COST OF COMPLIANCE 2018

Stacey English
Susannah Hammond

THOMSON REUTERS®

The answer is Thomson Reuters Regulatory Intelligence

Thomson Reuters Regulatory Intelligence is a single solution that empowers you to make well-informed decisions to confidently manage regulatory risk, while providing the tools to make proactive decisions and action change within your organization.

Learn more at risk.tr.com

THOMSON REUTERS®

REUTERS/Ilya Naymushin

Table of contents

Front cover: © Dreamstime

With thanks to Chloe Bloomfield and Helen Camfield

REUTERS/Shutterstock

EXECUTIVE SUMMARY

Thomson Reuters has carried out its annual survey on the cost of compliance and the challenges financial services firms expect to face in the year ahead. The survey is now in its ninth year and generated responses from over 800 compliance senior practitioners worldwide, representing global systemically important financial institutions (G-SIFIs), banks, insurers, broker-dealers and asset managers. As with all previous years, the report builds on annual surveys of similar respondents and, where relevant, highlights year-on-year and regional trends.

The cost of compliance survey report has become the trusted voice for risk and compliance practitioners around the world. Last year's report was read by nearly 9,000 entities including firms, G-SIFIs, regulators, law firms, domestic governments and consultancies. The unparalleled insight into the frank concerns and issues shared by practitioners have, once again, given a wealth of information into the reality and challenges faced across all industry sectors. Thomson Reuters extends its profound thanks to all respondents along with a continued assurance that the responses will remain confidential.

The survey findings aim to help regulated firms with planning and resourcing, while allowing them to benchmark their own practices and experiences to determine whether their strategy and expectations are in line with the wider industry. The experiences of G-SIFIs are analyzed where these can provide a sense of the approach taken by the world's largest financial services firms.

In the last couple of years, the cost of compliance survey reports have highlighted emerging resource constraints which, combined with continuing regulatory uncertainty, suggested something of a pivot point for firms and their approach to risk and compliance. This year what is beginning to emerge is, in addition to firms seeking more creative solutions to risk and compliance challenges, a sense of increasing pressure on senior managers to both understand and cope with evolving regulatory expectations.

The main points to note are:

- Biggest compliance challenges: Compliance practitioners continue to identify managing and coping with continuing regulatory change as their biggest challenge. For 2018, data privacy and the global ramifications of the implementation of the European General Data Protection Regulation (GDPR) have been specifically highlighted as a key concern, which is a distinct shift from the challenges highlighted for 2017.

- Compliance budgets continue to increase: 61 percent of firms are expecting an increase in their total compliance budget in 2018 (53 percent in 2017). This is somewhat moderated in the G-SIFI population where 49 percent reported that their total compliance team budget would increase in the year ahead. This is in part reflected in the marginal rise in the expectations regarding the cost of senior compliance staff, with 66 percent of firms expecting an increase in the next 12 months compared to 60 percent in 2017.

- Evolving compliance resources: Alongside increasing budgets for 2018, 52 percent of firms expect the size of their compliance team to remain the same in 2018 and 43 percent expect it to grow. In the G-SIFI population, 43 percent expect the size of their compliance team to stay the same, 46 percent expect the team to grow and 11 percent expect the team size to reduce in 2018. G-SIFIs have been seen as a leading indicator for future compliance trends and the changing picture presented by the largest of firms shows the early signs of beginning to reconsider the shape, size and skill set of compliance as some teams grow and others are reduced as particular regulatory projects come to an end.

- Increasing personal liability: Personal liability continues to be a key concern for compliance professionals with 54 percent (48 percent in 2017) expecting personal liability to increase in the next 12 months (18 percent expecting a significant increase). This is likely to reflect the implementation of individual accountability regimes around the world together with the unrelenting focus on regulatory risk as shown by 74 percent of firms reporting an increase in the focus on managing regulatory risk over the next 12 months (24 percent expecting a significant increase).

- Board challenges: The biggest challenges facing boards this year have again been highlighted as continuing regulatory change and the intensity of supervisory scrutiny. In line with compliance challenges, data privacy and GDPR have been specifically highlighted as a key board challenge for 2018.

- Impact of technology: Technology is having a major impact on compliance. On the one hand, the anticipated benefits of new technology are driving an increase in the compliance function's involvement in considering solutions, with 41 percent (33 percent in 2017) expecting to spend more time assessing fintech and regtech solutions over the next 12 months, rising to 55 percent in the G-SIFI population. Balanced against the potential benefits of technology are the heightened regulatory risks associated with cyber resilience, data privacy and IT infrastructure.

- Increased regulatory liaison: The majority of firms (58 percent) are expecting to spend more time in the next 12 months liaising and communicating with regulators and exchanges with 16 percent expecting significantly more contact. There were regional variations with the Middle East (66 percent), United Kingdom (63 percent), Asia (63 percent) and Australasia (62 percent), expecting to spend the most time liaising with regulators. This, in part, reflects the need for continued personal relationship management and dialogue on regulatory expectations, ranging from culture and conduct to the implementation of personal accountability regimes.

- Outsourcing remains a major factor in compliance strategy: Almost a quarter (24 percent) of firms continue to outsource all or part of their compliance functionality (28 percent in 2017, 24 percent in 2016). The drivers for compliance outsourcing included the need for additional assurance on compliance processes, a lack of in-house compliance skills and cost. Among the specific compliance activities outsourced were annual policy reviews and email reviews.

- Accurately benchmarking total compliance spend is near impossible, particularly for larger firms, given the wide variations in scope, activities and definition of what is covered by compliance, ranging from cyber resilience and data security to conduct matters. Of those who responded, over half of firms (54 percent) allocate up to 25 percent of their total spend on operating costs maintaining continuing compliant business operations which gives an indication of the level of investment needed to meet evolving risk and compliance regulatory requirements.

INTRODUCTION AND RESULTS

Thomson Reuters Regulatory Intelligence conducted its ninth annual cost of compliance survey in Q1 2018. Over 800 responses were received from risk and compliance practitioners worldwide, including Asia, Australasia, Canada, Europe, Middle East, United Kingdom and the United States, representing firms across all sectors and sizes of the financial services industry including asset management, insurance, banking and investment.

> "Under the Hong Kong MIC regime, firms are primarily required to identify those individuals in charge of core functions and map out their responsibilities and reporting lines. In other words, we are requiring firms to consider who is accountable for what within their firms to improve overall governance. This requirement would of course help enforcement identify responsible individuals when things go wrong. And you can assume that we will make use of this additional information to hold responsible individuals accountable."
>
> **Thomas Atkinson, Executive Director, Enforcement Division, at the Securities and Futures Commission (SFC). Keynote speech at Thomson Reuters' 8th Pan Asian Regulatory Summit, Hong Kong. (October 2017)**

The world of financial services regulation continues to evolve. 2018 will see the implementation of several substantial pieces of European legislation with global ramifications. On January 3, 2018 most of the Markets in Financial Instruments II (MiFID II) and the associated Regulation (MiFIR) came into effect, though there are already questions emerging as to how long the legislation will be in place before it is reviewed again, particularly with regard to the data requirements. In May 2018, the General Data Protection Regulation came into effect, which has been highlighted as a key challenge for both boards and compliance functions. For many financial services firms there has been a huge amount of work to do on all aspects of data privacy, not least of which is the ability to consistently evidence compliance with the heightened new requirements.

A key feature of new and emerging regulatory policy is the focus on the interrelated issues of misconduct, incentives and senior manager accountability. Jurisdictions as diverse as Hong Kong, Ireland, Australia and Singapore have all introduced or are planning to introduce personal accountability regimes modeled on the Senior Manager and Certification Regime in the UK. At the supranational level, the Financial Stability Board has made the explicit link between incentives and misconduct and in April 2018 published a 'toolkit' for both firms and supervisors with the aim of strengthening governance frameworks to mitigate misconduct risk. The toolkit identifies 19 tools that firms and supervisors could use to address three overarching issues identified by the FSB as part of its earlier work on misconduct, namely:

- Mitigating cultural drivers of misconduct – including tools to effectively develop and communicate strategies for reducing misconduct in firms and for authorities to effectively supervise such approaches.
- Strengthening individual responsibility and accountability – including tools that seek to identify key responsibilities and functions in a firm and assign them to individuals to promote accountability and increase transparency.
- Addressing the "rolling bad apples" phenomenon – including tools to improve interview processes and onboarding of new employees and for regular updates to background checks to avoid hiring individuals with a history of misconduct.

The FSB stops short of making definitive guidance that jurisdictions should introduce a responsibility and accountability regime for senior managers, but the implicit suggestion is there that national authorities could do worse than to consider a regime like the senior managers regime in the UK. The FSB does suggest that jurisdictions consider developing a responsibility and accountability framework whereby national authorities could assess the implementation of a framework for responsibility and accountability that includes, inter alia,

- the identification of key responsibilities for individuals in the firm
- allocation of those responsibilities to specific individuals; and/or
- holding individuals accountable for the responsibilities to which they have been assigned.

The discussion goes on to consider various practical means whereby national authorities could develop a framework to identify responsibilities for individuals and hold those individuals accountable for the responsibilities to which they have been assigned. Other tools discussed include documenting responsibilities (e.g. through a responsibility map) to help authorities monitor the effectiveness of a firm's governance and identify the individual responsible for a given activity.

The continued and indeed increasing focus on personal accountability remains a challenge for firms, particularly when many regulators have evolving culture and conduct expectations.

These are pivotal times for compliance and financial services. From the focus on conduct and accountability, to disruptive developments in business models and managing regulatory risk, there's no let up in the pressure on compliance teams in the year ahead. That said, the challenges bring opportunities, from improving outcomes for customers to enabling compliance resources to add the greatest value.

We hope the findings are useful in developing and benchmarking your firm's practices.

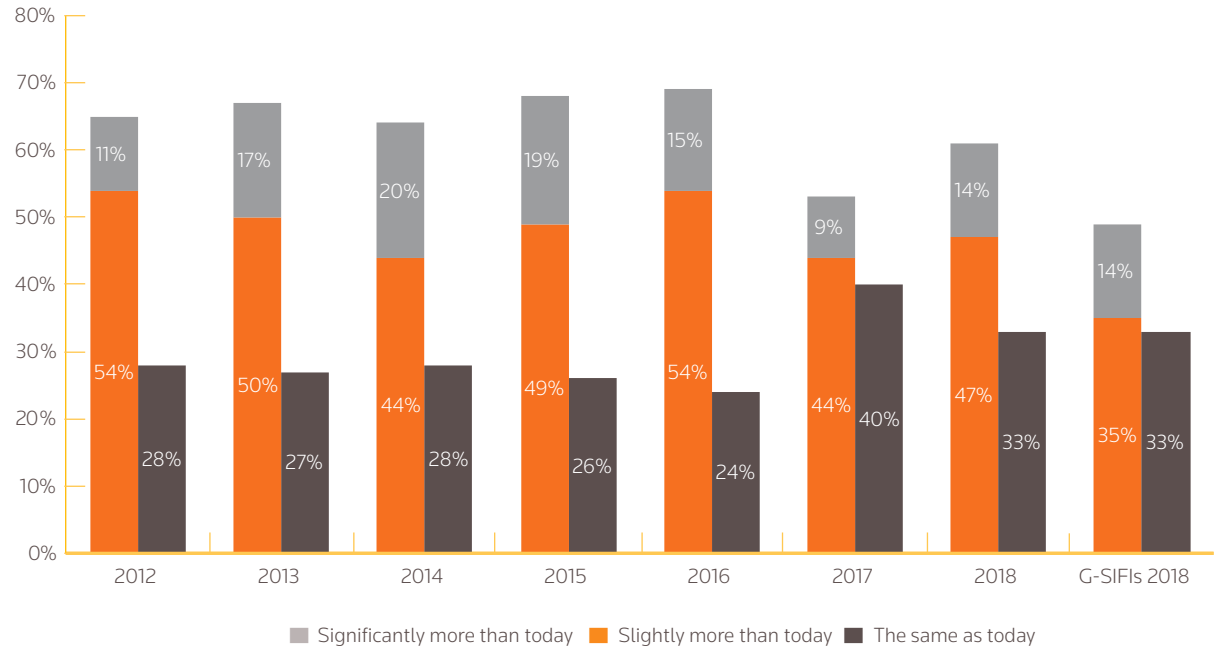
Stacey & Susannah

BUDGET AND SKILLED RESOURCES

"The industry has in turn, invested heavily in their compliance function. It is estimated that some firms could spend up to 10% of their revenues on compliance within the next few years. This is by no means an insignificant amount."

Muhammad bin Ibrahim, Governor of the Central Bank of Malaysia (Bank Negara Malaysia). Keynote address at the 9th International Conference on Financial Crime and Terrorism Financing (IFCTF), Kuala Lumpur. (October 2017)

Figure 1: Firms who expect the total compliance team budget to be the same or more over the next 12 months



Source: Thomson Reuters Regulatory Intelligence - Cost of Compliance 2018

As with prior years, the vast majority of firms (94 percent) are expecting their compliance team budget to remain the same or grow in the coming year. While this is undoubtedly good news for compliance and risk functions, resources continue to be a challenge, as they need to keep pace with unrelenting regulatory change, evolving regulatory expectations and increasing personal liability.

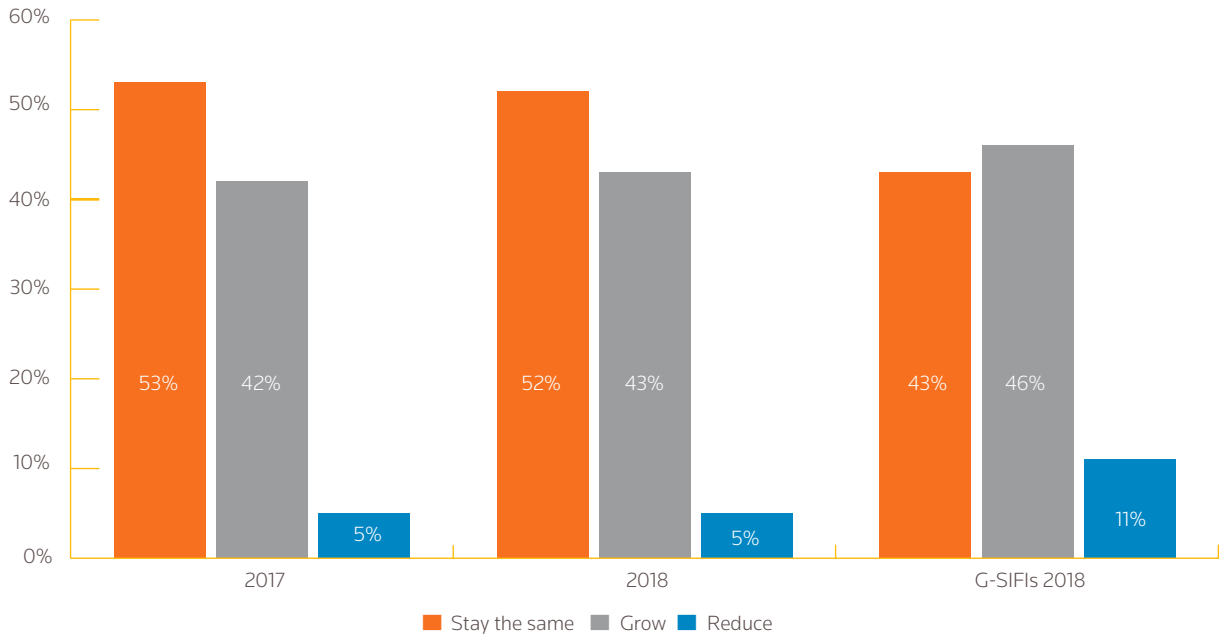
Sixty one percent of firms are expecting an increase in their total compliance team budget in 2018 (14 percent a significant increase). There were variations in the picture with 49 percent of G-SIFIs reporting their total compliance team budget would increase in the year ahead (14 percent a significant increase).

There were also variations in the regions with the majority of firms in Asia (66 percent) and the United Kingdom (65 percent) expecting total compliance team budgets to grow in the coming year.

Practitioners gave details on why they expect compliance team budgets to be slightly or significantly more in the coming year as:

- Additional legislation;
- Need for additional skilled and senior resources;
- Developing internal policies and procedures;

Figure 2: Over the next 12 months, I expect the size of my compliance team to...



Source: Thomson Reuters Regulatory Intelligence - Cost of Compliance 2018

- Focus on implementing new regulatory requirements (GDPR, MiFID II compliance);
- More training required;
- Outsourcing specific services;
- Compliance monitoring tools and activities;
- Increased personal liability.

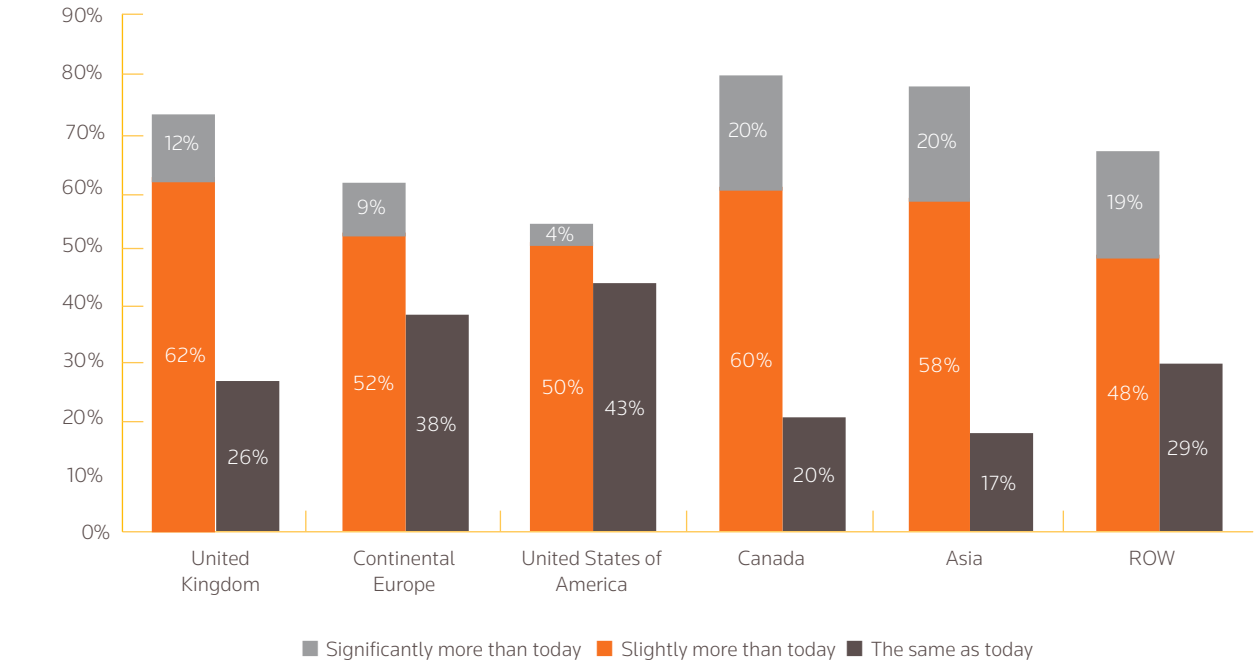
In the overall population of firms, the year on year results are very consistent with 52 percent of firms expecting the size of their compliance team to remain the same in 2018 and 43 percent expecting it to grow.

There is a more changeable picture for G-SIFIs. For 2018, 43 percent of G-SIFIs expect the size of their compliance team to stay the same (50 percent in 2017), 46 percent expect the team to grow in 2018 (42 percent in 2017), whilst at the other end of the scale, 11 percent expect the team size to reduce in 2018 (8 percent in 2017). G-SIFIs have been seen as a leading indicator for future compliance trends and the changing picture presented by the largest of firms shows the early signs of beginning to reconsider the shape, size and skill set of compliance as some teams grow and others are reduced as particular regulatory projects come to an end.

Regionally, there are some variances. Over half (51 percent) of firms in Asia and 45 percent of firms in Continental Europe expect their compliance teams to grow in the coming year. However, only 29 percent of firms in the United Kingdom expect compliance teams to grow in the year ahead, the lowest percentage across all other regions.

> "Our regulatory system was not designed as a police state, and this is deliberate. Instead, our system was designed on the premise that participants should also do their part to ensure the system operates appropriately. I think 'professionalism' is a good description of the role that is expected of participants."
>
> James Shipton, Chair of the Australian Securities & Investments Commission (ASIC). Regulatory address at the AFR Banking and Wealth Summit 2018, Sydney. (April 2018)

Figure 3: Over the next 12 months, I expect the cost of senior compliance staff to be...



Source: Thomson Reuters Regulatory Intelligence - Cost of Compliance 2018

There were also some clear regional variances on the cost of senior compliance staff. A fifth of firms in Canada and Asia expect the cost of senior compliance staff to increase significantly over the next 12 months, compared to just 4 percent of firms in the United States of America.

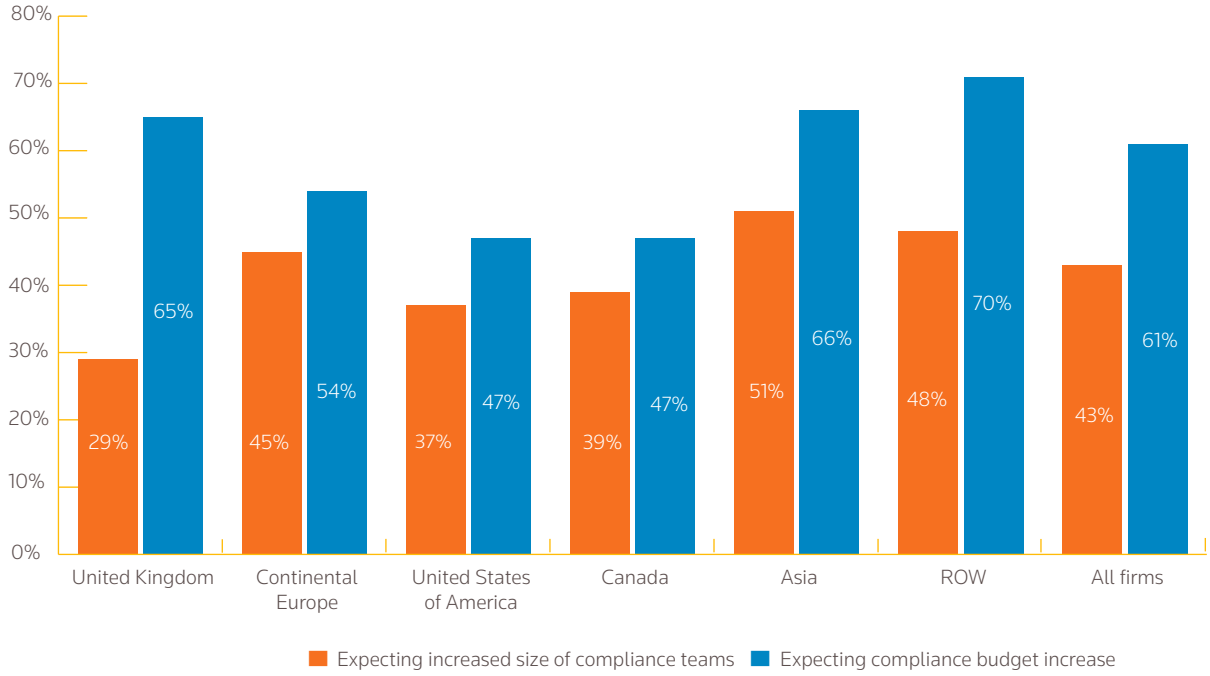
The top three reasons why firms expect senior compliance to be significantly more expensive in the coming year were:

- Demand for skilled staff and knowledge (86 percent);
- Additional senior staff required to cope with volumes of regulatory requirements (73 percent); and
- Increased personal liability (52 percent)

Overall there is a clear picture that the vast majority of firms expect the cost of senior compliance staff to either remain the same or grow in the coming year. The increase in expected cost of senior compliance staff is reflected in the results for both total team budget and the expected size of compliance teams. It is also apparent that the consistent demand for high quality compliance skills and knowledge has not abated reflecting the diverse and often challenging remit of senior compliance professionals in financial services.

Across the board the expectation is that compliance budgets will grow, though it will be a firm-by-firm consideration as to whether the expected increase in compliance budget is sufficient to cover the likely increase in the size of compliance teams. Overall a positive picture is painted with 43 percent of firms expecting the size of their compliance team to increase being outweighed by the percentage of firms who expect the size of their compliance budget to grow (61 percent) in the next 12 months.

Figure 4: Expected increase in the size of compliance teams versus expected increase in total compliance team budgets



Source: Thomson Reuters Regulatory Intelligence - Cost of Compliance 2018

REUTERS/Clodagh Kilcoyne

PERSONAL LIABILITY

"By being smart and resourceful in the Cyber arena, we hope to discourage misconduct before it takes root. And in a world of finite resources, it is imperative that enforcement actions advance goals of specific and general deterrence.

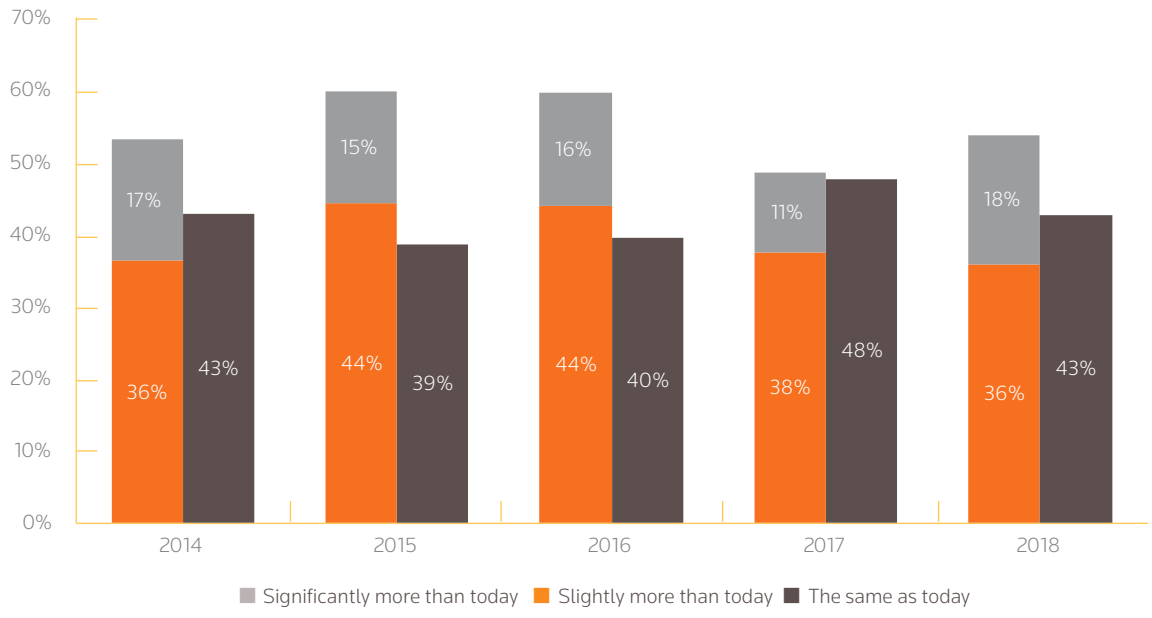
One of the primary ways we do that is with a focus on identifying and charging culpable individuals. Bad actors undermine the hard-earned trust essential to the health and stability of our capital markets. I view individual accountability as perhaps the most effective general deterrent tool in our arsenal, because it can have a broad effect on corporate culture in a way that immeasurably benefits individual investors, preventing misconduct before it starts."

Steven Peikin, Co-Director, Division of Enforcement at the U.S. Securities and Exchange Commission (SEC). Keynote address to the UJA Federation, New York. (May 2018)

Personal liability and accountability continues to be a key concern for compliance officers. While there has been some fluctuation in views over the last five years, the perception that the personal liability of compliance professionals will either stay the same or grow has shown remarkable persistence. Of potential additional concern for 2018 is the 18 percent who expect the personal liability of compliance professionals themselves to be significantly more in the coming year, which may reflect the roll out of personal accountability regimes around the world.

The introduction of accountability regimes worldwide, such as the UK's Senior Managers and Certification Regime (SMCR), Hong Kong's Managers-in-Charge (MIC), and Australia's Banking Executive Accountability Regime (BEAR), has had its impact on practitioners' view on personal liability. Almost a quarter (24 percent) of firms in Asia, and almost a fifth (19 percent) of firms in the UK, expect personal liability to significantly increase in the year ahead.

Figure 5: Over the next 12 months, I expect the personal liability of compliance professionals to be:



Source: Thomson Reuters Regulatory Intelligence - Cost of Compliance 2018

"Clear accountability and proper conduct are important elements of good governance and sound business practice. Persistent misconduct and a lack of individual accountability by persons in charge will erode public confidence in our Financial Institutions (FIs). We expect the boards and senior management of FIs to instil a strong culture of responsibility and ethical conduct."

Mr. Ong Chong Tee, Deputy Managing Director (Financial Supervision) at the Monetary Authority of Singapore. Response to Proposed Guidelines on Individual Accountability and Conduct. (April 2018)

Regional regulatory response: Singapore

In April 2018 the Monetary Authority of Singapore (MAS) proposed guidelines to strengthen individual accountability of senior managers and raise standards of conduct in financial institutions (FIs). The guidelines are a key part of MAS' broader efforts to foster a culture of ethical behaviour and responsible risk-taking in the financial industry. The proposed guidelines set out MAS' supervisory expectations of boards and senior management with respect to individual conduct and behaviours. They are not designed to be prescriptive. It is ultimately the responsibility of each FI to hold its senior managers accountable for their actions and ensure proper conduct amongst their employees.

The guidelines reinforce FIs' responsibilities in three key areas:

- Promote individual accountability of senior managers - FIs should identify senior managers who are responsible for core management functions and clearly specify their individual accountabilities. FIs should ensure that senior managers are fit and proper for their roles and hold them responsible for the actions of their staff and the conduct of the business under their purview. The FI's management structure and reporting relationships should be clear and transparent.
- Strengthen oversight of employees in material risk functions - FIs should identify employees who have the authority to make decisions or conduct activities that can significantly impact the FI's safety and soundness, or cause harm to a significant segment of the FI's customers or other stakeholders. FIs should ensure that such employees are fit and proper and are subject to an appropriate incentive structure and effective risk governance.
- Embed standards of proper conduct among all employees - FIs should have in place a framework that promotes and sustains the desired conduct among employees. The conduct framework should articulate the standards of conduct expected of all employees and be effectively communicated and enforced throughout the organisation. Policies and processes should be implemented to ensure regular monitoring and reporting of conduct issues to the board and senior management. There should also be appropriate incentive systems and effective feedback channels, such as whistle-blowing mechanisms, in place.

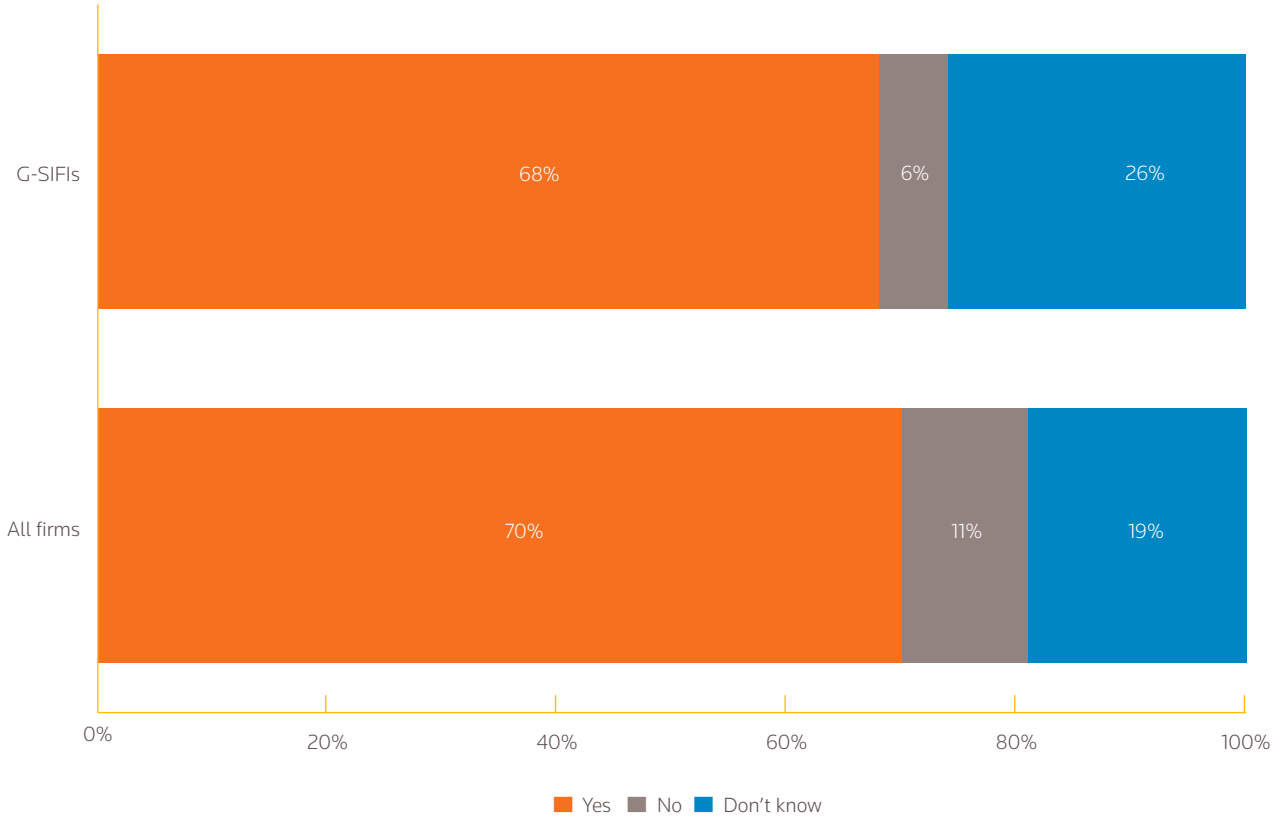
The guidelines are designed to provide FIs with the operational flexibility to determine the most appropriate ways to achieve the desired outcomes of proper accountability and conduct. The MAS has made clear that it intends to monitor FIs' progress in implementing the guidelines through its regular supervisory engagements.

> "Culture is often viewed as a "soft" topic, but I would disagree. The financial penalties associated with misconduct are anything but soft—with bank fines since the crisis estimated at more than $320 billion as of year-end 2016. The hit to a bank's reputation from misconduct can also be quantified through, for example, the associated impact on its share price or funding costs. Culture should be about concrete incentives and behaviors that help achieve specific goals, implying that it should not be viewed as a "soft" issue."
>
> William C. Dudley, President and Chief Executive Officer of the Federal Reserve Bank of New York. Remarks at the US Chamber of Commerce, Washington DC. (March 2018)

In Ireland there are also moves towards a personal accountability regime with, in January 2018, the Central Bank of Ireland (CBI) 'strongly' recommending that reforms to assign responsibility to senior personnel should be adopted and that such reforms 'should be modeled on the Senior Managers and Certification Regime in the UK'. The CBI noted that the UK Financial Conduct Authority has found the new approach 'effective' and that 'great benefit has been found in other jurisdictions in relation to the adoption of this policy'.

Culture and conduct risk are likely to also be a key driver of personal liability concerns as was highlighted in Thomson Reuters' fifth annual Culture and Conduct Risk survey report which found that 70 percent of firms consider the regulatory focus on culture and conduct risk will increase the personal liability of senior managers.

Figure 6: Do you think that regulatory focus on culture and/or conduct risk will increase the personal liability of senior managers?



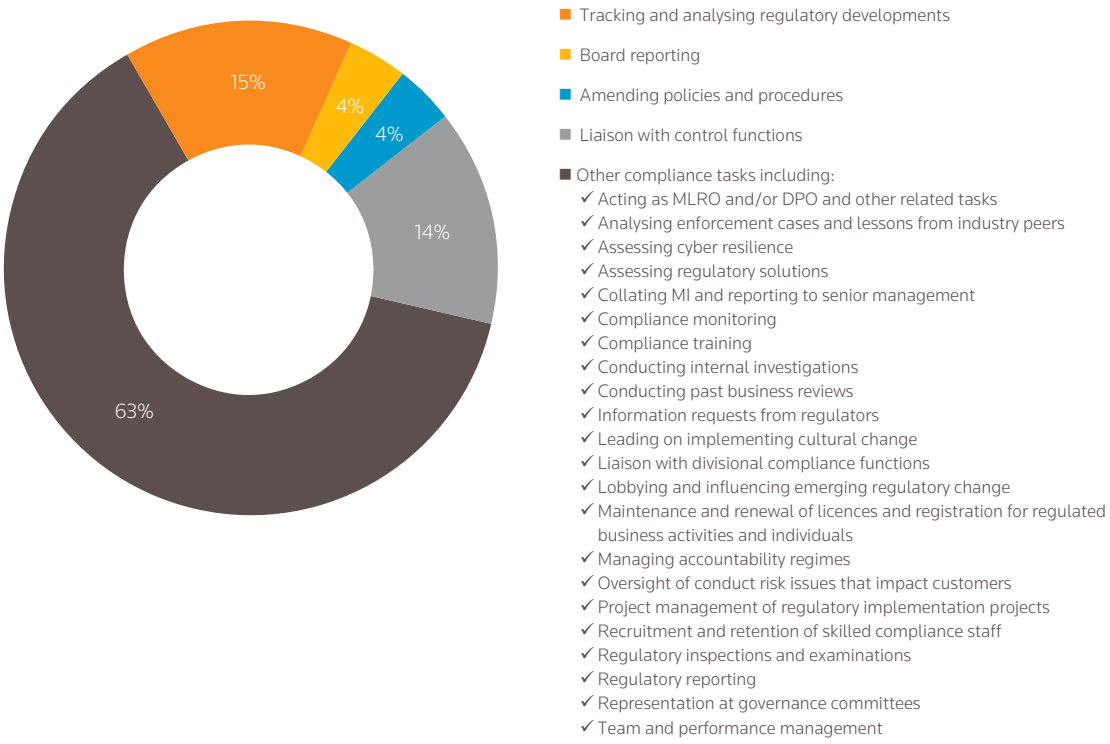
Source: Thomson Reuters Regulatory Intelligence - Culture and Conduct Risk 2018 survey

TYPICAL WEEK OF A COMPLIANCE OFFICER

"...I would recognise that there are risks of you being spread too thinly; and the evolution of your responsibilities not being matched by the changes in resource levels and skillsets. And, perhaps this is evidenced by the issues that we continue to see in firms, including in compliance functions. You need to be bold and noisy not only in the identification of risk and issues, but also in your own needs, to serve your businesses and your customers as you need to, and they deserve."

Ed Sibley, Deputy Governor of the Central Bank of Ireland. Address at the Association of Compliance Officers of Ireland annual conference, Dublin. (November 2017)

Figure 7: Typical week of a compliance officer in 2018



Source: Thomson Reuters Regulatory Intelligence - Cost of Compliance 2018

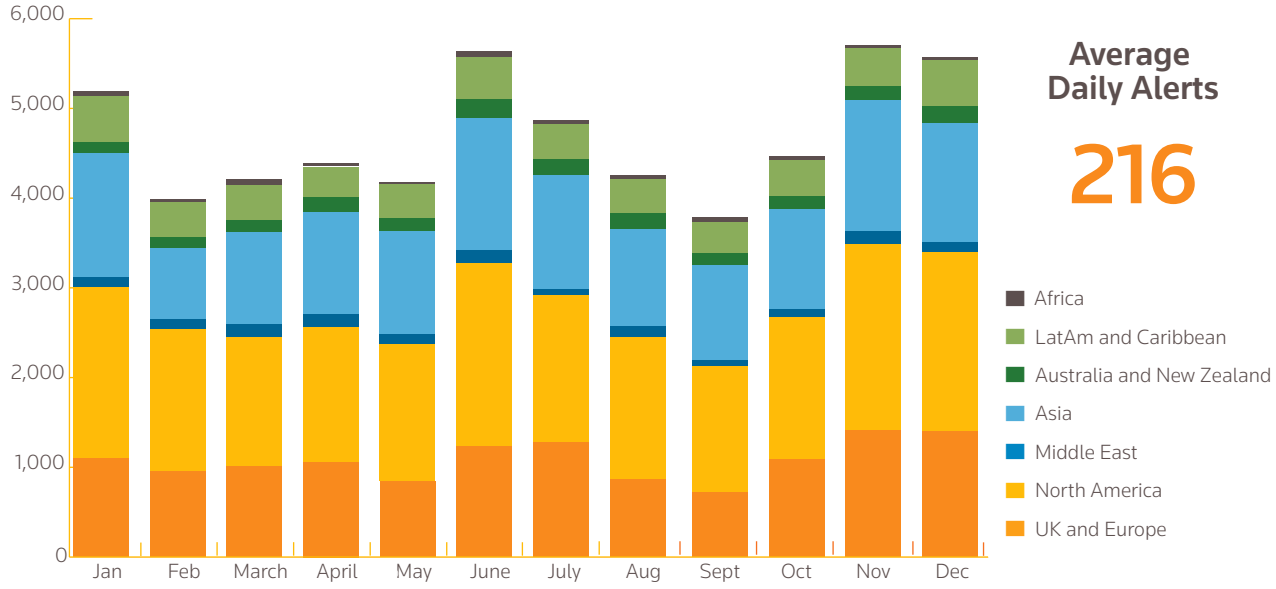
Being a financial services compliance officer has always been a juggling act of expanding remit and expectations, potentially limited resources, the need for additional or enhanced skills all with an overlay of increasing personal liability. What could be seen as the 'core' compliance tasks of tracking and analyzing regulatory developments, board reporting, amending policies and procedures and liaising with other control functions have to compete for attention with the sheer breadth of 'other' compliance activities often deemed to be part of the role of the compliance function.

REGULATORY CHANGE AND CONTINUING UNCERTAINTY

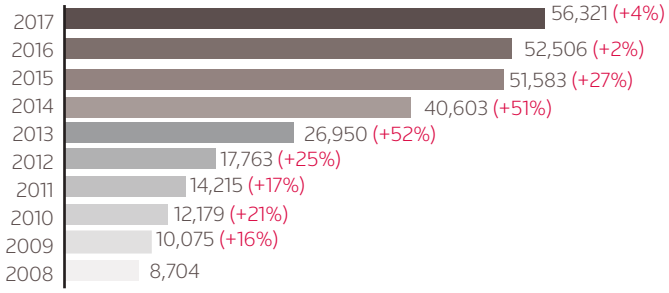
"I have no doubt that the current regulatory framework could be improved. Indeed, the official sector should assess the efficiency and effectiveness of regulations on an ongoing basis. I agree with Vice Chairman Quarles' observation that there is more we can do to make the regulatory regime more efficient, transparent, and simple—including relief for small banks, greater tailoring based on a firm's level of systemic importance, and simplifying the Volcker Rule. Some of these changes have already been adopted or are in process."

William C. Dudley, President and Chief Executive Officer at the Federal Reserve Bank of New York. Speech at the U.S. Chamber of Commerce, Washington, D.C. (March 2018)

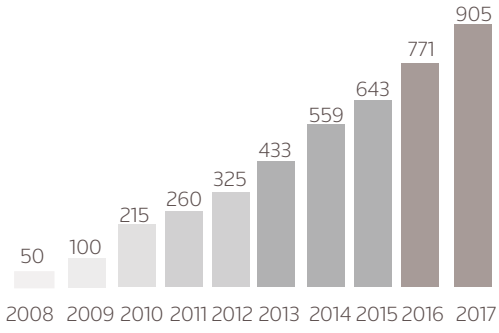
Figure 8: Regulatory Activity Tracked in 2017



Total Yearly Alerts



Total Organisations Monitored



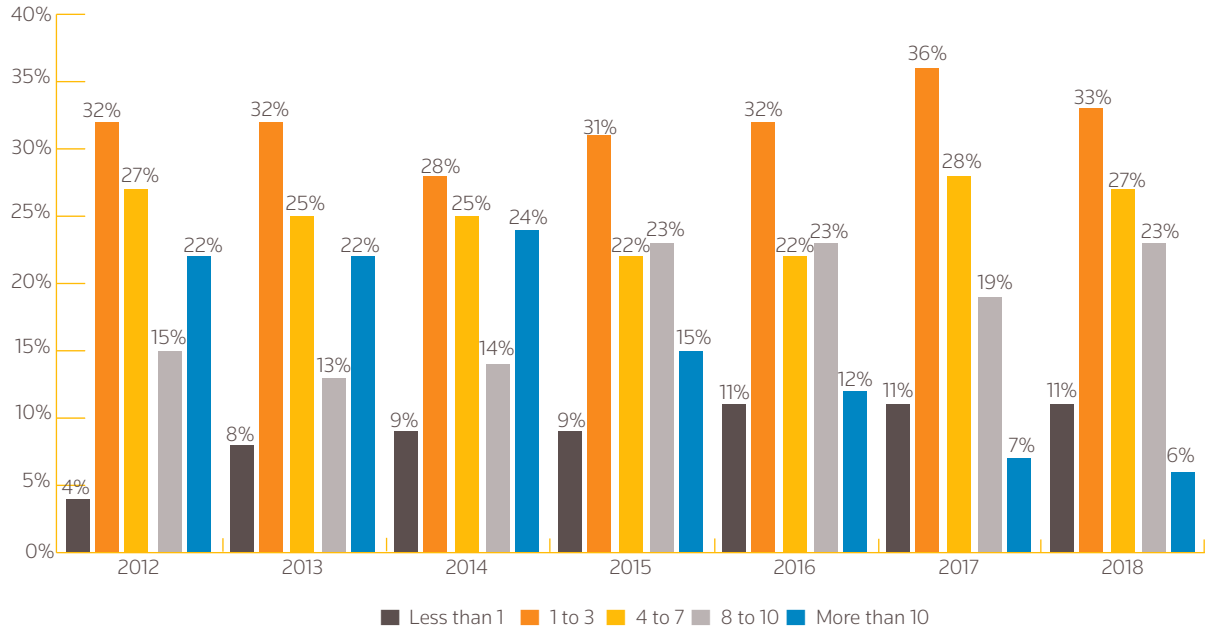
Source: Thomson Reuters Regulatory Intelligence - Cost of Compliance 2018

The pace and scope of regulatory change is continuing unabated. Both the Financial Stability Board and the EU have signaled that they are to review the implementation and impact of regulatory changes to assess whether the changes are operating as intended and have the desired effect(s). Whilst it is positive that rules and requirements are to be reviewed for effectiveness, it does mean the potential for yet more regulatory change.

During 2017, Thomson Reuters Regulatory Intelligence captured 56,321 regulatory alerts from over 900 global regulatory bodies averaging 216 updates a day. This is in comparison to an average of 201 alerts for the prior year, which in part reflects Thomson Reuters' continued expansion of regulators and rulebooks monitored.

Continuing the trend from last year's survey results, the percentage of firms spending more than 10 hours a week tracking and analyzing regulatory developments is falling. In 2018, just six percent spend more than 10 hours a week tracking and analyzing regulatory developments, after reaching a peak (24 percent) in 2014.

Figure 9: In an average week, how much time does your compliance team spend tracking and analysing regulatory developments? (in hours)

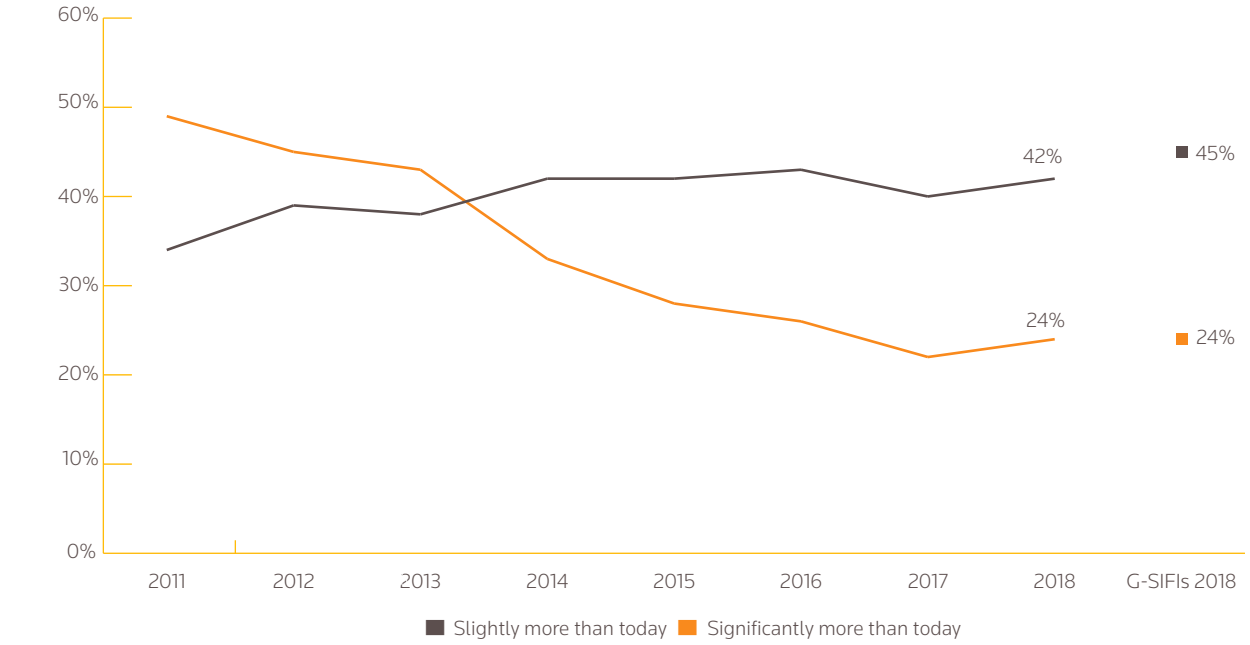


Source: Thomson Reuters Regulatory Intelligence - Cost of Compliance 2018

"Undoubtedly, the costs associated with compliance with the new regulations increase disproportionately for those entities that, due to their size, are less able to take advantage of the economies of scale that characterise the systems and processes of regulatory compliance. As I said before, the greater complexity of the new standards derives partly from the sophistication of the business models of some institutions, in many cases those that are large and internationally active. It thus could be argued that smaller institutions that specialise in more traditional intermediation activities in the domestic market face excessive costs due to the burden of complying with regulations that are not calibrated to the risks they generate."

Fernando Restoy, Chair of the Financial Stability Institute, Bank for International Settlements. Speech, "The post-crisis regulatory agenda: What is missing?" at the Círculo Financiero La Caixa, Barcelona. (February 2018)

Figure 10: Over the next 12 months, I expect the amount of regulatory information published by regulators and exchanges to be....



Source: Thomson Reuters Regulatory Intelligence - Cost of Compliance 2018

The increased use of technology and the use of creative solutions may be a driver for fewer firms reporting spending more than 10 hours in an average week on tracking and analyzing regulatory developments (6 percent in 2018; 7 percent in 2017; 12 percent in 2016).

The total number of hours compliance teams spend tracking and analyzing regulatory developments per week has remained consistent year on year, irrespective of significant regulatory developments in recent years. However, this year's results show a slight uptick, with two thirds of firms (66 percent) expect the amount of regulatory information published by regulators and exchanges to be slightly or significantly more over the next 12 months.

From a regional perspective, over a quarter (28 percent) of firms in Australasia and a quarter of firms in Asia and Continental Europe expect a significant increase in the amount of regulatory information published by regulators and exchanges. Conversely, only 8 percent of firms in the United States expect the amount of regulatory information published to increase significantly in the coming year.

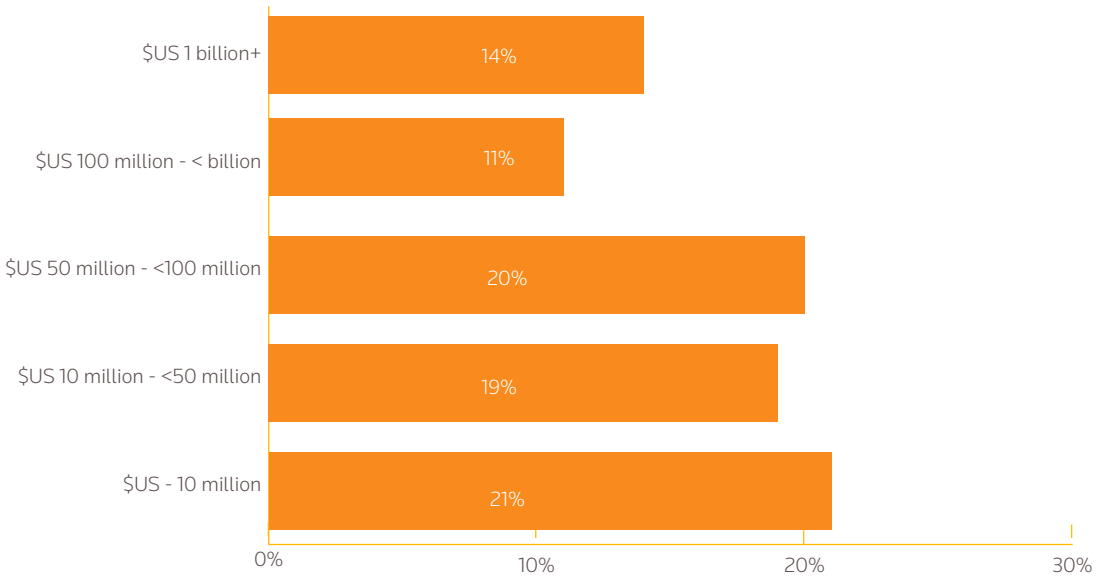
The costs of regulatory arbitrage or inequivalent regulatory regimes were the topic of a review and report by the Organization for Economic Co-operation and Development and the International Federation of Accountants.

> "...the way forward must surely be to bank our Day 1 defacto equivalence. ...and shape a regime to manage future regulatory change that ensures that... ...while our rule systems may evolve separately... ...we deliver fully equivalent regulatory outcomes... ...maintaining commitments to support open-markets and fair competition.
>
> As these rules systems for financial services evolve, the United Kingdom cannot simply be an automatic 'rule taker'.
>
> **Philip Hammond, Chancellor of the Exchequer. Speech on financial services at HSBC, London. (March 2018)**

"The findings show that regulatory divergence costs financial institutions 5-10 percent of their annual turnover (on average). This consumes scarce senior management time, as well as capital, that could otherwise be focused on identifying emerging risks in the financial system. Ultimately, these costs are a barrier to international growth: more than $780 billion annually in costs to the global economy are conservatively inferred by the findings."

Regulatory Divergence: Costs, Risks, Impacts. An International Financial Sector study by Business at OECD and the International Federation of Accountants. (February 2018)

Figure 11: Costs of regulatory divergence for smaller and larger institutions



Source: The International Federation of Accountants (IFAC) 'Regulatory Divergence: Costs, Risks, Impacts' (April 2018)

The recommendations of the regulatory divergence report focus on making more effective regulatory cooperation and harmony a priority for policy makers. The key steps highlighted to seek to curb regulatory divergence include:

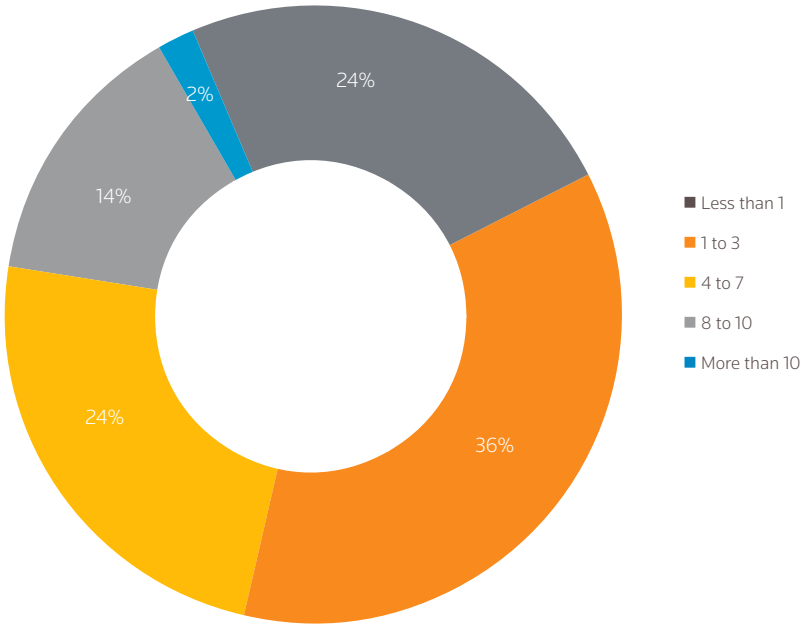
- Enhanced international regulatory cooperation
- Overall increased alignment in rules
- Improved alignment in regulatory definitions
- Better communication and awareness among regulatory agencies internationally to avoid duplicating reporting requirements and processes
- Greater overall clarity in rules and regulation

REGULATORY REPORTING

"The compound set of regulatory changes that will become applicable in 2022 require both banks and supervisors to revisit the way risk is represented, both in terms of reporting requirements and requirements of disclosure towards the markets."

Andrea Enria, Chairperson of the European Banking Authority (EBA). Speech, "Basel III 'Are we done now?'" at the Institute for Law and Finance Conference Goethe University Frankfurt Am Main. (January 2018)

Figure 12: In an average week, how much time does your compliance team spend creating and amending reports for the board (in hours)?

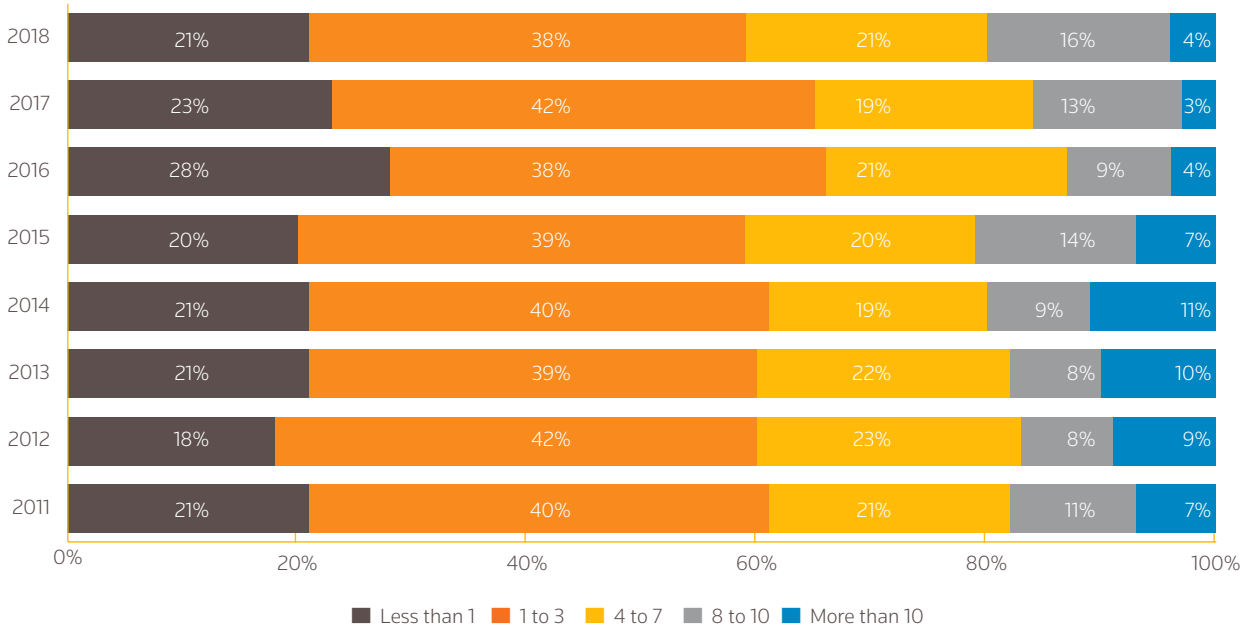


Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

Despite a marginal year-on-year fall since 2016 (29 percent), almost a quarter (24 percent) of compliance teams are still spending less than an hour a week creating and amending reports for the board. There are some regional variances, with 43 percent of firms in the United States and a third of firms in Canada spending less than an hour a week, compared to just 16 percent of firms in Asia.

All forms of internal reporting need care and attention, even more so in the current regulatory climate and focus on culture and conduct risk where context is crucial. Board reports form part of the corporate governance of a firm and are routinely reviewed by supervisors as well as the boards themselves. The qualitative nature of culture and conduct risk means that compliance reporting, along with policies, procedures and monitoring, will need to stay under constant consideration as the firm's risk-based approach continues to evolve.

Figure 13: In an average week, how much time does your compliance team spend amending policies and procedures to reflect the latest regulatory rules (in hours)?

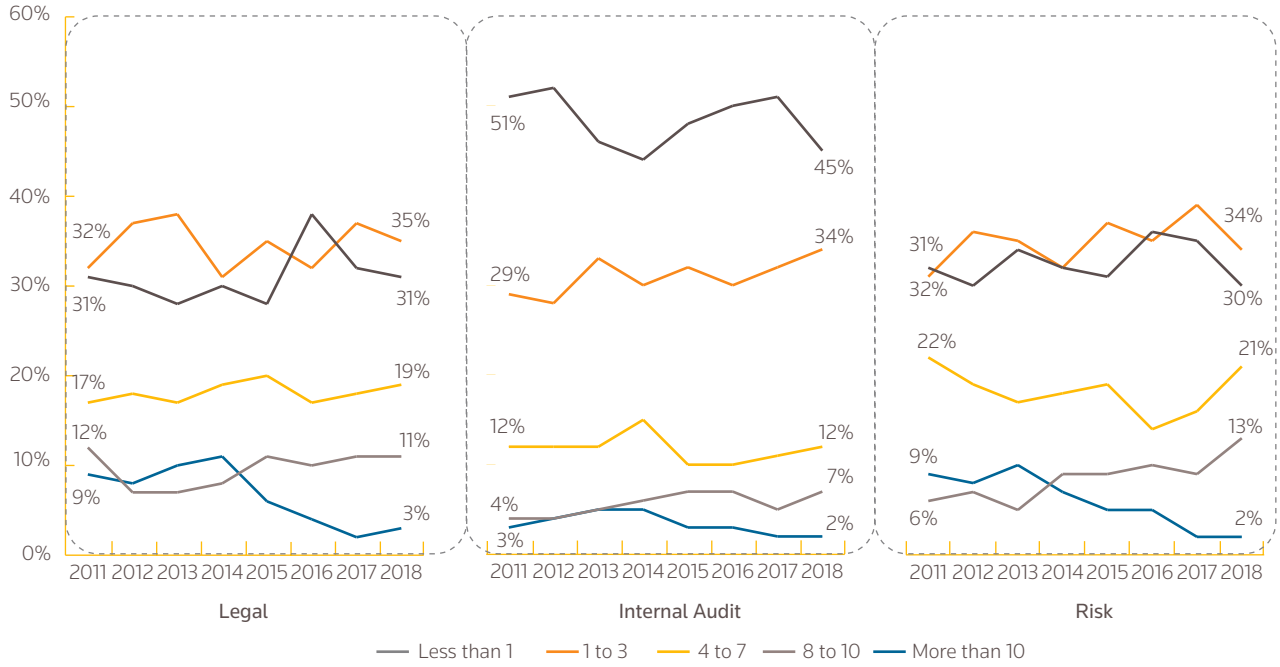


Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

REUTERS/Shutterstock

ALIGNMENT WITH OTHER RISK AND CONTROL FUNCTIONS

Figure 14: In an average week, how much time does your compliance team spend consulting with the legal, internal audit and risk functions on compliance issues (in hours)?



Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

The alignment in terms of the interaction between the compliance function and legal, internal audit and risk has been mixed with the number of compliance teams who spend less than an hour a week with other control functions a potential concern. The control functions in a firm all have distinct roles and remits but firms should be aware of the potential benefits which greater liaison and cooperation may bring.

The scarcity and value of skilled compliance resources has been highlighted by both the expected increase in the cost of senior compliance staff and the continued use of outsourcing to gain the compliance skills needed. Firms can seek to make the best use of in-house skills by optimizing the alignment, cooperation and coordination between the risk and control functions to ensure there is coverage of the key risks to the organization and all associated reporting is consistent particularly when covering culture and conduct risk.

> "Banks' risk management and internal control functions can and should help to develop and monitor the risk appetite framework. The experts working in these areas can ensure that all the risk measures are accurate. They can check whether the risk limits imposed on specific business activities or on specific risks are appropriate. They can answer questions like "How can risks be reported?", "What actions should be taken if limits are close to being breached or have been breached?" It's important for banks to have clear answers to these questions right from the start. Internal audit also needs to regularly review how effective the risk appetite framework is."
>
> Danièle Nouy, Chair of the Supervisory Board of the ECB. Speech, "Risk appetite frameworks: good progress but still room for improvement" at the International Conference on Banks' Risk Appetite Frameworks, Ljubljana. (April 2018)

LIAISON WITH REGULATORS

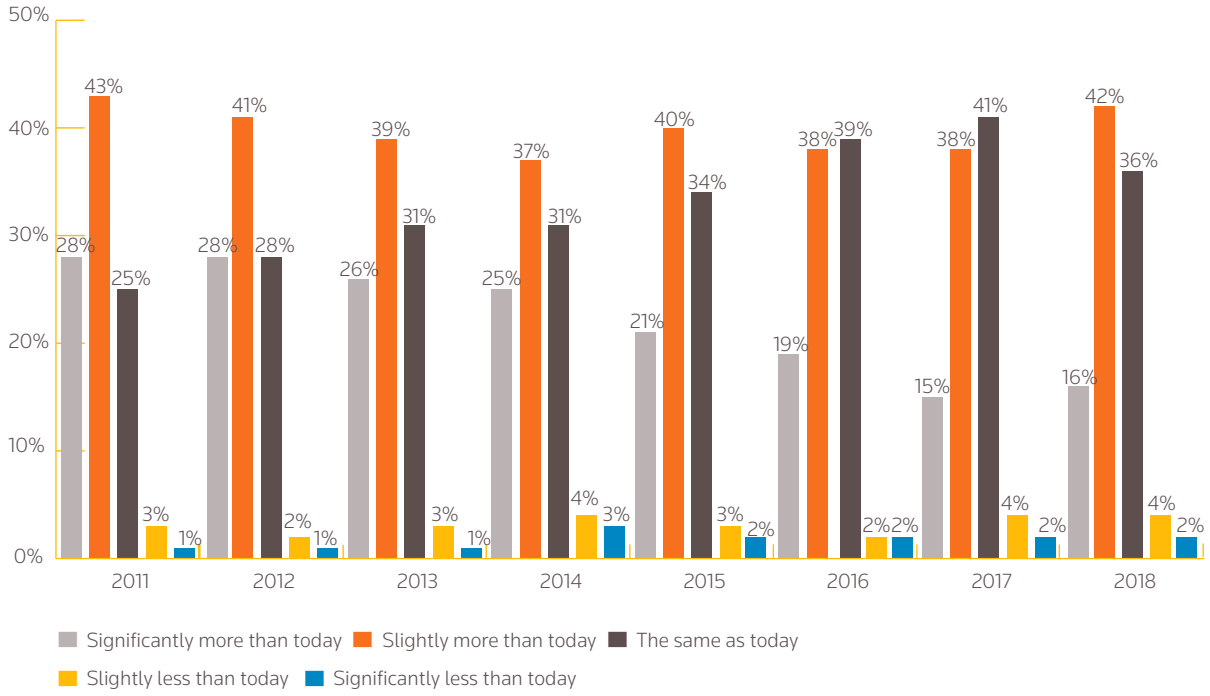
With continuing regulatory developments, expectations of good firm culture, conduct risk, increasing personal liability and growing scrutiny, firms and individuals, now more than ever, need appropriate in-house compliance expertise, skills and experience. Liaising and communicating with regulators and exchanges is one area where technology is unlikely to be of significant assistance. Building and maintaining a strong working relationship with regulators requires skilled senior in-house compliance officers interacting on a personal basis with all relevant supervisors.

There has been gradual shift over the years in the time expected to be spent liaising and communicating with regulators and exchanges. In 2018, over half of firms (58 percent) expect to spend more time liaising with regulators and exchanges with 16 percent expecting significantly more. The expected increase is higher among the G-SIFI population at 66 percent. The top three reasons given as to why firms expect more time spent liaising and communicating with regulators were:

1. More onerous regulatory and reporting requirements;
2. Increased information requests from regulators; and
3. Need to understand changing regulatory expectations.

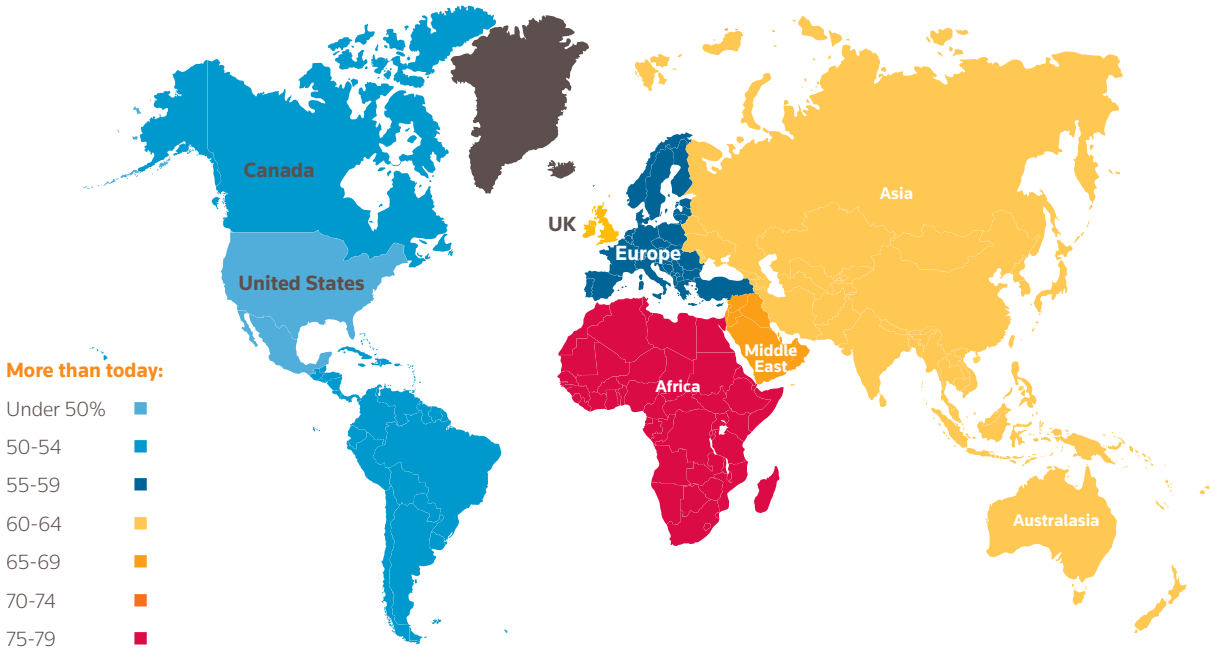
Of those firms who expect significantly more time spent liaising and communicating with regulators were based in Canada (25 percent); the Middle East (25 percent); Australasia (18 percent); and Continental Europe (16 percent). For these regions, more onerous regulatory and reporting requirements, and more intensive supervision, were among the priority areas driving expectations.

Figure 15: Over the next 12 months I expect the time spent liaising and communicating with regulators and exchanges to be...



Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

Figure 16: Over the next 12 months I expect the time spent liaising and communicating with regulators and exchanges to be...



Over the next 12 months I expect the time spent liaising and communicating with regulators and exchanges to be...

	United Kingdom	Continental Europe	United States of America	Canada	Asia	Africa	Australasia	South America	Middle East
Less than today	5%	5%	6%	6%	4%	7%	5%	9%	11%
The same as today	32%	37%	58%	44%	32%	7%	33%	39%	23%
More than today	**63%**	**59%**	**35%**	**50%**	**63%**	**86%**	**62%**	**52%**	**66%**

Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

MANAGING REGULATORY RISK

"Rules and standards cannot replace judgment. Good supervisory instincts and technical competence are required to discover, scrutinize and evaluate key risks. This can only be done if banking supervisors do not see their role as a mere compliance function. An effective banking supervisor must be able to assess a bank's understanding of its risks, its business practices as well as judge its corporate governance and culture."

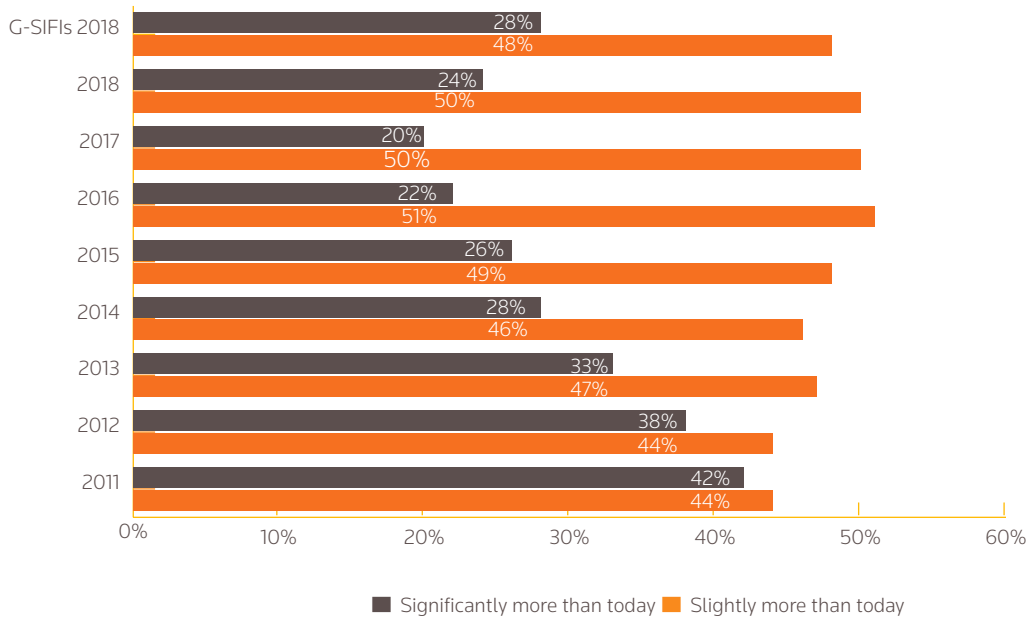
Ong Chong Tee, Deputy Managing Director (Financial Supervision) of the Monetary Authority of Singapore. Speech at the 13th Asia-Pacific High Level Meeting on Banking Supervision, Singapore. (February 2018)

The expected focus on the need to manage regulatory risk is unrelenting. Seventy four percent of firms expected the regulatory focus on managing regulatory risk to increase in the coming year, 24 percent expecting a significant increase. In the G-SIFI population 76 percent expected an increase with 28 percent expecting a significant increase (up from 15 percent in 2017).

A third (33 percent) of firms in Australasia, and over a quarter of firms in Asia and Canada (27 percent) expect managing regulatory risk to significantly increase over the next 12 months. These may be attributed to various regulatory efforts to hone in on poor culture and misconduct, including Australia's banking inquiry, Banking Executive Accountability Regime (BEAR), and the Hong Kong SFC's Managers-in-Charge (MIC) regime.

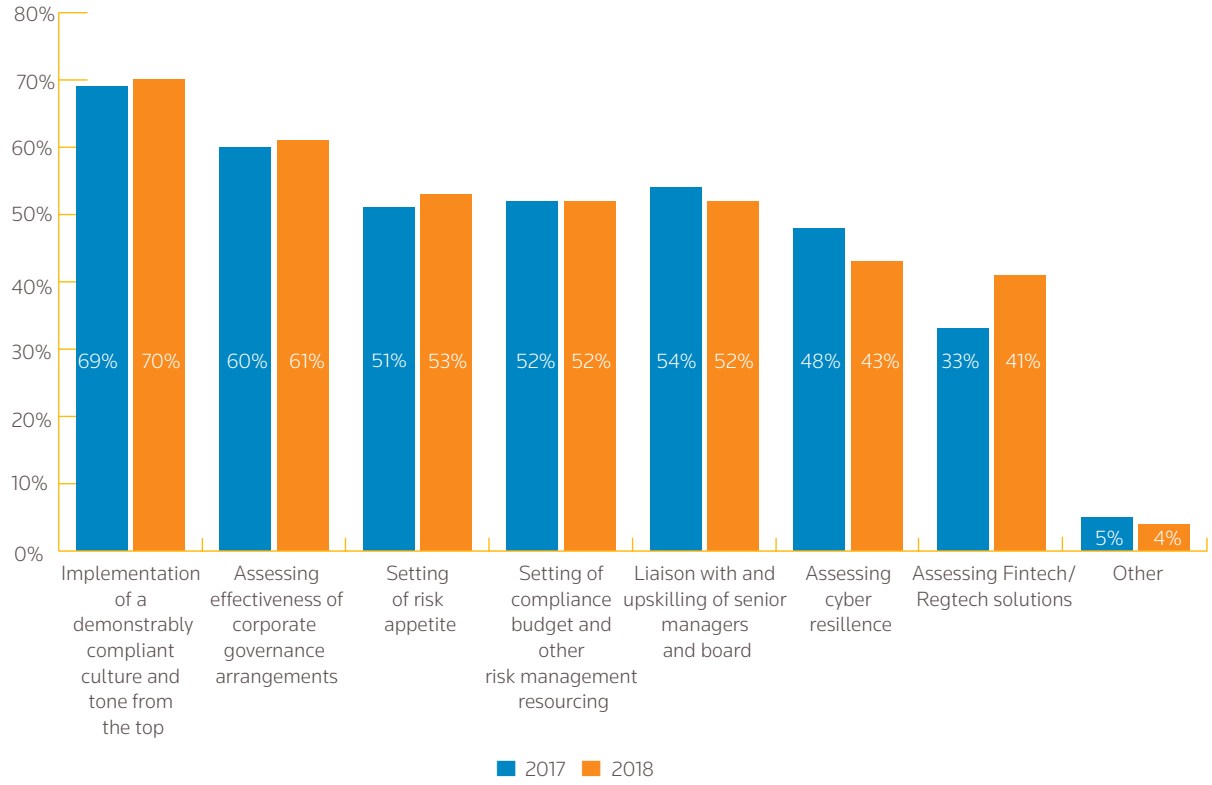
The areas where compliance teams are expecting to have more involvement have shown relative consistency year on year, with the exception of the assessment of fintech/regtech solutions, which has increased from 33 percent to 41 percent. This increases further for G-SIFIs, where more than half (55 percent) of practitioners expect more compliance involvement in assessing fintech and regtech solutions.

Figure 17: Expectation that the regulatory focus on managing regulatory risk will increase over the next 12 months



Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

Figure 18: Over the next 12 months I expect more compliance involvement in...



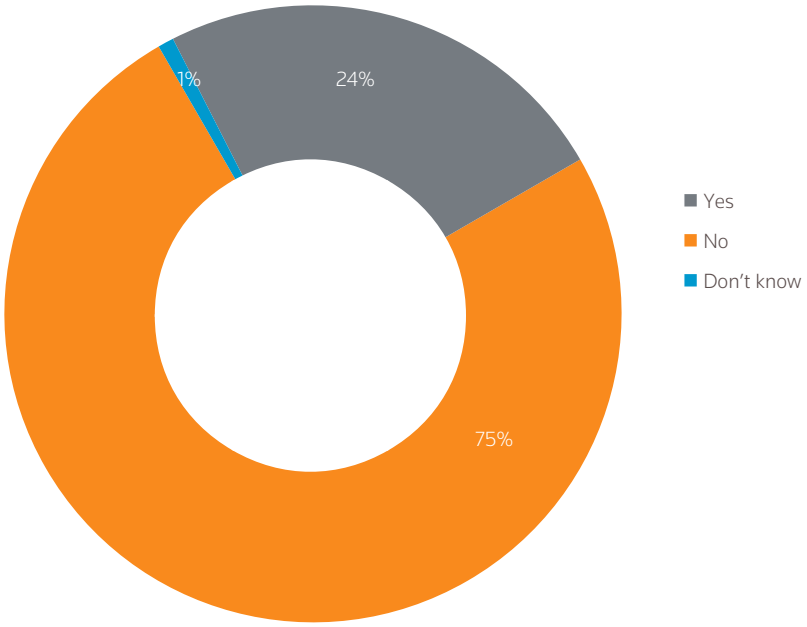
Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

Practitioners provided specific details on other areas in which they expect more compliance involvement over the next 12 months. These include:

- Improving surveillance;
- GDPR readiness;
- Assessing privacy and data protection regulations;
- Conduct risk management;
- Liquidity risk management;
- KYC processes;
- Training;
- Facilitating a process to spread knowledge of regulations in the first line;
- Greater focus on behavioral matters;
- Embedding an appropriate compliant culture;
- Policy management;
- Hotline compliance;
- Increased participation in product development;
- New regulations;
- Burdensome regulatory reporting;
- Assisting with development of self-testing protocols for business line staff;
- Assisting business line staff in identifying risks and creating effective controls in all system (computerized) solutions;
- Assessing regulatory change and the impact on the business;
- Local and international tax obligations e.g. CRS & FATCA.

OUTSOURCING

Figure 19: Do you outsource any or all of your compliance functionality?



Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

Upholding the trend from 2016, when the question on outsourcing was first introduced to the survey, almost a quarter (24 percent) of all firms still outsource all or part of their compliance functionality.

In line with previous years, the top three reasons for outsourcing have remained relatively consistent year on year:

1. Need for additional assurance on compliance processes;
2. Lack of in-house compliance skills; and
3. Cost.

Regionally, there are some wide disparities. Over a fifth (21 percent) of firms in the United Kingdom, Continental Europe,

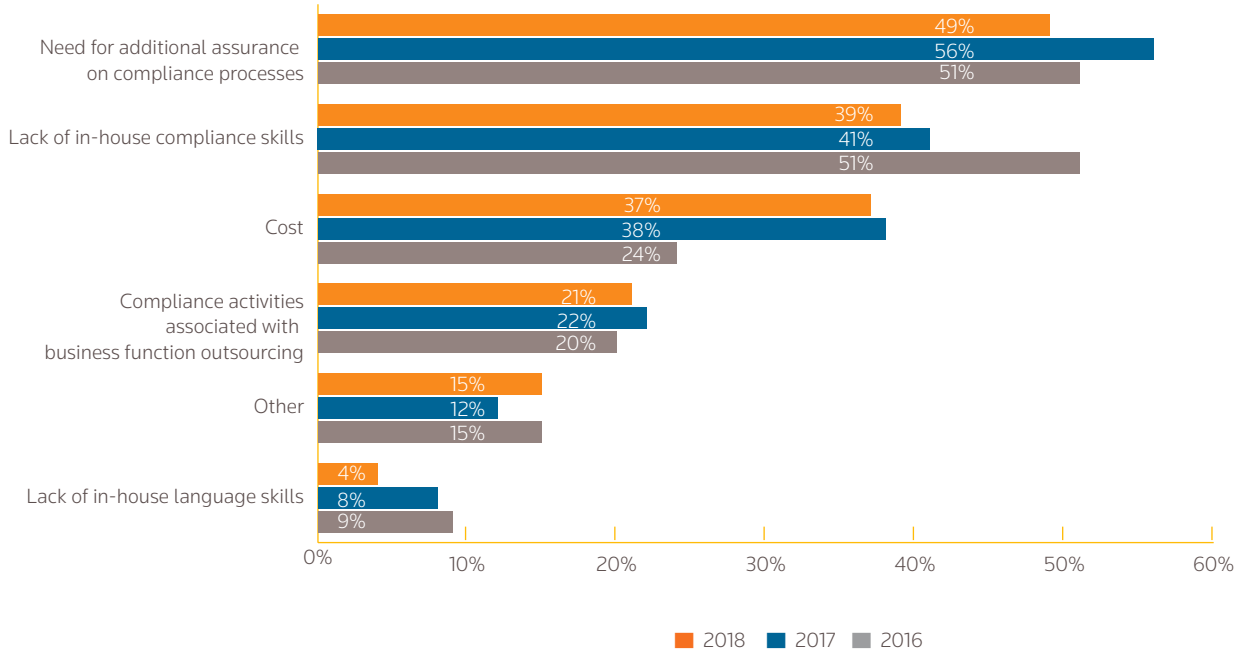
> "There is a significant regulatory duty imposed on these companies to ensure that they have the best understanding of existing risks as well as new and developing risks on an ongoing basis. Experience has shown that when risk- consciousness is present in a company's daily business, bad things are less likely to happen: companies using a risk-based approach are more successful in the long run and more likely to meet the expectations of regulators and stakeholders and maintain a high degree of trust and confidence in the business in the long run."
>
> International Chamber of Commerce. Guide, "Outsourcing – a practical guide on how to create successful outsourcing solutions." (February 2018)

Canada, and 20 percent of firms in Asia outsource all or part of their compliance functionality, compared to 42 percent of firms in the United States.

Of potential concern is the persistence in the need to outsource activities in order to supplement a lack of in-house compliance skills. There is no substitute for having the appropriately skilled compliance resources. One area where firms and their compliance officers may be seeking to bridge a skills gap is with regard to evolving technology, notably in the shape of fintech developments and regtech solutions. Whilst it is encouraging that compliance functions have recognized any skills gap, firms need to keep the balance between in-house expertise and any outsourcing under review. It is critical that firms continue to invest in all aspects of their risk and compliance infrastructure, an essential part of which is the skills of the compliance function.

No matter what the reason, the golden rule for successful outsourcing is that while activities can be moved to a different group, company, or a third party, the skills to manage those activities must be retained in-house. This may be less obvious in an intra-group outsourcing scenario - but for a separate legal entity with a separate license, it is essential. Equally, if there is a branch or other structure involved, then the firm needs to consider the efficacy of the outsourcing arrangements and the skills, governance and local responsibilities of the branch.

Figure 20: Main drivers for outsourcing all or part of the compliance function



Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

CYBER RESILIENCE

"It is critical that business leaders understand what a cyber-attack could do, how to respond and recover. We understand this makes demands of already busy senior leaders. But we think it is important this is no longer confined to the technology department. It needs to move into the Boardroom. It needs to be understood as a significant risk to the operation of a business, its consumers and wider markets."

Robin Jones, Head of Technology, Resilience & Cyber at the FCA. Speech at the PIMFA Financial Crime Conference, "Building Cyber Resilience", London. (January 2018)

There are a number of angles to the impact of technology on the compliance function not least of which is the need to assess cyber resilience. Overall expected compliance involvement on assessing cyber resilience fell somewhat in 2018 (43 percent in 2018; 48 percent in 2017 and 2016). The decrease could be associated with other areas picking up more of the work or perhaps the use of outsourcing. It would be a matter of concern if the decrease was due to a lack of required resources.

In June 2017, the UK FCA published an update to its cyber resilience advice and its expectations such that firms should be aware of the threat, able to defend themselves effectively, and respond proportionately to cyber events. As part of the advice, the FCA quoted a number of statistics to illustrate the increasing threat from cyber attacks, perhaps the most startling of which was the 1,700 percent increase in cyber attacks reported to the regulator since 2014.

It is clear that what was previously often seen as simply an IT issue has become a key issue for risk and compliance functions with the FCA stating its goal to 'help firms become more resilient to cyber attacks, while ensuring that consumers are protected and market integrity is upheld.'

REUTERS

The FCA expectations on effective cyber security practices include:

- Managing the risk in particular by having an accurate and up-to-date picture of all information held together with an understanding of why that information is retained;
- Encryption is critical and all sensitive data must be identified as such and protected;
- Disaster recovery plans must be in place and tested with the ability to backup critical systems and data as and when required;
- Network and computer security must be kept up-to-date with all 'patches' applied as soon as is feasible;
- Use and device credentials need to be fit for purpose with all staff required to use strong passwords and the default administrator credentials changed on all devices;
- Training and awareness is an essential part of good cyber security with the 'people factor' to be considered an integral part of the approach to cyber resilience;
- Consideration to be given to gaining a recognized accreditation to improve firm-wider cyber security; and
- Sharing threat information with peers through approved networks

The FCA is all too aware of the sheer breadth of cyber issues facing firms with more than half of UK businesses reported to have been hit by ransomware attacks. The expectation is that firms should seek to put all reasonable measures in place to protect against this particularly prevalent form of attack. There is no single type of ransomware attack but whichever form of ransomware is used, all will seek to prevent a firm or an individual from using their IT systems and will ask for something (usually payment of a ransom) to be done before access will be restored. There is of course no guarantee that paying the fine or doing what the ransomware attacker demands will restore full access to all IT systems, data or files.

All too many firms have found that critical files often containing client data have been encrypted as part of an attack and large amounts of money are demanded for restoration. Encryption is in this instance used as a weapon and it can be practically impossible to reverse-engineer the encryption or 'crack' the files without the original encryption key – which is deliberately withheld by the cyber attackers.

"And remember: security is a boardroom-level issue. We have seen too many major breaches where companies process data in a technical context, but security gets precious little airtime at board meetings.

If left solely to the technology teams, security will fail through lack of attention and investment. These companies may have the best policies in the world – but if those policies are not enforced, and personal data sits on unpatched systems with unmanaged levels of employee access, then a breach is just waiting to happen."

Elizabeth Denham, Information Commissioner at the ICO. Speech at the National Cyber Security Centre CYBERUK 2018 event, "Building the Cyber Security Community", Manchester. (April 2018)

DATA PROTECTION AND GDPR

The new data privacy requirements are deliberately global in their reach and the UK ICO has been a leading policymaker in translating the new European Regulation into practical guidance for firms. One key area for consideration is the core concept of 'consent', which is one of the six lawful bases (or conditions) for processing personal information. The definition and role of consent remains similar to that under the previous requirements but the new law contains more detail and codifies existing guidance and good practice.

In May 2018, the ICO published its final guidance on consent which is structured as a series of questions – what's new, why is consent important, when is consent appropriate, what is valid consent and finally how should we obtain, manage and record consent?

The GDPR sets a deliberately high standard for consent with the expectation that firms will have clear, granular opt-in methods, good records and simple easy-to-access ways for people to withdraw consent. The changes reflect a more dynamic concept of consent as an organic, continuing and actively managed choice rather than a simple one-off tick box.

The ICO has highlighted a number of key changes, the biggest of which is the practicalities around consent mechanisms including:

- Unbundled: consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service;
- Active opt-in: pre-ticked opt-in boxes are invalid – use un-ticked opt-in boxes or similar active opt-in methods (e.g. a binary choice given equal prominence);
- Granular: give distinct options to consent separately to different types of processing wherever appropriate;
- Named: name your organization and any other third party controllers who will be relying on the consent. If you are relying on consent obtained by someone else, ensure that you were specifically named in the consent request – categories of third-party organizations will not be enough to give valid consent under the GDPR;
- Documented: keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented;
- Easy to withdraw: tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you need to have simple and effective withdrawal mechanisms in place; and
- No imbalance in the relationship: consent will not be freely given if there is imbalance in the relationship between the individual and the controller – this will make consent particularly difficult for public authorities and for employers, who should look for an alternative lawful basis where possible.

For firms, getting the approach to consent right is a fundamental element of data protection. Under the GDPR, the requirements and the penalties for getting it wrong will be enhanced. It is a measure of the central nature of consents that infringements of the basic principles for processing personal data, including the conditions for consent, are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of total worldwide annual turnover, whichever is higher.

It is not just the size of the possible monetary sanctions that firms need to consider. The ICO is to be given expanded powers of investigation and enforcement which will enable it to have greater (and quicker) rights of access, as well a wider range of available sanctions including the ability to stop an entity from processing data.

Consent is not a one-off. The ICO is recommending the consideration of an automatic refresh of consent at 'appropriate intervals'. The interval will depend on the particular context, including people's expectations, whether or not the firm is already in regular contact with the person concerned, and how disruptive repeated consent requests would be to the individual. The ICO has stated that 'if in doubt, we recommend you consider refreshing consent every two years'.

Consents need to be specific and granular and so the records equally need to be specific and granular to evidence exactly what the consent covers. The ICO has made clear that firms will be expected to have an effect audit trail of how and when consent was given together with the ability to provide evidence if challenged. Firms will need to keep the evidence for as long as it is still processing based on the consent, so it can demonstrate compliance on a continuing basis with accountability obligations. Good records are also seen as helping firms to monitor and refresh consent as appropriate.

Figure 21: Preparing for the General Data Protection Regulation (GDPR)

1. Awareness
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. Information you hold
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3. Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. Lawful basis for processing personal data
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7. Consent
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8. Children
You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9. Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Data Protection by Design and Data Protection Impact Assessments
You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation

11. Data Protection Officers
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12. International
If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Source: Information Commissioner's Office. Guidance – Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now (April 2017)

"I have no intention of changing our proportionate and pragmatic approach after 25 May. My aim is to prevent harm, and to place support and compliance at the heart of our regulatory action. Voluntary compliance is the preferred route.

But we will back this up by tough action where necessary; hefty fines can and will be levied on those organisations that persistently, deliberately or negligently flout the law. Report to us, engage with us. Show us effective accountability measures. Doing so will be a factor when we consider any regulatory action."

Elizabeth Denham, Information Commissioner at the ICO. Keynote speech at IAPP Europe Data Protection Intensive 2018, London. (April 2018)

The ICO has stipulated that firms must keep good records that demonstrate the following:

- Who consented: the name of the individual or other identifier (e.g. online user name, session ID);
- When they consented: a copy of a dated document, or online records that include a timestamp; or, for oral consent, a note of the time and date which was made at the time of the conversation;
- What they were told at the time: a master copy of the document or data capture form containing the consent statement in use at that time, along with any separate privacy policy or other privacy information, including version numbers and dates matching the date consent was given. If consent was given orally, your records should include a copy of the script used at that time;
- How they consented: for written consent, a copy of the relevant document or data capture form. If consent was given online, your records should include the data submitted as well as a timestamp to link it to the relevant version of the data capture form. If consent was given orally, you should keep a note of this made at the time of the conversation - it doesn't need to be a full record of the conversation; and
- Whether they have withdrawn consent: and if so, when.

"If your organization is still on their journey to GDPR compliance you should continue with your efforts to be ready before the law takes full effect on 25 May. But remember that this date is the start and not the end of GDPR compliance. Organizations need to sustain their compliance processes over time – this is the best way to take people with you on your business journey."

Steve Wood, Deputy Commissioner for policy at the ICO. Blog, "Raising the bar – consent under the GDPR". (May 2018)

REUTERS

CHALLENGES COMPLIANCE OFFICERS EXPECT IN 2018

Figure 22: The greatest compliance challenges I expect to face in 2018 is/are:

o Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

Compliance practitioners were asked to explain their greatest challenge in the year ahead. The top 5 identified for 2018 were:

1. Continuing regulatory change;
2. Data privacy and GDPR;
3. Enhanced monitoring and reporting requirements;
4. Increased regulatory scrutiny; and
5. Implementation of regulatory change.

There is a fair degree of consistency with the challenges identified in 2017 with the notable exception of the inclusion of data privacy and GDPR for 2018.

The sheer breadth of challenges compliance officers expect to encounter in the coming year illustrates, once again, the need for senior compliance staff to be polymaths. The theme of 'coping' is something many practitioners highlighted. Coping with regulatory change, coping with data privacy and GDPR and coping with enhanced monitoring and reporting requirements all while also coping with potentially limited skilled sources is likely to make 2018 another very busy year for compliance practitioners.

Specific areas of regulation which pose the greatest challenge for the coming year were highlighted as:

- Fourth Money Laundering Directive (4MLD);
- Countering America's Adversaries Through Sanctions Act (CAATSA);
- Common Reporting Standard (CRS);
- US Fiduciary Rule;
- General Data Protection Regulation (GDPR);
- Home Mortgage Disclosure Act (HMDA);
- Insurance Distribution Directive (IDD);
- International Financial Reporting Standard 9 (IFRS 9);
- The Markets in Financial Instruments Directive II (MiFID II);
- The Packaged Retail and Insurance-based Investment Products (PRIIPs);
- The Revised Payment Services Directive (PSD2);
- Sapin II (France);
- Sarbanes-Oxley Act;
- The Senior Managers and Certification Regime (SMCR); and
- Suspicious Transaction and Order Reports (under the Market Abuse Regulation (MAR))

Figure 23: The greatest compliance challenges the board expects to face in 2018 is/are:

o Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2018

Compliance practitioners were also asked to explain the board's greatest challenges in the year ahead. The top 5 for 2018 were identified as:

1. Continuing regulatory change;
2. Enhanced supervisory scrutiny;
3. Data privacy and GDPR;
4. Cyber security; and
5. Balancing compliance and commercial demands

In line with the compliance challenges identified, there is a fair degree of consistency with the challenges highlighted in 2017, with the notable exception of the 2018 inclusion of data privacy and GDPR. If compliance challenges were characterized by the need to 'cope', the challenges for the board were characterized by the need to 'understand' the risk and compliance implications of the regulatory year ahead.

"Inductive methods begin with a broad scope of enquiry to see what emerges. A starting point for this methodology is establishing clear definitions of the various dimensions which characterise the topic of culture; for example, tone from the top, risk capability, openness and challenge, accountability and risk governance. Each dimension is then explored systematically and analysed to arrive at a set of themes that adequately reflect the data set. This approach provides a good opportunity to obtain a clear representation of a firm's unique characteristics, but it requires collecting a broader set of data and perhaps more sophisticated analytic techniques. It also makes benchmarking across and within firms more difficult."

Financial Stability Board. Strengthening Governance Frameworks to Mitigate Misconduct Risk: A Toolkit for Firms and Supervisors. (April 2018)

CLOSING THOUGHTS

The global focus on the need to eradicate misconduct in financial services is the driver for much of the current regulatory approach. The FSB's toolkit on misconduct is a landmark document and sets the international regulatory agenda on the suggested approach to and sanctions for misconduct in financial services firms. This will keep the spotlight on the need to manage all regulatory risks and has been the underlying reason for jurisdictions implementing, or planning to implement, accountability regimes for senior managers.

Compliance officers have recognized that personal liability is, and will remain, high. The underlying thread of compliance officers needing to 'cope' with the challenges expected in the year ahead is set against that backdrop. Compliance may well take the lead in determining how best to identify, manage and mitigate the increasing personal accountability.

There are several benefits for compliance officers thinking through how to best manage their own personal regulatory risk. Most obviously is that they themselves stay out of regulatory trouble. Other benefits include being able to advise other senior managers on the likely best practices associated with managing personal regulatory risk and once their own risk is appropriately managed they will be able to devote more attention back to the day job of firm compliance.

Compliance officers expressed their potential concern about the board's overarching 'understanding' of key compliance challenges. Board members are not expected to be experts in everything but they do need to have sufficient knowledge and to have an appropriate range of skills to understand the issues, able to set an appropriate risk appetite, drive a strong compliant culture, understand and challenge all risk and compliance reports as well as engage appropriately with regulators.

One means by which firms could seek to tackle any potential issues around a possible lack of individual or collective understanding is through training. For boards a strong and effective suite of training needs above all else to be tailored to the audience. Given the seniority and diversity of experience at the board level bespoke training tends to be used with regular, often face-to-face, bite-sized updates to accommodate busy schedules. It is critical that any and all training is robustly and consistently captured and recorded with any absences from training course(s) followed up and completed in a timely manner. Specifically, training needs to be seen as a key mechanism by which individuals (senior or otherwise) can use to identify, manage and mitigate any and all personal regulatory risks.

"Risk management, compliance and internal audit must inform the decisions that are taken at the top. The heads of these areas must report regularly and directly to the board of directors. If they don't, risks might not be taken properly into account when decisions are taken. In addition, they must be able to meet with the board and its relevant committees without the bank's senior management being present.

At the same time, the board must assess whether internal control functions are working efficiently and effectively. All too often, this is not done."

Danièle Nouy, Chair of the Supervisory Board of the ECB. Speech at the second banking supervision conference, "Governance expectations for banks in a changing financial environment", Frankfurt. (March 2018)

About the authors

Stacey English is head of regulatory intelligence for Thomson Reuters with over 20 years of regulatory compliance, risk and audit experience in financial services as a regulator and practitioner.

uk.linkedin.com/in/stenglish @regexperts

https://blogs.thomsonreuters.com/financial-risk/authors/stacey-english/

Susannah Hammond is senior regulatory intelligence expert for Thomson Reuters with more than 25 years of wide-ranging compliance, regulatory and risk experience in international and UK financial services.

uk.linkedin.com/in/susannahhammond @SannaHamm

https://blogs.thomsonreuters.com/financial-risk/authors/susannah-hammond/

Visit risk.tr.com

THOMSON REUTERS®

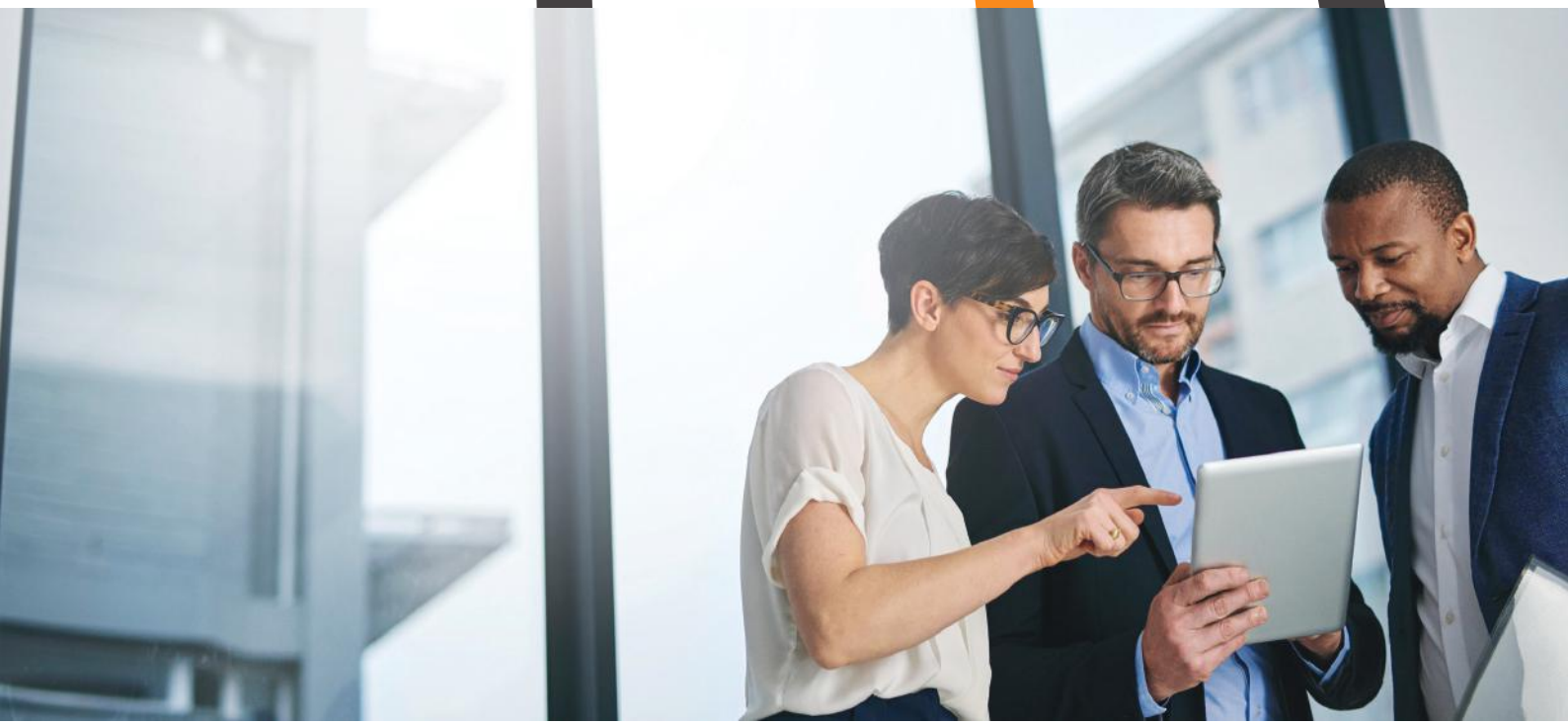
Adapt to evolving Integrated Risk Management needs

Take confident action on critical challenges with a consolidated, enterprise-wide view of risk.

Rely on Thomson Reuters Connected Risk to manage and mitigate risk with confidence by utilizing internal and external data more effectively. Organizations benefit from a holistic enterprise-wide view of risk through advanced mapping and an extensible interconnected data model underpinned by streamlined workflows.

With Connected Risk, organizations are able to make informed decisions with greater ease and efficiency, delivering a focused view of their risk, compliance and audit landscape.

Discover more at: **risk.tr.com/connected-risk**



THOMSON REUTERS®