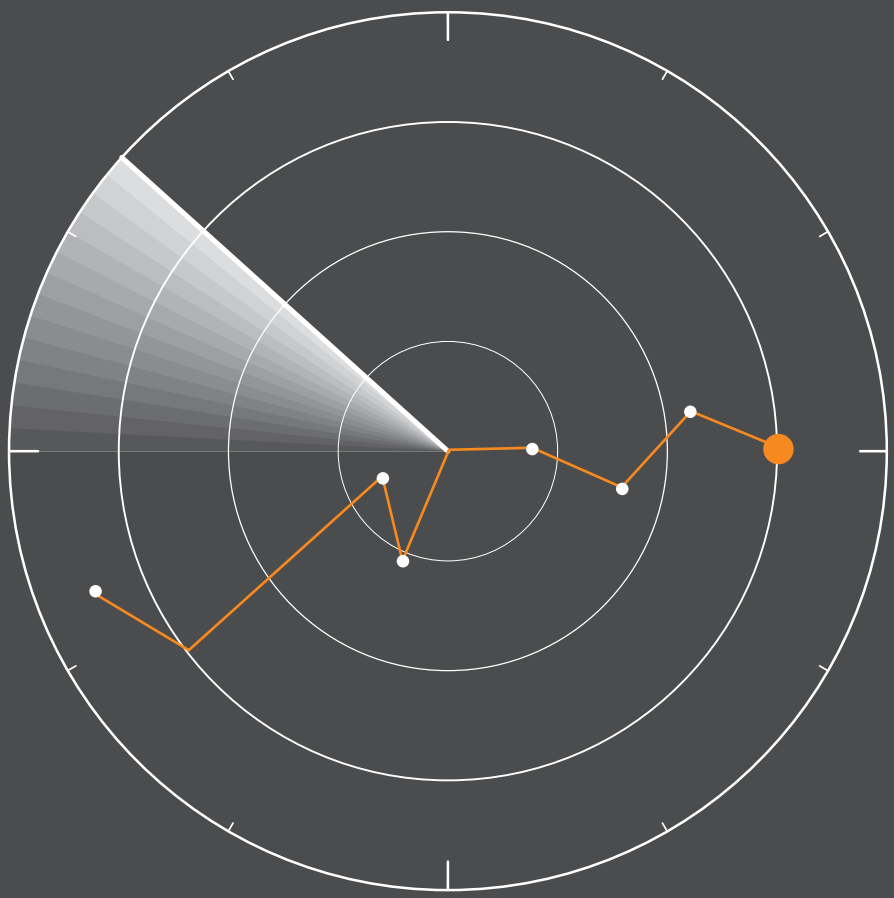


Trends in UK
Risk & Compliance

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

the answer company™
THOMSON REUTERS®

Contents

Executive summary

The last five years has seen a step-change in the profile of risk & compliance on the corporate agenda. No longer simply viewed as a box-ticking exercise, nor approached in a reactive hit and miss manner, risk & compliance programmes and departments are growing in sophistication, profile and resource.

UK-based respondents to Thomson Reuters' risk & compliance survey highlight key changes around risk & compliance management in recent years, with growing formality and reorganisation amongst the most common changes. Motivations for these changes differ by organisation, but are linked by a need to drive consistency across the corporate entity, clarify and specify key responsibilities, and ensure a properly coordinated approach to managing risk & compliance. Dedicated teams and key hires are a common means of achieving this—with overall personnel and, importantly, budgets rising in turn.

Well over half of organisations surveyed have a dedicated risk & compliance function managing their programme, with legal—or a combination of the two—taking care of most of the remainder[1]. Budget ownership differs to a degree, often coming through the finance department or devolved to business units, though risk & compliance and legal still look after the majority of budgets. Budgets are generally set to rise as risk & compliance concerns increase in prominence on the agendas of senior leadership: more and more often, it is now seen as a business enabler as opposed to a prohibiting factor.

Only three percent of respondents anticipated a decrease in budgets, with over half expecting an increase in budget. A progressively complicated risk landscape is responsible, along with organisation growth and increasing prominence of risk among leadership. Specific events also play their part, with Brexit and the introduction of the new General Data Protection Regulations (GDPR) opening a new set of risks and potential future compliance frameworks for corporate risk & compliance departments to react to—notably, cyber and data protection sit at the top of most risk registers currently creating new challenges in terms of people risk and training.

As teams and programmes have developed in sophistication, so to have corresponding processes. Risk registers and controls are becoming more common and central to decisions, with investment in staff training and software which enables risk & compliance personnel to keep up with a changing—and increasingly complex—regulatory framework. Outside of self-certification, internal and external auditing generally make up the bulk of monitoring process for assessing the effectiveness of controls. Though other assurance processes are often in place, there is limited uniformity of approach across organisations.

Despite increased preparedness as a whole, for a number of organisations there is still scope to tighten up management. Plans for incident management and business continuity tend to be in place and updated at least annually for most, but when it comes to testing these plans and training staff in their implementation, this research indicates a notable drop off. A third of organisations either have no processes or largely informal processes for measuring and assessing risk appetite, and almost a fifth take a largely reactive approach to monitoring regulatory changes. Outside help is available and drawing upon external support in this area is common, with 70 percent consulting law firms. Well over half of respondents also utilise other third parties—including accountants, consultants and other industry or professional membership bodies—to help them remain compliant in a changing regulatory landscape.

Thomson Reuters and Acritas would like to take this opportunity to express our thanks to all of the individuals who took the time to respond to the survey or to speak to us over the phone.

[1] However, several other departments play a role for some organisations.

Methodology

Thomson Reuters has undertaken primary investigative research in conjunction with the professional services research agency, Acritas, to assess the state the state of play of risk & compliance and the forward looking agenda. In total, there were 154 responses to the survey from risk & compliance and legal professionals.

154 responses from risk & compliance or legal professionals

100 web survey responses

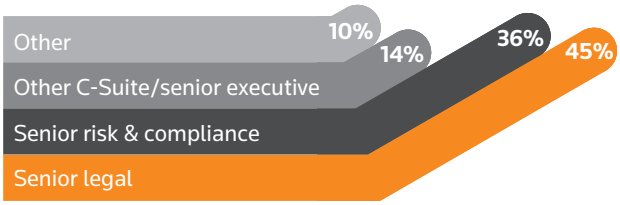
45 telephone interviews

9 face-to-face interviews

Demographics

Respondents were targeted based on the following criteria:

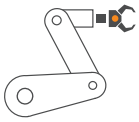
- UK-based respondents, representing regulated and non-regulated organisations with over £25m in revenue
- Senior-level legal or risk & compliance professionals, along with senior leadership / execs



Industry breakdown

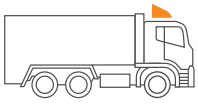
Respondents were distributed across the following key industries:

23% Financial services



11% Manufacturing

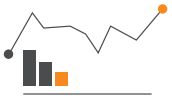
12% Technology/media



7% Transport/logistics

7% Retail/wholesale

7% Real estate



6% Banking

6% Energy utilities

6% Insurance

15% Other

Framing the risk & compliance challenge

Key risks on the risk register

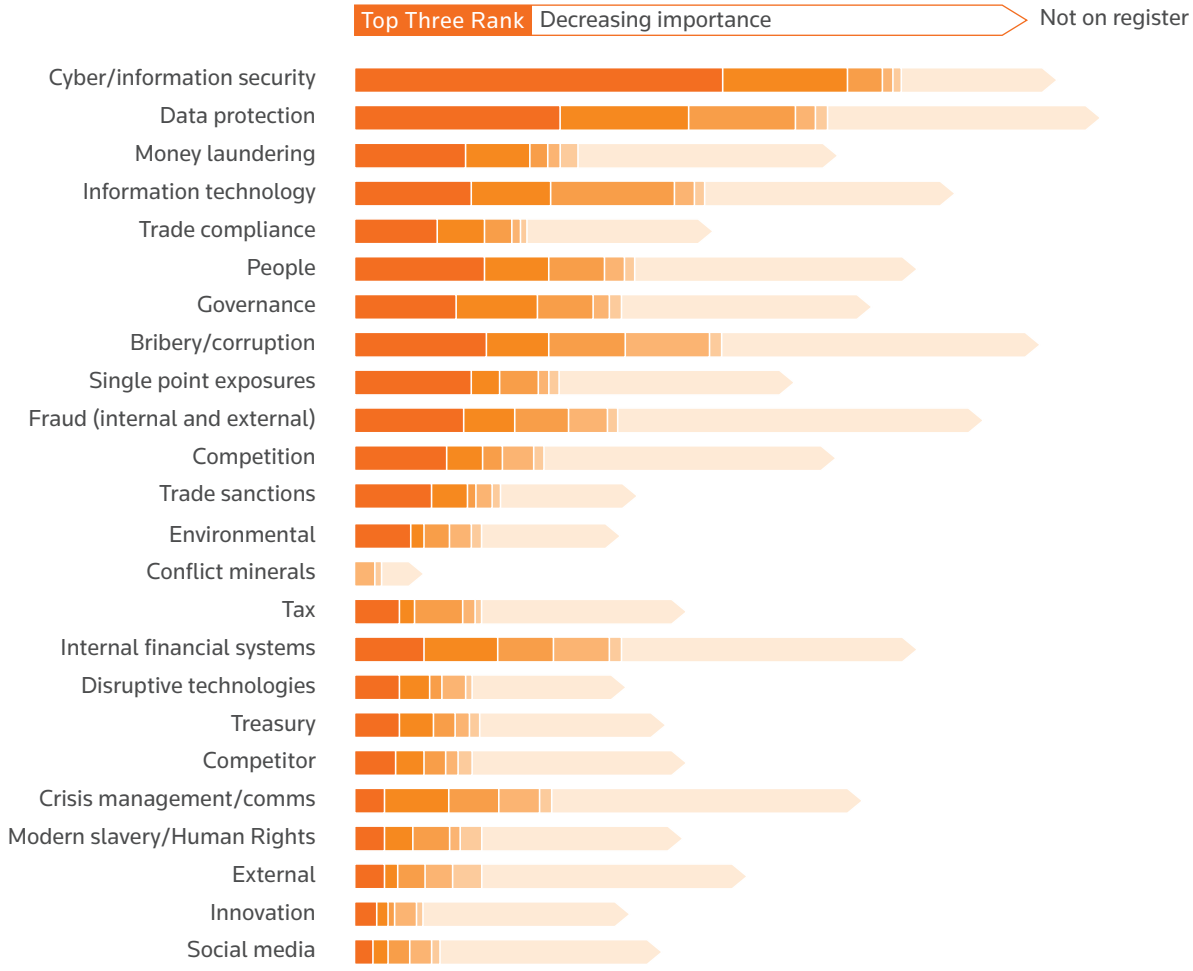
Understanding the risk-environment context within which UK organisations need to operate is important when developing and managing risk & compliance programmes. Respondents regularly cited a changing risk landscape, new or emerging risk, and a complicated compliance framework as factors in their strategic planning. But, which risks are on the agenda right now, and which are topping out UK risk registers?

From a common register of 24 key risks, respondents were first asked whether each appeared on their risk register, and then asked them to rank the risks in order of concern. Perhaps unsurprisingly, given the prevalence of high-profile cyber breaches in recent years, cyber security is by far the most common risk to appear on risk registers overall, as well as most likely to appear in the top three risks for UK organisations. This trend is accentuated somewhat when focusing in on highly regulated industries, with the majority placing this core risk at the top end of the registers, and a higher proportion than average reporting its presence on the register in general. Data protection is the second most common risk reported within this survey—the Data Protection Act and the arrival of GDPR onto the compliance agenda place this high on the spectrum for organisations of all sizes in terms of the need for heightened awareness.

Whilst some risks are prevalent across the organisations surveyed, a number of others appear far less frequently, but often have a high proportion ranking them highly in importance—for example, internal financial systems and crisis management. The potential impact on organisations from a reputational, financial and criminal point of view from risks such as money laundering, bribery and environmental issues are evident. For many organisations, these risks are just as important as cyber security and data protection.

Risks appearing on registers and the most important risks

Which of the following risks appear on your organisation's risk register?[2]



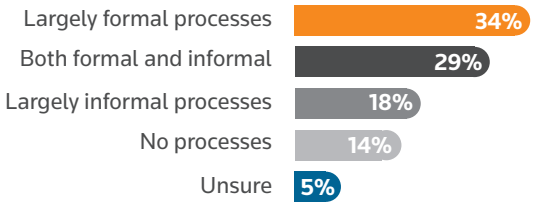
[2] Ranked in order of concern for the organisation. Q-Base = 149

Measuring risk appetite

Risk registers will be subject to change by necessity. Gauging the relative need for preparedness, regarding required resource versus potential impact—in terms of likelihood and severity—leads to an ongoing process of monitoring and adjusting an organisation's register against its risk appetite in key areas.

Processes for measuring risk appetite

Does your organisation have regular processes in place to measure and assess its risk appetite?



For over a third, this process is largely formal, with a similar proportion adopting both formal and informal processes, though one in five measure their risk appetite on a largely informal basis. As would be expected, where dedicated risk & compliance functions exist—and generally for highly regulated companies—the process is generally far more likely to be formalised.

In addition to summarising the content of risk registers, respondents were also asked to comment on the coverage of their compliance programmes, with a few differences emerging between the two areas.

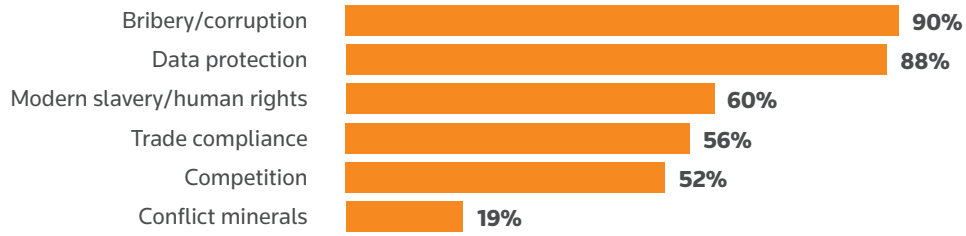
Nine out of 10 organisations cover bribery and corruption on their compliance programmes, which is a higher proportion than those reporting that this appears on their risk registers. This is also true for conflict minerals, with few identifying this as a specific risk, but a higher proportion required to be compliant in this area.

Bribery compliance is fundamental for most organisations, and all organisations with over £1 billion revenue include bribery in their compliance programmes. Clearly, data protection is high on both risk registers and compliance programmes. In the case of bribery and corruption, arguably awareness of these factors as business risks are high, and the steps and processes around mitigation well established. In the case of data protection, whilst not a new risk, it is a rapidly evolving area that many organisations struggle to keep pace. So, whilst it is strongly recognised on compliance programmes, there is clearly a great deal of nervousness around the effectiveness of controls, tools and assurance processes to enable organisations to successfully de-risk this area.

Coverage of compliance programmes

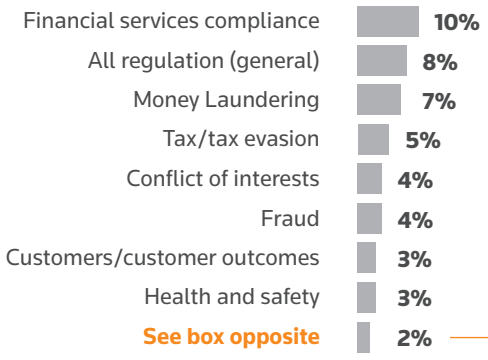
Which of the following areas does your compliance programme cover?[4]

PROMPTED



Which other key areas does your compliance programme cover?

UNPROMPTED



2% including: cyber security, supply chain, people risk, operational capacity, product compliance, whistleblowing and market abuse.

[4] Respondents were asked to select all that were applicable. Base = 149

Preparing for the worst

Business continuity planning and testing

Business continuity plans are clearly essential frameworks to enable organisations to mitigate against risk, both reputational and otherwise—and over 90 percent of organisations reported having these in place, with annual reviews proving most common.

However, the ability of organisations to effectively implement these plans, if they were ever required, appears slightly more questionable. Testing for business continuity plans is only in place for 73 percent of organisations surveyed, dropping to 57 percent when it comes to business continuity training for staff.

The exception to this pattern is highly regulated companies and those where risk & compliance teams control its budget– with a high degree of crossover report a far higher level of preparedness in terms of both testing and training to support their high-level business continuity plans.

Having a social media policy is also very common—albeit not to the degree of business continuity plans—but a similar situation emerges. Only a third of organisations have plans in place to provide any social media training for their workforce, relying on individuals' awareness of, and compliance with, the policy.

Risk & compliance training

When it comes to educating the workforce on risk & compliance, on average respondents reported a fairly comparable uptake of face-to-face versus online training, at 48 percent and 52 percent respectively. Whilst online training is creeping ahead on balance, 10 percent of respondent still relied on face-to-face training for all of their training needs, compared to only three percent solely relying on online training.

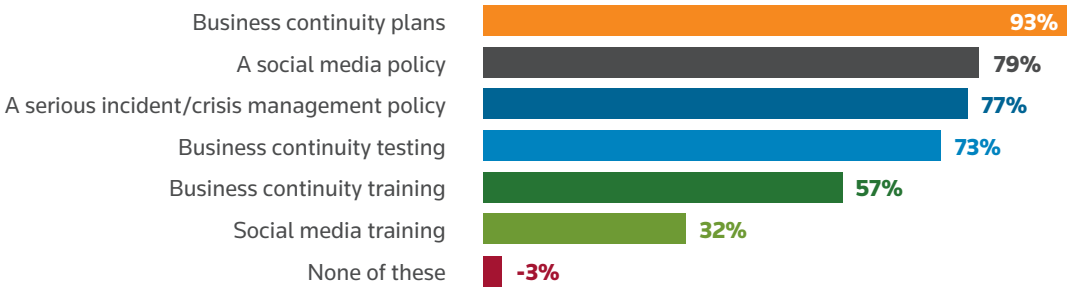
Uptake of online training, as a proportion, is well over half for several key groups: those with formal risk & compliance functions; those where legal or risk & compliance hold management responsibility for the programme; and, highly regulated organisations—financial institutions in particular.

Changing information requirements

As risk & compliance departments become more sophisticated, they increase in size and often operate autonomously from the legal department. The requirement for training these professionals around compliance requirements is still critical to ensure functions can appropriately advise the business on applicable laws and regulations—advice that may previously have been the preserve of the legal department, as indications show that risk & compliance departments are increasingly looking to online training. Running alongside this is the suggestion that demand for traditional 'legal' information and training around regulatory compliance may also be increasingly shifting towards a risk & compliance audience without specialised legal backgrounds. This may increase the demand on providers to communicate the necessary legal knowhow online in easy-to-understand formats.

Continuity and reputational risk measures

Thinking specifically about business continuity and related reputational risk, does your organisation have any of the following?[5]



[5] Base = 149

Controls, tools and processes

As part of the exercise of monitoring and mitigating against the specific risks which respondents identified, they were asked to select the types of controls, tools and processes that their organisations are using to help them manage these risks.

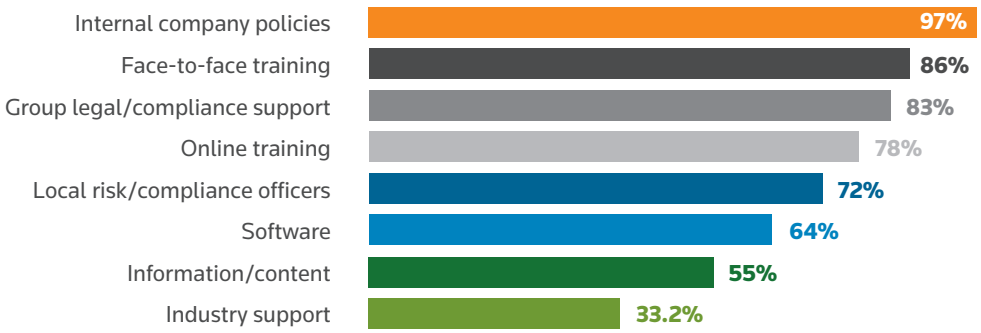
Company policies are the most common base level control tool around risk management, with additional support coming from face-to-face and online training. Group legal support is another common control—especially in the cases where legal is ultimately responsible for risk & compliance, with these organisations far less likely to draw on industry support.

The pattern of controls utilised highlights a couple of small differences when assessed by internal ownership. When the risk & compliance department is ultimately responsible for risk & compliance, use of software becomes more prevalent as a tool, as does the use of industry support.

Notably, where the risk & compliance team is the formally responsible party, organisations are also much less likely to solely rely on internal or external auditing to monitor control usage, highlighting the increased sophistication of operations, as other specific assurance programmes tend to be brought in alongside.

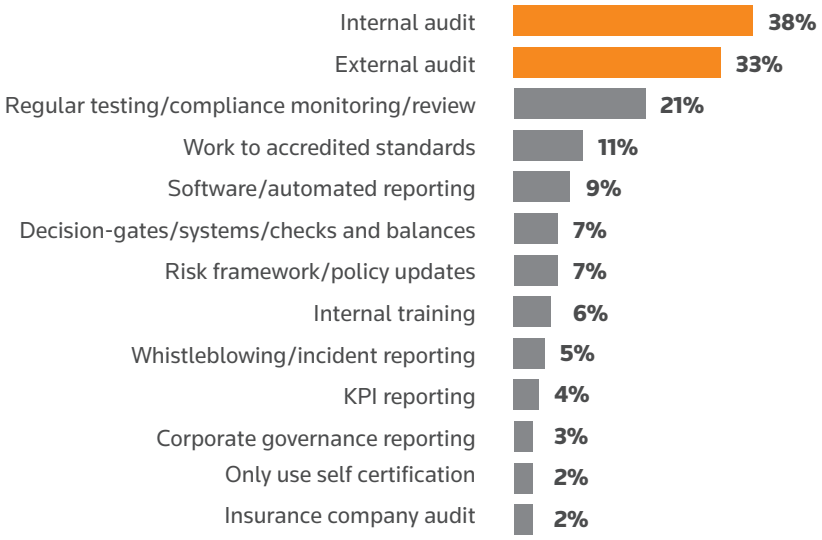
Controls, tools and processes used

What types of controls tools/processes is your organisation usi ng to help manage your risks?[6]



Processes other than self-certification

In addition to self-certification, what processes does your organisation have in place to monitor that the controls are being used?[7]



[6] Base = 151

[7] Base = 107

In addition to auditing and general testing, several key methods—albeit only used by a minority—are in place to monitor the use of controls (see box below).

As a rule, auditing in general, both internal and external, is by far the most common monitoring measure, with around half completely reliant on these to ensure the effectiveness of controls—alongside self-certification. Again, highly regulated companies prove the exception to the trend here—with a comparatively small proportion solely reliant on auditing. Overall, about half or organisations surveyed have some kind of assurance process in place outside of formal auditing.

ACCREDITED STANDARDS	SOFTWARE/AUTOMATION	DECISION GATES
"Accreditation using standards eg. ISO9001 etc". ***Engineering***	"Software controls and checks and balances for each dept". ***TMT***	"Internally there are strict governance pathways and risk registers, checks and balances". ***Banking***
"We are PCI compliant". ***Hospitality/leisure***	"Third party software which is integrated into ten ERP systems and managed through a series of authorisations which limits access to various parts of the system". ***Transport/logistics/distribution***	"Risk processes and inter departmental monitoring, matrix managements, collaborative processes". ***Education***
"We're ISO-something-or-other. [sic] for some of our quality control systems, which are interlinked with our risk management and the use of internal audits". ***Healthcare***	"We have internal systems, so for example, our trading systems have mechanisms to alert breaches of both our internal guidelines and our pooled fund regulations". ***Financial services***	"We have a series of hard-wired processes, effectively decision-gates, which are verified rather than self-certification; so a third-party validation is needed either via a legal team or an authorised individual...". ***Real estate***

Assurance processes

In additional to formal internal/external auditing, what assurance processes does your organisation have in place to measure the effectiveness of controls and monitoring?[8]

[8] Base = 142

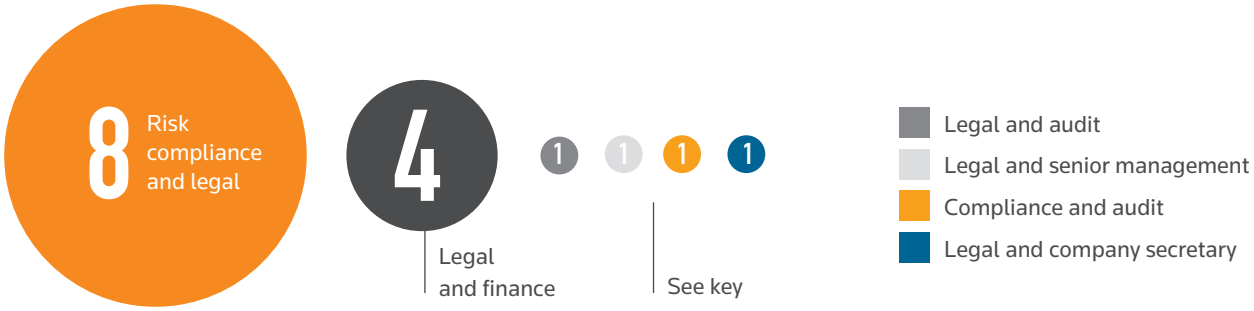
Managing risk & compliance functions

Current ownership of risk & compliance

Of the organisations approached, 55 percent reported that their risk & compliance programme is managed by a dedicated risk & compliance function—with a further 22 percent of programmes being managed by the legal department. The remainder cited a range of dual responsibilities, generally incorporating at least one of these departments, with a minority citing individual responsibility outside of these core departments.

Management of risk & compliance programmes

16 organisations use a dual responsibility model for managing risk and compliance.



8 organisations delegate management to another department or individual.

The changing risk & compliance landscape

Whilst comparatively few do not have a risk & compliance function at all, for many the development of the function has been a key change in the management of risk & compliance over the last five years:

> "[In the past five, we have] built the function in the first place, heavily revised and revamped standard processes and mechanics to best fit the organisation, spent a long time talking about the context the business faces to set the groundwork for compliance and ensure people embrace why it matters". ***Trade***

For others, the emphasis has been on generating a consistent approach across the organisation, ensuring each department is working from the same set of parameters:

> "We had a single, centralised compliance approach, and we've sought to dissociate that across the business whilst still having a strong central lead". ***Real Estate***

Increased inter-departmental dialogue

Viewing risk & compliance as an organisation-wide challenge and adopting an appropriate management strategy in turn—notably, the coordination of differing functions—was regularly reported as a successful change in approach by UK organisations:

Six out of eleven organisations without a formal risk & compliance function had plans to develop one in the near future.

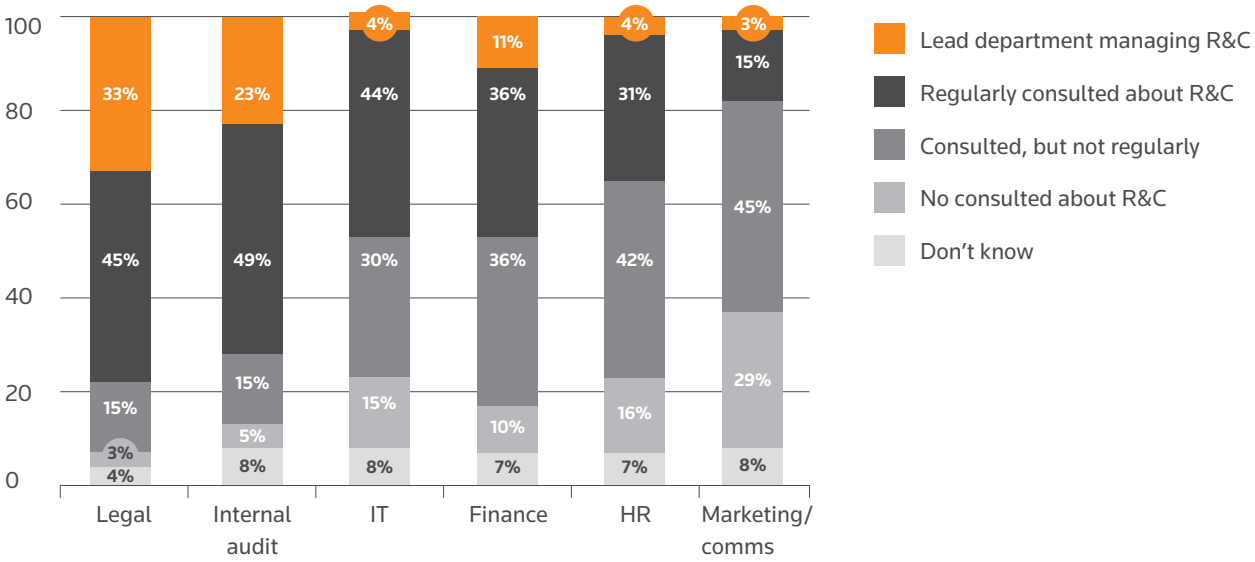
> "A lot more collaboration between the various functions who needs to be aware of matters in particular consultation to ensure there is proper coordination as and when required. More regular training rolled out for appropriate functions and locations. Even more recognition from senior management in terms of how important the topic is and how it is managed". ***Automotive***

For many, this was about ensuring inter-department dialogue and collaboration—with a central management structure to coordinate. However, the research findings indicate considerable differences in the degree to which different departments are brought into the process.

Recalculating results to allow for cases where individual departments do not exist, the findings show legal and internal audit as the primary custodians of the programme[9]. If not, they are at the least regularly consulted about risk & compliance. Beyond these two areas, a more fragmented picture emerges.

Engagement of departments with the risk & compliance programme

Please select the option which best reflects the contribution of each department to the risk & compliance programme.[10]



[9] Specific risk & compliance departments were not measured.
[10] Figures recalculated when departments do not exist at the organisation. Base = 111-141

Almost half of organisations either do not consult, or do not regularly consult, the IT or finance departments. In the case of IT, the department is not consulted about risk at all in 15 percent of cases. Placing this in the context of a common risk register, which sees cyber security and data protection as uppermost on the agenda, leads this to be a somewhat surprising finding.

Conversely, nearly half of organisations do regularly consult IT as a minimum, which seems a prudent and necessary approach given the department's remit in governing all of the information flows entering and leaving any given organisation. A good IT department can help risk & compliance management understand process flows, minimising manual steps and automating processes to ensure data is generally retained within the secure ecosystem of an organisation and, as such, help identify and mitigate associated risks to the organisation—such as, negligence-related data breaches.

For risk & compliance programmes going through the process of formalisation, regular consultation of IT is critical. The teams will have the greatest understanding of any areas of weakness within the systems infrastructure of an organisation and will be best placed to advise when procuring new solutions or making changes as to any potential security implications—particularly in the new age of GDPR compliance.

Continuing GDPR concerns are also likely to have an impact on the extent to which HR and marketing departments are consulted around risk. As things stand, HR is not consulted in 16 percent of cases, and marketing/communications is not consulted in 29 percent of cases—two departments central to GDPR adaptation, as personnel records and CRM system records are key potential risk areas in complying with this legislation.

As this report has identified, company policies are the first line of defence in terms of control tools to manage risk and HR will often play an important role in developing and educating the workforce on company rules and best practice behaviours, enabling a level of self-management of risk across the employee base. Similarly, the need to comply with data retention and processing requirements around personnel records, payroll, recruitment and a myriad of other areas highlight the importance of the HR department in the wider picture of risk management.

Many of these data retention risk factors would also apply to the marketing and communications departments; with general responsibility for client databases, CRM systems and distribution lists, the need to remain compliant with data protection is high on the agenda and obviously important. Marketing and communications teams also have a secondary role to play in protecting the organisation. Any reactive messaging that goes out in the event of an issue, or proactively to reassure clients and customers that the business is taking necessary precautions, is central to managing risk from a reputational point of view.

Evolution of risk & compliance programmes

Whilst formalising departments[11] has been central to organisational changes over the last five years, respondents to the research reported a number of other changes that have emerged over recent years, broadly slotting into six key categories.

The most common area comes under the theme of Organisation – clarifying the parameters of departments and identifying key responsibilities has been a key change over the last five years; bringing in key personnel to either oversee or focus on coordinating risk & compliance across an organisation to promote greater consistency:

> "In the last two and a half years, we have moved to a full, enterprise-wide risk management framework with full governance structure and reporting to the Exec and Board levels". ***Technology***

Main changes to the management of risk & compliance programmes

Please outline the main changes to the way the risk & compliance programme has been managed within your organisation over the last five years.[12]

Organisation	34%	Clarifying departmental responsibilities, assigning/hiring key roles, introducing new functions
Formality	25%	Formalising department, introducing a dedicated team
Detail	24%	Revision of controls and risk registers, training teams, introducing teams, introducing software, becoming formally accredited
Resource	22%	Greater level of resource assigned - in terms of personnel, budget and time
Prominence	22%	R&C becoming a business enabler, engrained in culture and increasing in prominence for leadership
Reaction	10%	Response to specific risk, ad hoc approach as items emerge

[11] In some instances, developing risk & compliance functions from scratch.
[12] Base = 134

Formality is another core development area – risk & compliance has developed into a specific function for many over the last five years with dedicated personnel and increased independence.

> "It's now structured and organised. Five years ago, it was hit or miss, whereas now we have a planned and strategic approach to compliance matters at a local and regional level". ***Natural Resources***

Generally trending upwards, **Resource** is a common area for change: budgets and team size have increased for many over recent years; often respondents link this to growth in the company and increasing compliance requirements, but also to better visibility with leadership.

> "Our budget has increased, and our remit has increased to the point where we're having to expand our team again, because obviously compliance develops over time, and as the business grows so does the compliance obligations; so, we are expanding our team as our business grows". ***Technology***

Whilst some changes are described in the abstract, others concentrate on the **'Detail'** of changes—Building in proper processes and internal controls to monitor and react to risk & compliance—with supporting risk registers and software – has been key. Implementing internal training to ensure staff are fully equipped and working towards accreditations are key examples of detail-orientated measures.

> "Up-skilling has been a key part of the programme, and continues to ensure staff have the knowledge and skills to make the judgements required, with high emphasis on supporting the business to get it right (rather than mopping up afterwards)". ***Insurance***

A rise on the agenda for leadership has increased the **Prominence** of risk & compliance across many organisations and ingrained the concept in the cultural fabric for many. Leadership is recognising risk & compliance management as a necessity, as opposed to a constraint.

> "Compliance are seen as an integral support to projects and business initiatives (rather than being perceived as the business prevention unit)". ***Insurance***

Reaction: external pressures driven by changes such as GDPR and Solvency II, and macro-events like Brexit, have prompted reviews and changes for a smaller number.

> "We have seen a huge increase in compliance requirements—particularly the Bribery Act, modern slavery, failure to prevent tax evasion and now GDPR". ***Manufacturing***

Changes to the departmental ownership of different facets of risk & compliance tends to be specific to individual organisations; however, most changes of this nature fit into four key categories (see table below).

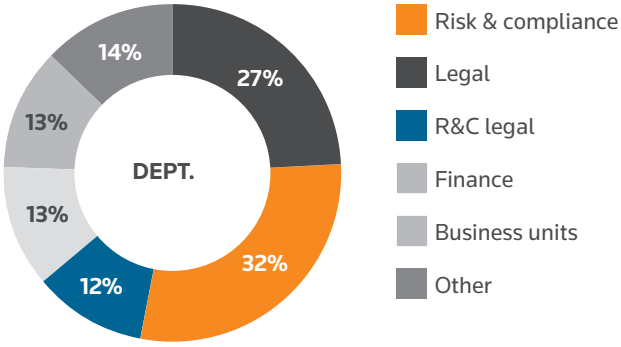
LEGAL OWNERSHIP	AUDIT FOCUS	SEPARATION	UNIFIED
"Following changes in personnel, the management for risk has been shifted to sit with legal, but compliance still sits within the company secretary". ***Transport/logistics/distribution***	"Internal audit split from risk management. Chief risk officer appointed. Compliance and privacy moved from legal to risk". ***Engineering***	"The main change has been the separation of the risk and compliance teams, with increased resources added to both teams". ***Banking/financial services***	"We've moved from various specialist pockets of compliance activity more towards a unified, overall, risk and compliance". ***TMT***
"Legal takes responsibility for it. Before it was a patchwork". ***Retail/wholesale***	"Expansion of internal audit and creation of an internal legal function to support". ***Food/farming/fisheries***	"Separated out the roles of head of corporate risk and head of internal audit" ***Hospitality/leisure***	"We had a single centralised compliance approach, and we've sought to dissociate that across the business whilst still having a strong central lead". ***Real estate***
"Compliance is headed by legal previously it was a standalone department". ***Financial services***	"The chief ethics and compliance officer is directly reporting into the Audit Committee [...] whilst the owner, the Ethics and Compliance department continues ownership of both the compliance program and for enterprise risk management". ***TMT***	"Separation of legal and compliance functions". ***Banking*** "Clearer separation of functions with independent reporting lines". ***Financial services***	

Budget changes

Of the organisations to respond, 27 percent reported that their legal departments managed the risk & compliance budget, with 32 percent passing responsibility to a dedicated risk & compliance function, though in general, where legal takes ownership, organisations are less likely to have this dedicated department. When taken in combination, just under three quarters of all budgets pass through one or both of these departments:

Ownership of risk & compliance budget

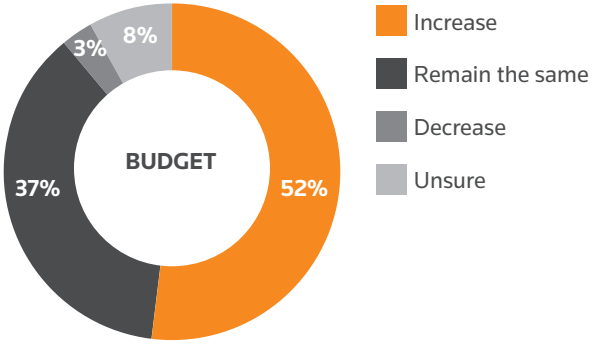
Which department manages your risk & compliance budget?[13]



A smaller proportion of organisations pass budget responsibility for risk & compliance[15] to the finance department or devolve down to individual business units. Interestingly, whilst most respondents were able to report where ownership sits, reporting on specific of budgets was more problematic—many respondents stated that budgets were not specifically broken down for risk & compliance, and many others did not have visibility of exact numbers. This was often due to the difficulties in assessing where budgets sit and whether or not they fall specifically under risk & compliance as opposed to other area—such as, training, external legal support and technology.

Expected changes to risk & compliance budgets

Do you expect the budget allocated to managing risk & compliance to increase, decrease or remain the same over the next year?[14]



Despite specific budgets proving hard to come by, there was far greater clarity on whether they were set to change. Only three percent felt there was likely to be a decrease, with 52 percent anticipating an increase and the remainder feeling budgets would remain steady.

For most, anticipated increases in budgets are a general reaction to the risk landscape; two thirds reported the general risk landscape as a key factor, with high proportions citing new emerging risks, or changes to existing risks.

> "Compliance is becoming so much more due to legislation which has a knock-on effect on compliance. There needs to be more tools, more people, more resources associated with it if you're going to do it properly". ***Transport***

> "With the advent of GDPR etc., risk and compliance has been more of focus". ***Real Estate***

[13] Base = 134
[14] Instead being a cost factored in other areas.
[15] Base = 53

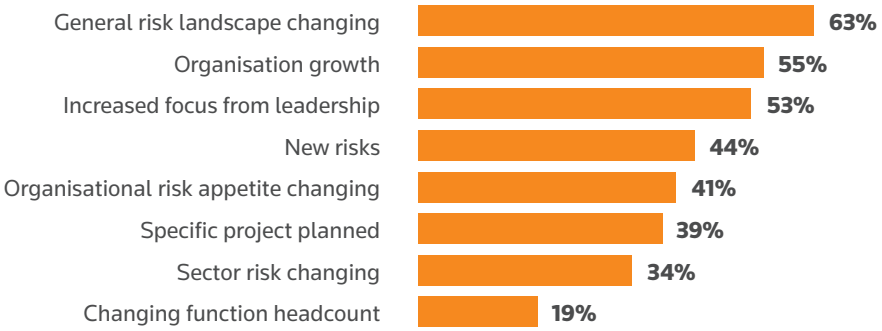
For over half, expected organisational growth is predicted to drive up risk & compliance budgets, with a similar number reporting that budgets are changing in line with an increased focus from firm leadership.

> "There's definitely very high visibility given to the board, which means it is being treated very seriously within the company". ***Transport***

Notably, whilst over half are expecting an increase in spend, comparatively few are reporting an expected increase in the functional headcount of internal risk & compliance teams. Clearly, for many the emphasis over recent years has been to get teams and key roles in place, which potentially explains this difference as many will already have made key hires. However, an ongoing challenge for many risk & compliance functions is likely to be managing increasingly sophisticated risks without a corresponding increase in internal personnel. The results suggest that many are drawing on third parties for support—with external ad hoc support likely to be easier to justify over headcount, and the added benefit of being able to draw upon more specific expertise.

Drivers of increased budgets

What are the key areas driving this change?[16]



Only **3%** anticipate a decrease in R&C spend, with **52%** anticipating an increase

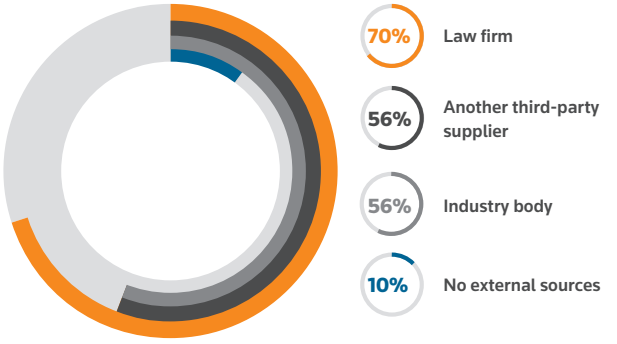
[16] Base = 80

External support

External audit support is particularly important when assuring processes, and similarly, the vast majority of organisations draw upon some sort of external support to help them stay informed about regulatory changes—in fact only 10 percent reported that they used no external sources for regulatory support. Where external support is drawn upon, law firms are the most common source of advice, with seven out of 10 turning to this. As would be naturally expected, where legal control the risk & compliance budget law firm usage is higher still, as it is for larger organisations, rising to nine out of 10 for those with greater than £1 billion revenue.

External support for regulatory changes

Which of the following external sources does your organisation use to keep informed of regulatory changes?[17]

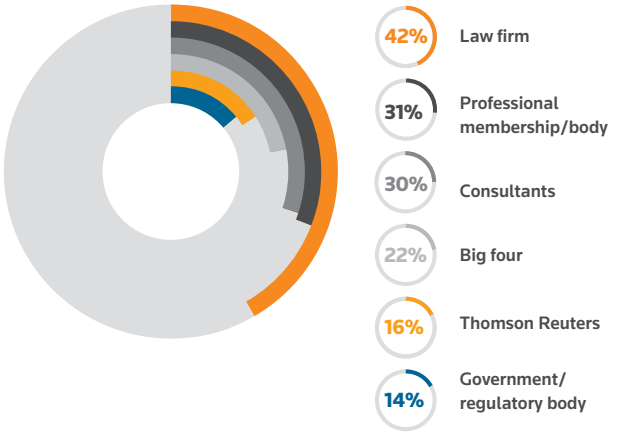


However, over half are also drawing on other third-party suppliers, with a comparable proportion looking to industry bodies for professional guidance. Beyond law firms, professional membership bodies are the next largest category of third-party support—with smaller organisations by revenue more likely to be utilising these as sources of advice. Individual consultancies are also deemed to be effective third-party suppliers, with numerous specialist agencies cited covering areas such as product compliance and health and safety, as well as risk management specialists and regulatory support agencies.

The Big Four also have a reasonable presence in this sphere, accounting for around a fifth of third parties used outside of law firms and industry bodies.

Third parties used

Which third party/parties do you use to help monitor changes in regulation?[18]



Whilst third party usage is common, not all of the support is formally mandated. A reasonable minority relying on third parties to distribute content via newsletters and generally raise their awareness of areas that require attention, but without a formal mandate for doing so.

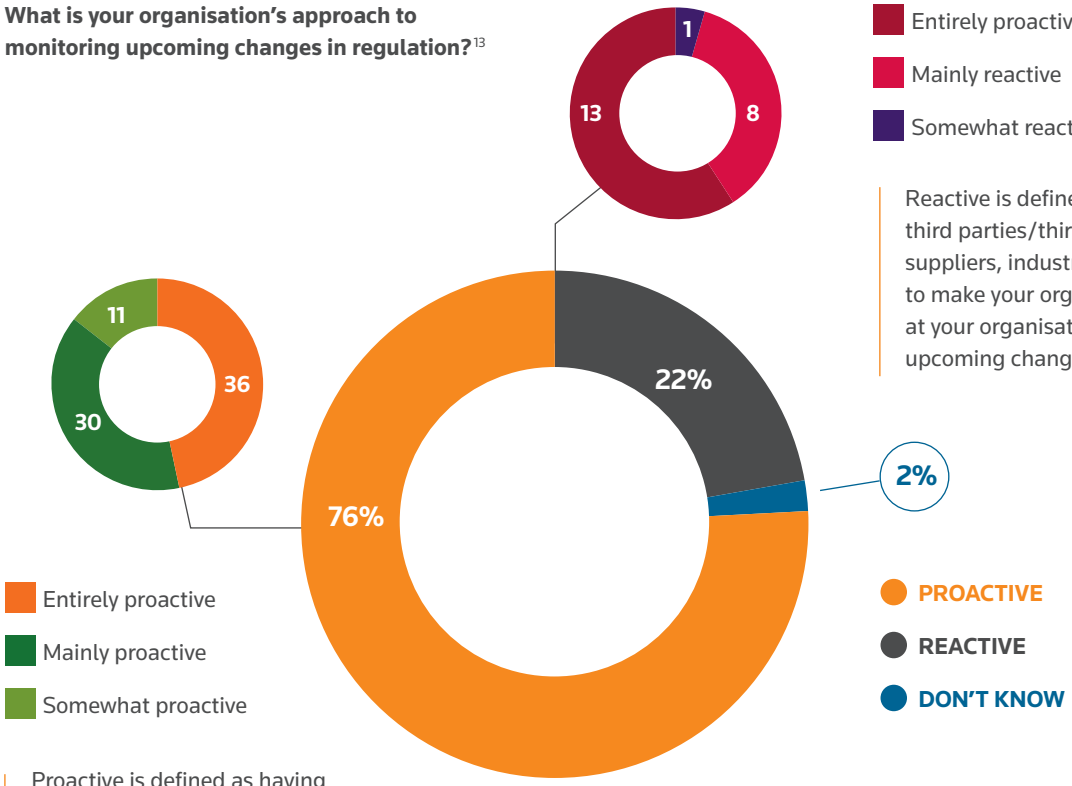
Where organisations have reached the stage where they have a dedicated internal risk & compliance function, the sophistication of approach becomes more evident. These organisations are more likely to be taking a proactive approach to this area of risk management—formally mandating internal staff or external suppliers with monitoring changes in regulations—reinforcing the notion of an increased appetite for legal information to be channelled directly to risk & compliance professionals. Whilst a higher proportion of organisations without these functions are increasingly, though by no means exclusively, taking a slightly more reactive approach.

A balance is being struck for most in this area. Only a small proportion report an entirely proactive approach, and only a tiny number report an entirely reactive approach. The majority are adopting a moderately proactive approach.

[17] Base = 80
[18] Of those using any third parties. Base = 64

Regulatory proactivity

What is your organisation's approach to monitoring upcoming changes in regulation?[13]



Reactive is defined as relying on third parties/third party content (e.g. suppliers, industry bodies, media etc.) to make your organisation/individuals at your organisation aware of current/ upcoming changes in regulation.

Proactive is defined as having internal individuals/external suppliers with formal responsibility/ mandates for monitoring changes in regulation and reporting back to the organisation

Communicating risk to leadership

As this report has identified, one of the most substantive changes around risk & compliance management in recent years—and one that has arguably enabled other changes—is the increased concern of risk & compliance to organisational leadership. As leadership become more engaged and concerned about key areas, budgets increase, team sizes increase, and the programme develops in sophistication, allowing it to become more embedded in an organisational culture.

Drawing upon this theme, this research identified the most common methods of reporting risks to the Board. Common formats remain rooted in conventional Word, Excel or PowerPoint deliverables, but the content varies depending on the Board's preferences, with some common areas outlined in the table on page 19.

Whilst reporting does vary, it tends to be rooted in a set of consistent areas: boards value a concise summary or scorecard of risks, often by RAG status, highlighting the key areas of most importance and relating risks to existing projects or strategies. Longitudinal analysis appears valuable to place each risk in context, and to help decide whether things need to be escalated or where actions need to be taken.

[16] Base = 152

Most common method of reporting risks to the Board

KRIs/scorecards	"The Board receive a report which shows the current view of aggregated risk to the company by each risk category, compared to the Board approved appetite thresholds. Risk events are reported against risk categories. A small number of KRIs are in place for each defined risk category". ***Investment***
Current risks	"Key current risks and mitigating actions, risk horizon, significant risk incidents, risk assurance outcomes". ***Insurance***
Mitigating actions	"We do formal papers, attaching the risk register, with tables showing if the risks are changing and also commenting on the risk appetite and mitigations". ***Manufacturing***
Escalation points	"Executive summary, top and emerging risks, matters for escalation from committees, matters for decision, matters to note, key trends". ***Investment***
Trends	"Information on high risk projects, major bids, compliance issues, risk trends, key risk indicators". ***Engineering***
Early warnings	"Key Risk Indicators' performance against risk appetite (i.e. early warning indicators)". ***Financial Services***
Longitudinal changes	"A table is produced showing trend, appetite and changes over since the previous reporting period and covering the strategic risks only". ***Transport/Logistics/Distribution***
Worst case	"The key ones are we have certain categories where the first one is a kind of tick-in-the-box to see whether it applies or not in that particular moment in time, and then we have details of the worst-case and what are actions being taken". ***Technology***
Incidents	"Risk register and heatmap; risk policies; KRIs; breaches; complaints etc". ***Financial Services***

Conclusion

The profile of risk & compliance professionals and teams will continue to develop and grow as functions become even more established and formalised. This will be driven by parallel growth in the challenges presented by business risks, which will continue to heighten risk & compliance priorities on corporate leaderships' agendas. This research indicates strong reactions to these challenges: growth in dedicated teams; significant investment in key personnel, training and technology; and a drive towards a consistent, properly coordinated approach to managing risk & compliance.

The sophistication of risk & compliance teams is developing to enable them to help their corporate entities navigate an increasingly complex risk landscape. Brexit, GDPR and growing cyber security concerns are just a handful of the current threats, and the indications we have seen of a growth in resources in turn – both in terms of budget and headcount – show no sign of dropping off.

The types of providers risk & compliance functions turn to for external support may also continue to develop in turn, especially as the type of content and knowhow they require changes and adapts. New controls and assurance processes are often brought in alongside formal auditing, utilising various technological techniques and systems, for which risk & compliance functions may need third party support. The growth of dedicated risk & compliance functions – often separate to the legal department – may also change the way information needs to be consumed, as demand for traditional 'legal' information and training around regulatory compliance has the potential to shift towards a risk & compliance audience without specialised legal backgrounds. This may increase the demand on providers to communicate the necessary legal knowhow online, in easy-to-understand formats.

Thomson Reuters

Thomson Reuters is the world's leading source of news and information for professional markets. Our customers rely on us to deliver the intelligence, technology and expertise they need to find trusted answers. The business has operated in more than 100 countries for more than 100 years. For more information, visit **www.thomsonreuters.com**.

Acritas
SHARPER INSIGHT

the answer company™
THOMSON REUTERS®