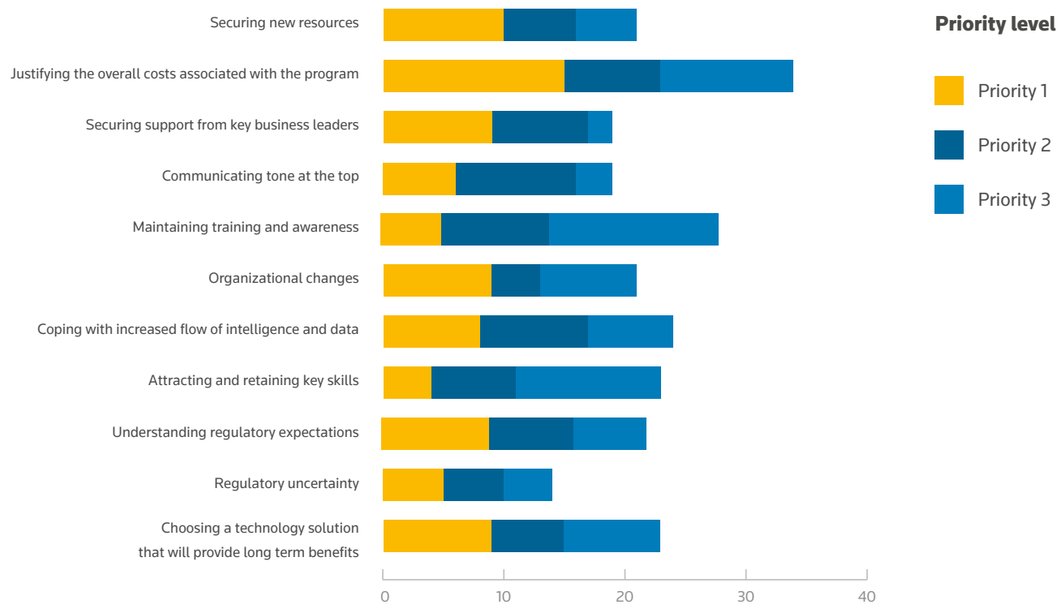
Question 13: In your organization, what do you believe is the key concern in terms of financial crime and compliance?



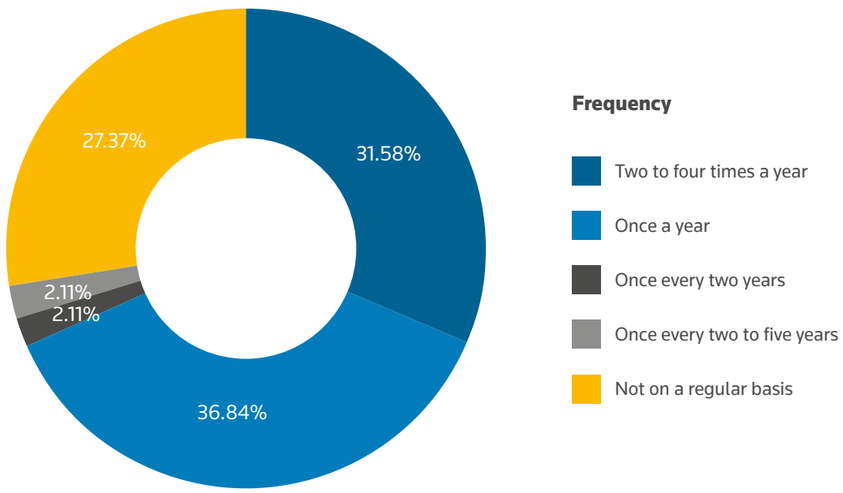
Question 14: What, in your opinion, poses the most risk to your organization?



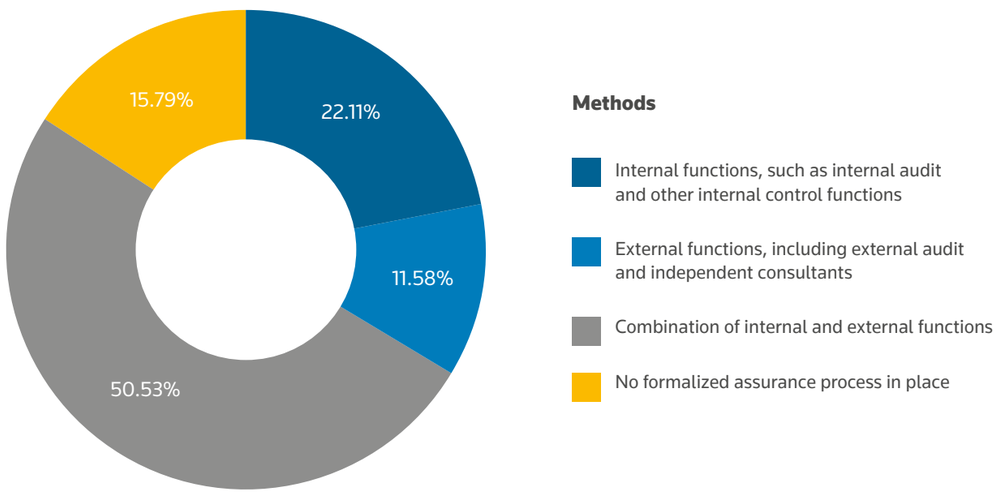
Question 15: Over the next two years what do you believe will be the biggest challenge in managing the various programs of your financial crime and compliance policy?



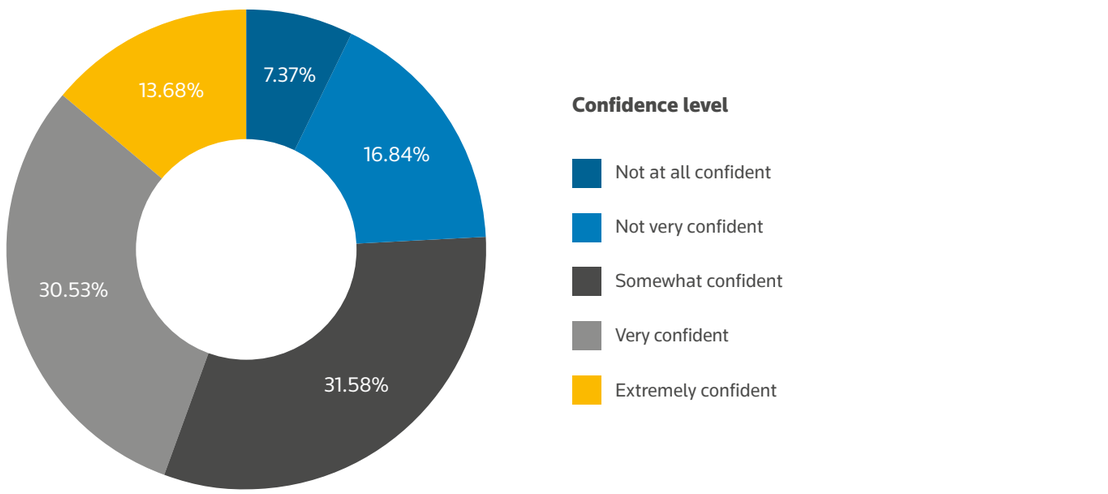
Question 16: How regularly do you assess the risks that financial crime poses to your organization?



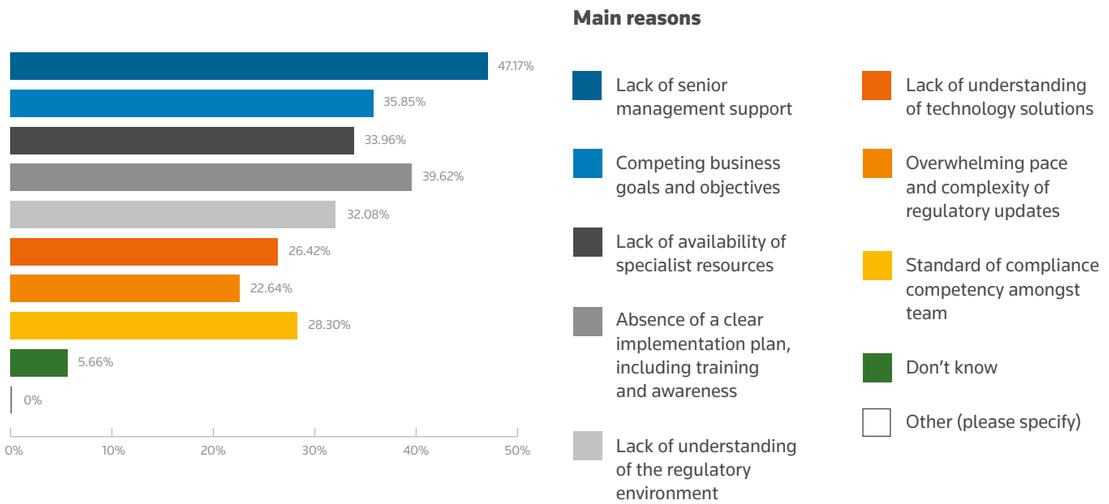
Question 17: How do you monitor and assure your financial crime program?



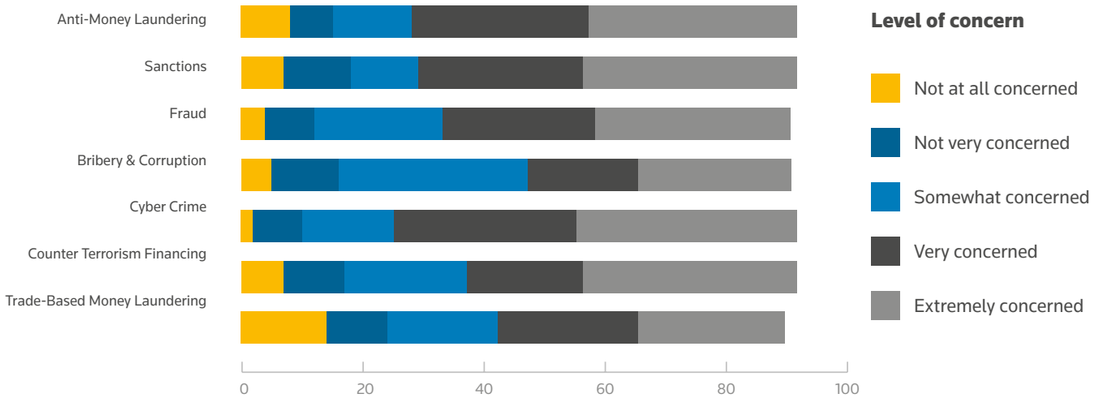
Question 18: How confident are you that your financial crime prevention program is compliant with domestic and international regulatory requirements, and that it prevents illicit activity?



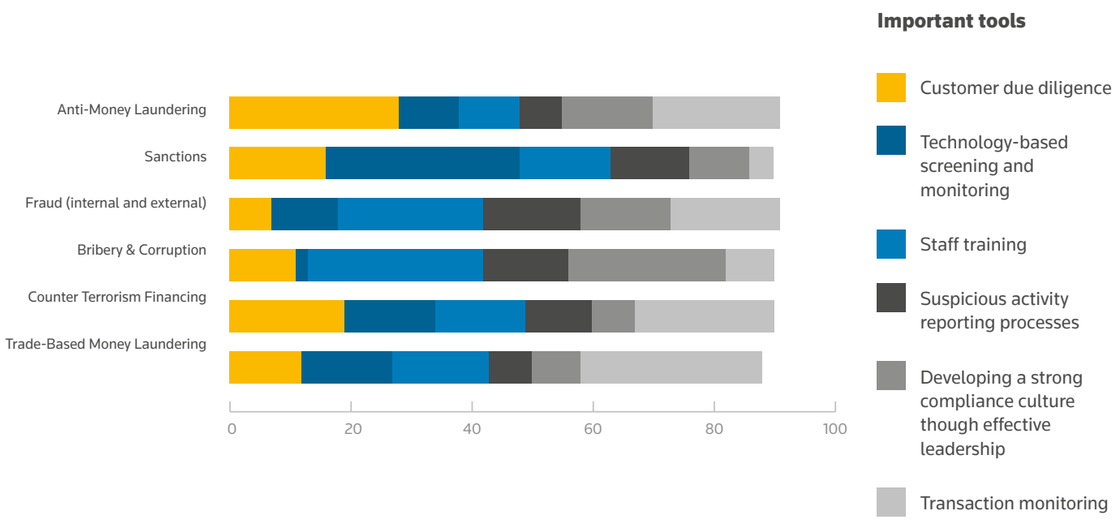
Question 19: Where there is a lack of confidence in your financial crime program, what are the main reasons?



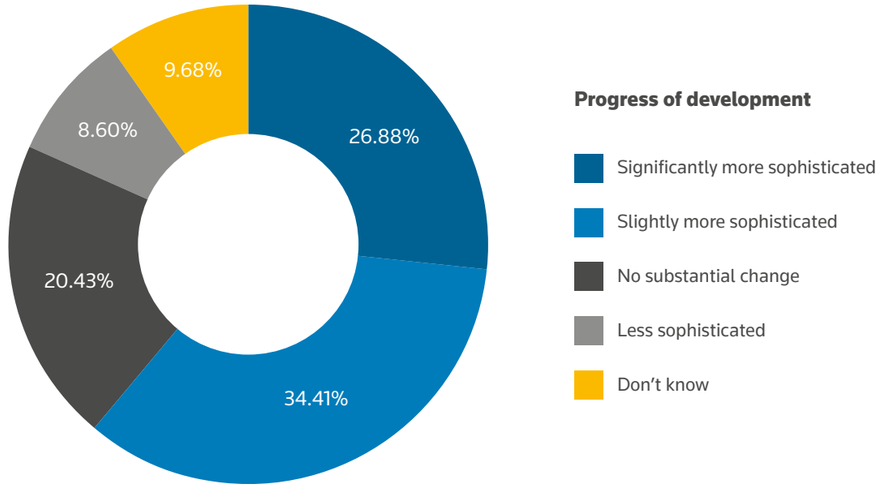
Question 20: Using the scale below, please indicate how concerned you are with the following financial crime issues?



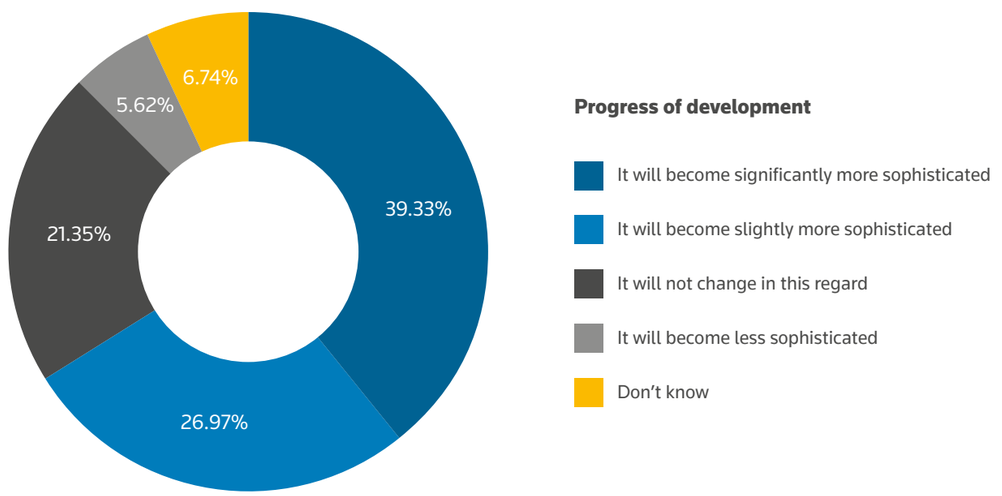
Question 21: For each of the financial crime programs shown below, please indicate which, in your opinion, is the most important tool in managing the prevention and/or detection of crime.



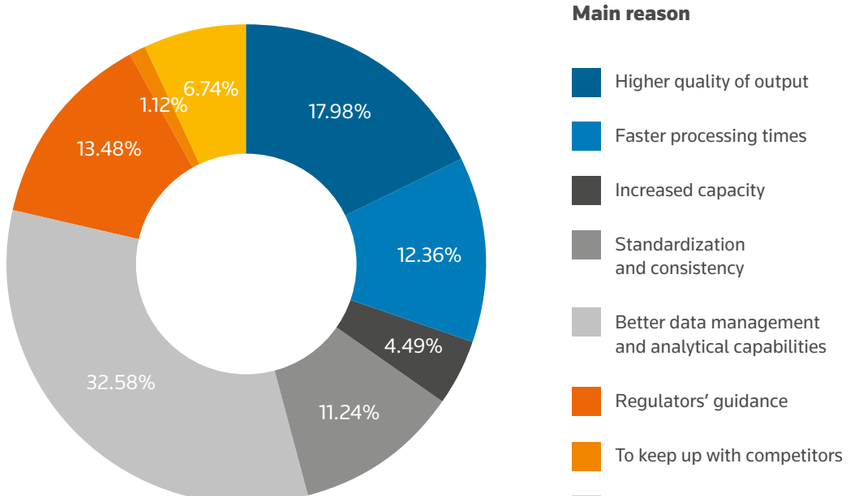
Question 22: The application of technology in the prevention of financial crime has become increasingly sophisticated, for example, the use of data analytics in transaction monitoring. In your opinion, how has your financial crime prevention program developed over the past two years?



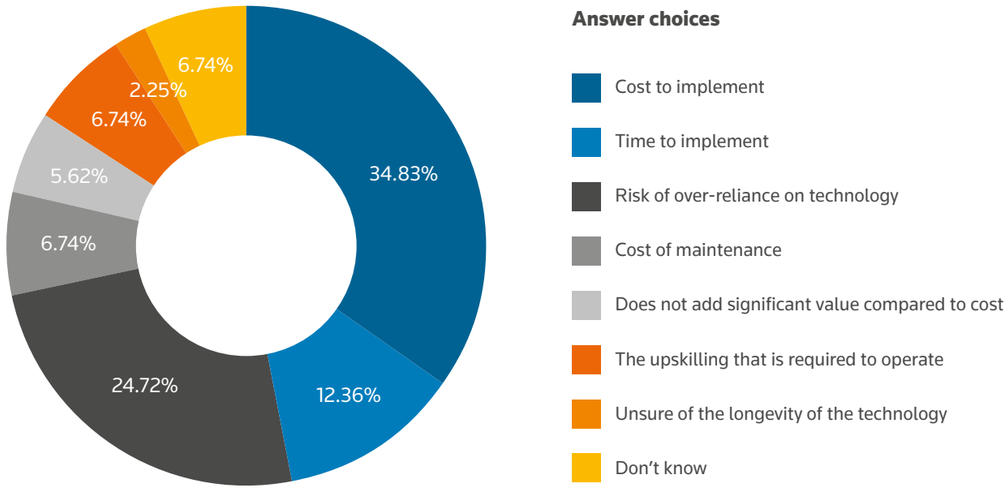
Question 23: How do you expect your technology to change in this regard over the next two years?



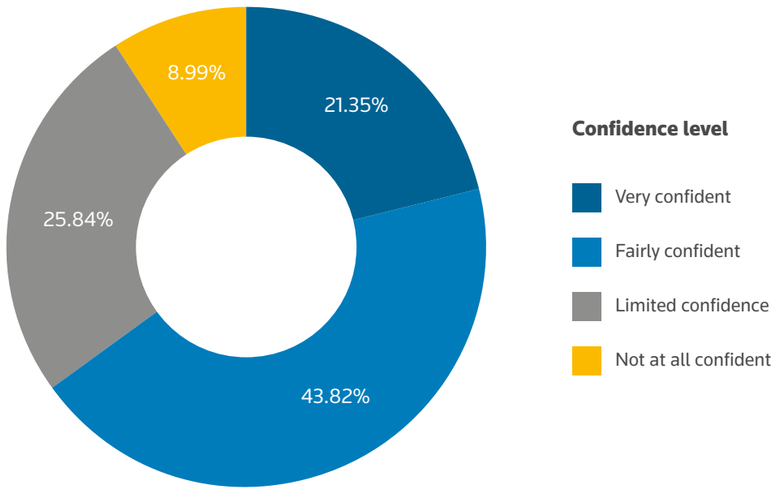
Question 24: What is the main reason you would invest in a technology upgrade?



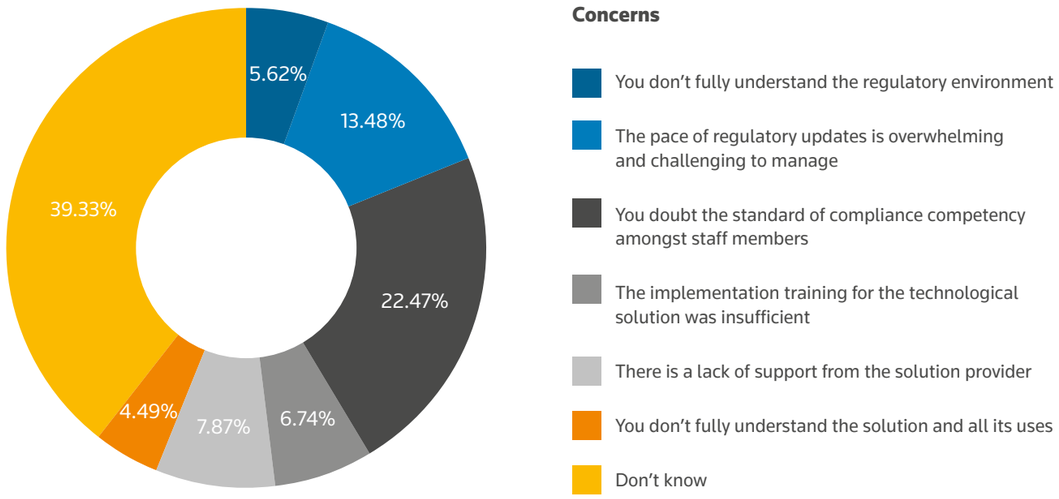
Question 25: What, in your opinion, is a major disadvantage of using an advanced technological solution?



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?



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



CLOSING THOUGHTS

There has been one constant for the compliance function over the years of this study, and that is change. It appears evident that compliance is undergoing a significant transformation, and that through the impact of innovative technology, this change may become more pronounced in 2018.

It is understandable that there is a cautiousness in compliance spend in this time of seemingly great transition.

It is important to move though, standing still invites failure, and some organizations, and compliance functions, do not have the luxury of choice. In times of uncertainty, when there is the need and desire to move forward but information is incomplete, or conflicting, it is possible to move forward by focusing on information that has a degree of certainty.

At the core of compliance is strong governance and leadership. Good, strong governance that is visible and well communicated can substantially allay concerns and boost confidence in organizational abilities, protect reputations and boost an organization's competitive edge. No matter how rapid the change may be, what level of turmoil results, if the basics of governance are strong, the compliance function and the greater organization will always benefit.

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