

ashurst

ashurst
RISK ADVISORY

IMPACT BEYOND TRADITIONAL MEASURES

Risk insights through the lens of a General Counsel

UK EDITION 22/23



Contents

Foreword	1
Executive Summary	2
1. Understanding of Risk & In-House Expertise	4
2. Data Management	6
3. Cyber Risk	8
4. Governance Burden & Responsibility Management	9
5. Crypto	10
6. UK Corporate Reform	11
7. Financial Crime	12
8. Financial Resilience, Incident Management & Operational Resilience	13
9. ESG	14
Benchmarking	15
Key Contacts	16

Foreword

This report provides a unique and valuable perspective for all C-suite and senior executives on current and emerging areas of risk and some insights on how to manage personal accountability in this volatile risk environment.

Our insights are based on:

1. perspectives from Partners in our Risk Advisory team and Partners in our Legal practice, and
2. a research-based survey conducted across a group consisting of 52 General counsels and senior legal executives spanning across various companies in a range of sectors and covering 40 detailed questions.

We would like to thank the organisations that took part in our survey and are delighted that so many took the time to participate.

This is our first year of running this survey which aligns to the introduction of our consultancy business, Ashurst Risk Advisory, to the UK market. We have also had requests for insights from the senior executives among our client community, who are currently facing the challenge of managing unprecedented and complex forms of risk.

Organisations are facing challenges on a scale that we have not seen since the financial crisis, albeit this time the level of uncertainty in the market is unparalleled. With interest rates rising much like the spread of a pandemic, war-driven supply chain issues, and the declining pound, the pressure on businesses is at a critical tipping point.

Add to this the dynamic forms of risks that businesses are facing – such as the increasing threat of cybercrime, managing data effectively, the evolving methods of financial crime, implementing ESG, overseeing operational risk, technology implementation, and the increasingly complex challenge around effective governance and accountability – there is a hefty list of risks to wade through before the 11 am coffee break on most days.

The savvy organisations are generally one step ahead in terms of understanding that there is an impact to their operational risk frameworks, but most are likely to have to do a lot of critical thinking in order to manage risk effectively in this challenging and unfamiliar economic and social environment.

Executive summary

In little more than two years, the UK economy, public finances, and companies have felt the consequences of a global health crisis caused by Covid-19, a global security crisis sparked by Russia's invasion of Ukraine, and a global energy crisis brought about by both. In a little over a decade, we have also felt the economic and fiscal consequences of a global financial crisis and the uncertainty created by the UK's decision to leave the EU and the negotiations that followed.

In the decades ahead, governments in the UK and around the world face perhaps the still greater economic and social challenges of addressing climate change, dealing with the costs of ageing, and managing all of these pressures and risks against a backdrop of potentially weaker productivity growth, higher levels of public debt, and elevated interest rates.

It is hard to escape the conclusion that the world is becoming a riskier place. It is against this backdrop that the role of an executive or senior manager within a company has become much more about effectively managing current risk and foreseeing future risk within the context of an increasingly regulated landscape.

The role of General Counsel in particular has always been about risk management, but likely more so now than ever. General Counsels have often been a moral, ethical, and regulatory compass for their organisations as well as the chief advisors on moderating reputational issues and addressing systemic risks.

Traditionally, the role of in-house legal counsel is to understand the pressure points, strategy and objectives of the business and effectively communicate the risks and legal issues involved in any decision to management. This enables management to make informed strategic choices within an acceptable legal risk profile.

While this position still holds true, the role of legal counsel is very clearly not limited to managing the legal risk associated with the businesses that they work within but spans across the entire organisations operations and its internal and external footprint.

Given the dynamic and wide-ranging nature of risk that companies now face which include internal and external stresses, the role of General Counsel is arguably more critical than ever to help an organisation navigate the storm and remain unscathed. Equally the relationship between the General Counsel and other C-suite executives is also crucial in managing risk effectively and proactively, both for the organisation and for *each individuals personal accountability*.

It is hard to escape the conclusion that the world is becoming a riskier place.

The lawyers that participated in our survey state that they face risks in the following areas and would like to gather insights from other companies on:



Cyber risk



Engagement with the regulator(s)
and changing regulations



GDPR, privacy and
data management risk



Governance and accountability



Financial crime



Operational risk and financial risk



Conduct risk



Crypto evolution



ESG

1. Understanding of Risk & In-House Expertise

Despite businesses across the globe working within a period of uncertainty, in-house legal teams are reporting their lowest level of risk-readiness in some time. This is partly because many of the top risks – such as personal accountability, the increasing risk of a cyber-attack, and operational risk readiness – are unprecedented. Notwithstanding this, senior lawyers have become seriously overstretched with the clear majority (58%) stating that they are just keeping up with their workload or falling behind (see Figure 1). With this level of risk and resource stretch it is clearly a balancing act for most and an indication that the General Counsel must work closely with other executives such as the CEO, COO and CRO to prioritise focus, while remaining agile in their response to the unexpected.

Figure 1: UK legal team workload



Many lawyers who participated in our survey report that without the thinking time to assess risk effectively they are often left firefighting with the business to protect the company from regulatory risk, client detriment, and reputational damage. Almost a third (29%) report they lack the time to address matters with the level of detail required, and almost as many (27%) suggest this is preventing them from being able to proactively plan for emerging risks.

Participants in the survey report that the following harm has crystalised within their company in the last twelve months (see figure 2):

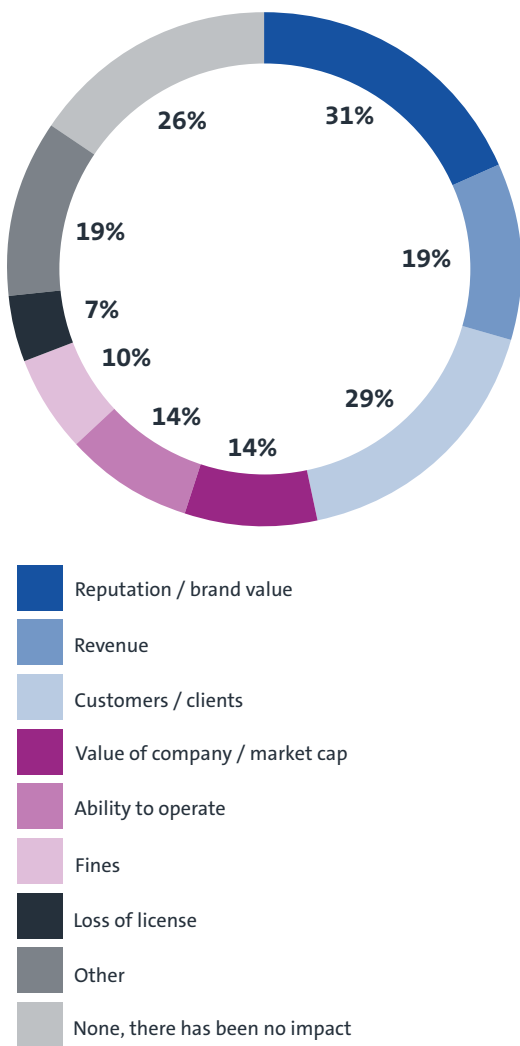
Figure 2: Crystalised risks that companies have faced in the last 12 months



Many of the top risks – such as personal accountability, the increasing risk of a cyber-attack, and operational risk readiness – are unprecedented.

More alarmingly 74% report that crystallised risks have caused various levels of impact such as reputational risk and detriment to customers (see figure 3).

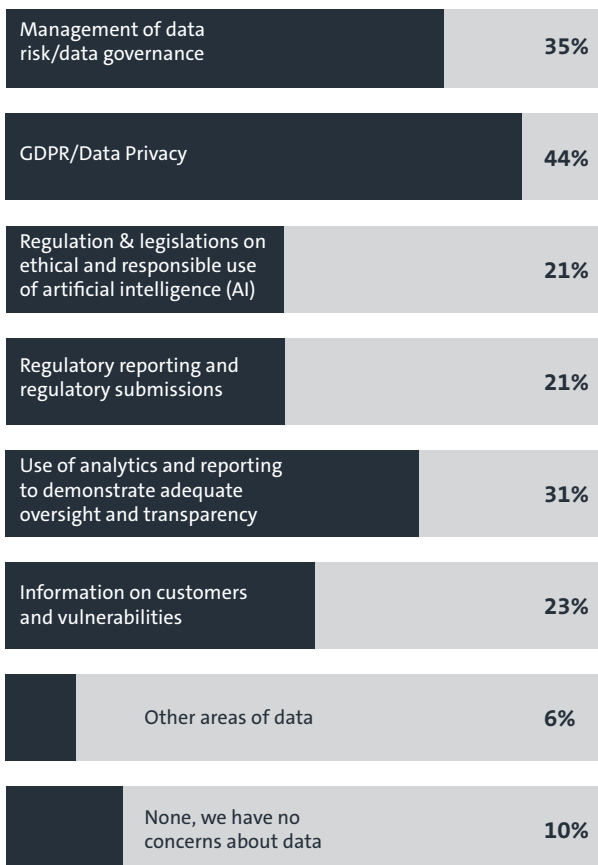
Figure 3: Crystallised impact of risk companies have faced in the last 12 months



2. Data Management

As businesses are increasingly going digital and business models are data driven, data governance remains an overwhelming concern with 35% of company lawyers reporting that management of data risk and governance is a key concern. A staggering 67% are also concerned about GDPR, data privacy and information on customers and their vulnerabilities (see figure 4).

Figure 4: Company concerns for data management over the next 12 months



Unsurprisingly, these concerns are exacerbated by the broader trend of digitalisation of business models and products, the reliance on data and automation, and the accelerated capture and use of increasing amounts of personal information. This has led to significant data challenges for Counsels to deal with. The European Company Lawyers Association found in its report Data-Driven Business Models that while GCs have ambition to drive and enable the businesses that they support to embrace data-driven models, there are significant obstacles to progress given this comes within the context of a more complex legislative and regulatory framework¹.

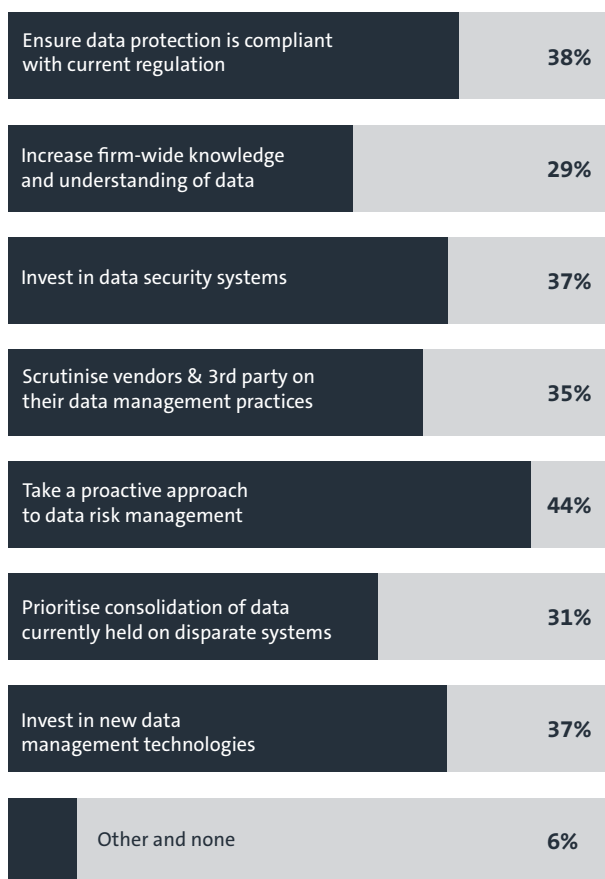
As the rate of digitalisation increases, and the threat of cybercrime heightens, organisations need to continue re-thinking how they manage emerging areas of data risk. Additionally, as well as helping to manage governance risk, new risks can also be created by the mismanagement of data, for example, when data is held across disparate systems and does not enable an accurate assessment of risk.

To mitigate data management risk, 44% of lawyers agree that their company needs to take a proactive approach, and 37% say that their company needs to invest in new data technologies and data security systems. A staggering 35% are concerned about the level of scrutiny of third-party suppliers in the context of the evolving regulations in this space and the threats posed by cybercrime (see figure 5).

¹ <https://ecla.online/data-driven-business-models/>

Concerns are exacerbated by the broader trend of digitalisation of business models and products, the reliance on data and automation, and the accelerated capture and use of increasing amounts of personal information.

Figure 5: Mitigations required to manage data risk



Interestingly, 38% feel the need to prioritise compliance with current data protection regulations, which comes against a backdrop of regulatory uncertainty and the high cost of compliance. Meanwhile 40% of those surveyed are particularly concerned with expected post-Brexit reform to GDPR, which although cited as a simplification is likely to cause more complexity for businesses with a cross-border impact through the introduction of new legislation in the Data Protection and Digital Information Bill. In addition, 42% of our population of lawyers quite rightly remain concerned about the risk of GDPR non-compliance through data processing across multiple systems and personnel, and 35% struggle with obtaining assurance on GDPR compliance from their third-party suppliers and data processors in their supply chains.

While GDPR remains high on the list of data management risks, it is clear from the results of our survey that data management has become much more complex in this digital age and is a vital contender for the boardroom to consider when managing the risk profile of a company.

3. Cyber Risk

While technological advancement is generally a good thing, it also introduces new levels of risk. In our survey, 40% of lawyers state that their company was concerned with mitigating cyber risks and 33% were concerned with the associated threat of litigation (see figure 6).

Figure 6: Concerns over cyber risk



It was reported earlier this year by the BBC that 74%¹ of all money made through ransomware attacks in 2021 went to Russia-linked hackers. Statistical research also found that the average cost of a UK data breach in 2021 was \$5.05 (£4.48) million and 18% of UK companies experienced a data breach at least once a month.² Add to this the fact that many cybercriminals continue to be well funded, with the means to invest in new technology and resources, and it is clear why organisations and government continue to be on high alert.

More than two-thirds, 69% of our survey respondents, state that their company faces challenges when

Many cybercriminals continue to be well funded, with the means to invest in new technology and resources, and it is clear why organisations and government continue to be on high alert.

implementing cyber regulations and standards, despite having some internal expertise. A staggering 48% go on to state that they are not comfortable with their company's defences against a cyber-attack.

These results are not surprising given that a Denial of Service or extortion campaign can lead to institutions losing an inordinate amount of revenue, even without a ransom being paid.

In a typical Denial of Service attack, a key system is likely to be impacted which will result in downtime for that system and other connected systems for a period of time until the site can be put back online. This might be because of a flood attack, or simply for damage control during an investigation and recovery period. Evidence has shown that even a few minutes of downtime can have a severe impact on a company's bottom line and public reputation. In total it is estimated that the total financial burden to the UK is likely to exceed an eye-watering £1 billion per year³.

Any defences in this area are only likely to work where there has been a realistic challenge in terms of the stress tests that are applied given that the impact of a cyberattack can be felt for a long period after the event. Additionally, as the cybersecurity landscape becomes more complex and hackers develop new and innovate ways to access data, companies must factor this into their solutions to ensure that they can continually provide a secure experience for their customers. This is another example of a risk where lawyers and subject matter experts must work together to ensure an adequate, well-tested and thought through plan is put in place.

¹ <https://www.bbc.co.uk/news/technology-60378009>

² https://www.statista.com/topics/8131/cyber-crime-and-companies-in-the-uk/#topicHeader__wrapper

³ <https://datacentre.solutions/news/56573/cost-to-uk-economy-of-ddos-cyber-attacks-may-exceed-1-billion-per-annum>

4. Governance Burden & Responsibility Management

Given the role of General Counsel within the risk management framework of a company, much like any executive from the C-suite, Counsels face challenges in carrying out effective risk management due to a range of factors including the fact that their role now requires a holistic consideration of risk across the various functions and departments within the company. Getting this cross-functional oversight model right is a significant challenge. Add to this the level of accountability that now goes hand in hand with a Board role and the expected standards of risk management, it is a challenge that should not be underestimated.

In our survey, 58% of lawyers confirm that their oversight responsibility now extends to other functions within the company outside the Legal department. 58% also highlight that they feel exposed by the responsibilities that they must delegate to other departments, with a majority (54%) claiming that there is not enough transparency for effective risk management. 48% of our population added that management information is inadequate and does not objectively provide a view of risk.

Counsels face challenges in carrying out effective risk management due to a range of factors including the fact that their role now requires a holistic consideration of risk.

A third of company lawyers state that miscommunication is a barrier to managing risk. However, there was also a variety of other reasons provided including outdated risk assessment practices, inadequate governance arrangements, and a lack of knowledge (see figure 7)

Figure 7: Barriers to managing risk.



5. Crypto

Of the company lawyers that we surveyed, 54% of the population state that their company is involved in some form of crypto based activity, either for themselves, for their clients, or both.

The Financial Stability Board states that crypto-asset markets are fast evolving and could reach a point where they represent a threat to global financial stability due to their scale, structural vulnerabilities and increasing interconnectedness with the traditional financial system.

On the basis that crypto can no longer be considered a niche area and is expected to be subjected to an incoming wave of regulation it is certainly an area that requires attention.

Almost three quarters (73%) of company lawyers state that financial crime and fraud risk relating to crypto is continually evolving and becoming more sophisticated. This statement is supported by the fact that one of the most significant levels of cybercrime over the past couple of years has been seen across crypto platforms. Perhaps the scariest and most shocking fact is that, while cyberattacks on crypto platforms requires a basic understanding of how cryptocurrency transfers and wallets function, they do not currently require sophisticated tooling to find success.

The Chainalysis 2022 Crypto Crime Report found that crypto-related crime hit an all-time high in 2021 with illicit addressing receiving \$14 billion over the course of a year, approaching twice the \$7.8 billion extracted in 2020.¹ The majority of the crime was related to scams, as in previous years, but the share of outright stolen funds increased substantially.

Over two-thirds of company lawyers believe the UK regulatory and legislative framework is insufficient with respect to crypto, and in particular, that safeguarding regulation is required over crypto (see figure 7).

On this particular matter, the Financial Conduct Authority (FCA) has been consulting on how the client asset principles and safeguarding rules might apply to crypto assets through a recently hosted Regulatory Sandbox event. However, as was debated during the Sandbox event by professionals in this space, there is much work still to do given that

Over two-thirds of company lawyers believe the UK regulatory and legislative framework is insufficient with respect to crypto, and in particular, that safeguarding regulation is required over crypto.

crypto assets do not meet all the characteristics of a traditional security, and the third parties usually offering and holding crypto assets will require wholesale change to behave as a custodian or sub-custodian and comply with the relevant rules.

New legislation is certainly needed more than ever as evidenced by public reaction to the recent insolvency loss disclosures made by large crypto houses such as Coinbase. As seen in more recent times, there is also a significant level of regulatory arbitrage while the market remains open to interpretation. For example, practices such as crypto lending is common even though it is not yet subject to the same market practices as would be the case with traditional securities lending, which can mean that loans are not always collateralised adequately and customers are left exposed.

Figure 8: Crypto risks and challenges



¹ <https://go.chainalysis.com/2022-Crypto-Crime-Report.html>

6. UK Corporate Reform

The UK Government recently responded to its corporate reform package which represents a significant change that, for in scope companies, not only extends the information that companies are mandated to report, but could also require directors to disclose how they gain comfort around the information obtained to support their assertions before the disclosures are made. The reform will have far-reaching impacts on Boards and their accountable executives, as well as audit committees, finance teams, audit firms and professional bodies.

Notwithstanding the clearly significant impact that the reform will have, 63% of company lawyers agree that the Government's proposals are suitably proportionate, and an overwhelming 81% agree that the objective of strengthening Boardroom focus on internal control matters is required.

Unsurprisingly 60% of lawyers are concerned about the impact of the reform package on both stakeholders and shareholders. 31% are also concerned about the requirement for the Board to disclose its internal control assessment and the basis for that assessment (see figure 9).

This concern is well-founded as the savvier General Counsel will appreciate that the internal controls assessment mandated by the reform extends beyond regimes such as SOX, which are focused on financial control risk, and instead requires the directors to provide a view on the effectiveness of the internal control frameworks in the broadest sense.

Alarming, this means that scope is not limited and includes everything from financial controls, to operational controls, and compliance controls. The directors will also be required to disclose a resilience statement that sets out how they have assessed

UK corporate reform will have far-reaching impacts on Boards and their accountable executives, as well as audit committees, finance teams, audit firms and professional bodies.

the organisations prospects and addressed the challenges to the business model over the short, medium, and long term.

While some respondents state that their companies are prepared for the reform, we believe that the likely impact and the level of work required to prepare the organisation and its Board for making such public affirmations has not reached the office of General Counsel. This is an example of another key area where the CEO, the COO and the CRO will need to work closely with General Counsel as the business frames its programme of work in support of the director assessments and public disclosures that must be made.

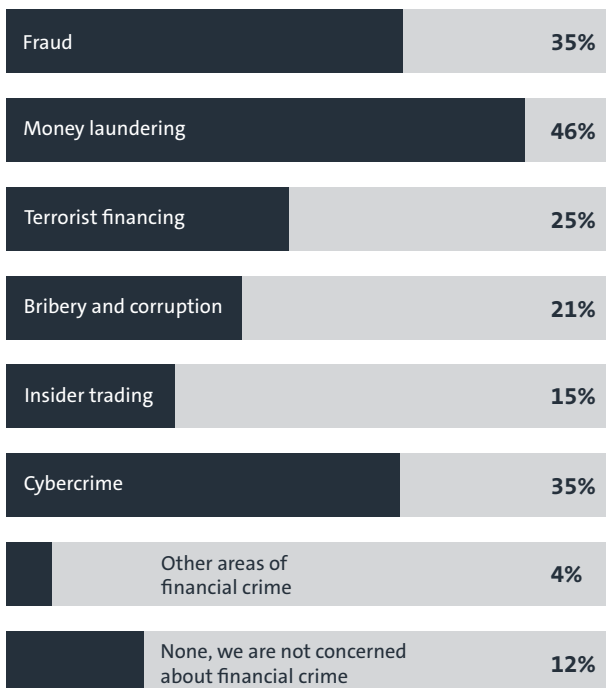
Figure 9: Areas of concerns in relation to the UK corporate reform



7. Financial Crime

Despite international anti-money laundering initiatives (and an ongoing UK review with legislation planned), financial crime remains at the forefront of risk and concern among company lawyers, with 88% concerned about experiencing some form of it in the next 12 months. High levels of concern exist in relation to fraud, money laundering, terrorist financing, bribery and corruption, and cybercrime (see Figure 10).

Figure 10: Financial crime concerns next 12 months



Both internal and external threats to an organisation are at unprecedented levels with the increased risk profile that comes with digital advancement, and the fact that consumers are still often easy targets.

The fears about financial crime are certainly not unfounded. Both internal and external threats to an organisation are at unprecedented levels with the increased risk profile that comes with digital advancement, and the fact that consumers are still often easy targets. Three-quarters of company lawyers state that internal risk is just as concerning as external risk.

Add to this the fact that criminals continue to adopt increasingly complex attack techniques and more sophisticated methods of financial crime, and it seems to be an uphill struggle where the ground never gets to an even standpoint. 67% of lawyers have concerns over their company's ability to keep up with the evolving methods of financial crime.

A Social Market Foundation report found that fraud has become the UK's most common form of crime and estimates that it costs the country £137 billion per year, which it suggests results from both underfunding of law enforcement and outdated institutional arrangements.¹

An alarming 73% of respondents to our survey report that financial crime could be better assessed across the company's three lines of defence model, 71% state that financial crime related risk reporting to senior management requires improvement, and 63% are concerned that evidence to support the company's assessment of its financial crime risk is not adequately maintained.

In terms of regulators and supervisory bodies with an interest in financial crime, it is clear that company lawyers have a unique line of sight across this wide range of stakeholders. Among our survey population, 42% of clients are concerned with the FCA, 38% are concerned with the Financial Reporting Council, 40% are concerned with HMRC and 23% are concerned with the SFO.

¹ https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/

8. Financial Resilience, Incident Management & Operational Resilience

Financial resilience, incident management and operational resilience continue to be a key concern for regulators and companies.

The litmus test is whether a firm has proper frameworks in place which have been challenged personally by the Board and tested against extreme stress scenarios. For example, is the organisation robust enough as a going concern to allow for orderly wind down as a gone concern, and, in the event of an extreme trigger or market event, is the organisation operationally resilient and can it continue?

Notwithstanding that these risks remain a high priority area for many members of the C-suite, including the CEO, the COO and the CRO, the General Counsels surveyed were largely unaware of this as a key open risk for their organisations and 90% of them felt that their organisation must have a plan in place.

Alarming this single assumption causes the greatest cause for concern. While financial risk management and operational risk management are largely not within the day-to-day remit of the General

Counsel, we would expect that lawyers are involved in understanding what planning is in place, what stress tests are performed and, more importantly are being made aware of what residual risk their organisations are exposed to. This expectation arises both because of the fact that the role of General Counsel is largely about risk defence but also by nature of the fact that every member of the C-suite is likely to be held personally accountable.

The litmus test is whether a firm has proper frameworks in place which have been challenged personally by the Board and tested against extreme stress scenarios.



9. ESG

ESG has become a buzz phrase within the media. However, the letters E, S & G, which seem so innocuous on paper, have the power to shift industries for the better. The challenge for companies remains how to address ESG risk effectively given that it has wide-ranging impacts from investment strategies, to product design, diversity goals, and staff facilities.

ESG risk is now very much a part of regular business risk. The fact of the matter is that ESG cannot be approached as a remediation exercise, and instead should be a fundamental change in the mentality of the organisation and the way to operate. It is about conscious decision making and a shift in the paradigm of the normal operating model.

Consideration of ESG factors has grown from a niche concern among sustainable investors to becoming a widespread expectation from society as a whole and a mandatory requirement for many organisations. Consequently, there are financial and reputational risks associated with the exposure of detrimental practices, despite being legal, and not living up to socially-imposed high standards of corporate citizenship.

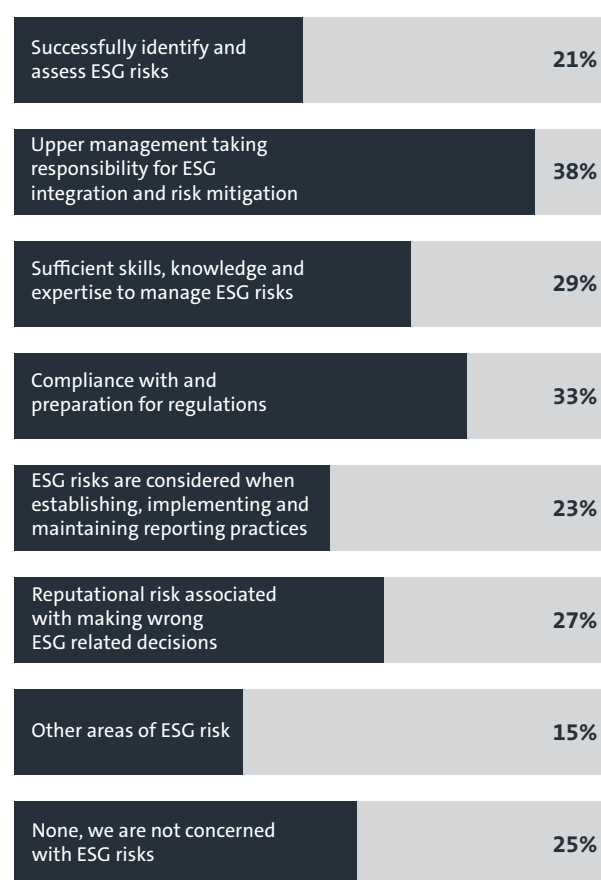
While many companies are no doubt sincere, certain companies are being accused of greenwashing. Whether the greenwashing is intentional or unintentional, the consequences to reputation seems to be the same, and the risk of litigation is tangible.

Company lawyers need to be concerned about ESG not just from a legal perspective but also from the very real threat of the commercial damage that can arise from activities such as activist campaigns and consumer boycotts.

75% of respondents state they were concerned about ESG-related risks over the next 12 months. Specifically, almost two-in-five company lawyers were particularly concerned about senior management taking responsibility for ESG integration and risk mitigation, while just under a third were concerned with the lack of skills, knowledge and expertise within their organisation to manage ESG effectively (see figure 11).

Surprisingly, only 27% of lawyers state that they were concerned with the reputational risk associated with making wrong ESG-related decisions. This is particularly shocking given that this is an area where reputation could be subjected to significant harm in a very public forum, with a serious knock on impact to commerciality.

Figure 11: ESG risks causing concern over the next 12 months



Consideration of ESG factors has grown from a niche concern among sustainable investors to becoming a widespread expectation from society.

Benchmarking

Ashurst Risk Advisory surveyed 52 company lawyers mainly working in the UK, representing companies with a combined turnover of £10bn and 740,000 employees. General Counsels and heads of legal made up two-thirds of this population. The largest proportions work in a global headquarters (42%) or regional headquarters (37%), with the remainder based in country offices (21%).

Respondents' companies are from a wide variety of economic sectors, with the biggest proportions in financial services and real estate and the remainder split across sectors such as technology, telecommunications, industrials, and healthcare.

Research was conducted online during Q3 2022. As a consequence of rounding up percentage results, the answers to some questions might not always add up to 100%.



Key Contacts

RISK ADVISORY



Nisha Sanghani
PARTNER
T +44 20 7859 2733
M +44 7917 004 608
nisha.sanghani@ashurst.com



Matthew Russell
PARTNER
T +44 207 859 2498
M +44 7909 987 629
matthew.russell@ashurst.com



Matthew Worsfold
PARTNER
T +61 2 9258 5776
matthew.worsfold@ashurst.com

LEGAL



Lee Doyle
PARTNER
T +44 20 7859 1837
M +44 7826 930 768
lee.doyle@ashurst.com



Jake Green
PARTNER
T +44 20 7859 1034
M +44 7876 030 472
jake.green@ashurst.com



Ruby Hamid
PARTNER
T +44 20 7859 3922
ruby.hamid@ashurst.com



Rhiannon Webster
PARTNER
T +44 20 7859 3070
M +44 7917 005 541
rhiannon.webster@ashurst.com



Will Chalk
PARTNER
T +44 20 7859 3066
M +44 7823 341 024
will.chalk@ashurst.com



Etay Katz
PARTNER
T +44 20 7859 3133
M +44 7795 456 441
etay.katz@ashurst.com



Anna-Marie Slot
PARTNER
T +44 20 7859 3724/+85 228 468 966
M +44 7788 710 892/+85 297 081 522
anna-marie.slot@ashurst.com



Nathan Willmott
PARTNER
T +44 20 7859 2036
M +44 7720 561 220
nathan.willmott@ashurst.com



This publication is a joint publication from Ashurst LLP and Ashurst Risk Advisory LLP. Both are part of the Ashurst Group which comprises Ashurst LLP, Ashurst Australia and their respective affiliates (including independent local partnerships, companies or other entities) which are authorised to use the name “Ashurst” or describe themselves as being affiliated with Ashurst. Some members of the Ashurst Group are limited liability entities.

Ashurst LLP is a limited liability partnership registered in England and Wales under number OC330252. It is a law firm authorised and regulated by the Solicitors Regulation Authority of England and Wales (SRA) under number 468653. The term “partner” in relation to Ashurst LLP is used to refer to a member of Ashurst LLP or to an employee or consultant with equivalent standing and qualifications.

Ashurst Risk Advisory LLP is a limited liability partnership registered in England and Wales under number OC442883. It provides services under the Ashurst Risk Advisory brand. Such services do not constitute legal services or legal advice and are not provided by qualified legal practitioners acting in that capacity. Ashurst Risk Advisory is not regulated by the SRA or any other regulator of legal services in other jurisdictions. The term “partner” in relation to Ashurst Risk Advisory is used to refer to a member of Ashurst Risk Advisory or to an employee or consultant with equivalent standing and qualifications.

For more information about the Ashurst Group and the services offered, please visit www.ashurst.com.

This material is current as at November 2022 but does not take into account any developments after that date. It is not intended to be a comprehensive review of all developments in practice, or to cover all aspects of those referred to, and does not constitute professional advice. The information provided is general in nature, and does not take into account and is not intended to apply to any specific issues or circumstances. Readers should take independent advice. No part of this publication may be reproduced by any process without prior written permission from Ashurst LLP and Ashurst Risk Advisory LLP. While we use reasonable skill and care in the preparation of this material, we accept no liability for use of and reliance upon it by any person.

ashurst.com