Ashurst Risk Advisory

Risk in Real Life

Challenges facing General Counsel in Australia

Outpacing change

Foreword

With the constant barrage of change affecting businesses, the role of General Counsel has evolved into one that needs to deal with profound complexity across new and emerging risks. The responsibility of managing these challenges has become increasingly formidable, and can leave even seasoned professionals feeling overwhelmed.

It is understandable to feel daunted by the responsibility of being across all the right expertise at all times.

Our report aims to help you, your Executive and Board to be on the front foot for what is unfolding – and to take time to fully consider how to tap into the right expertise at the right time.

Not surprisingly, we are finding more of our clients raising their hand to say "I can't do this alone." In response to escalating complexity of changes, more in-house legal teams are acknowledging the impracticality of solely handling all areas of expertise in-house. Instead, they are looking to outside advisers to fill specific new skills gaps.

Managing all risk categories in-house is no longer feasible, and embracing external support offers a practical solution to the escalating demands of risk governance. That said, good planning is needed to understand where to invest in long-term capability in-house that is deep on expertise. This frees up the decision making on when, and where, to seek external support.

Our mission is simple: to equip you with the capabilities and expertise you need to excel in your role and protect your organisation. This means highlighting uncomfortable truths about the ability to have enough of the right expertise at the right time.

We equip in-house legal teams with the strategies you need to address risk appropriately, by helping you understand the legal requirements, and then together we design, implement, and embed effective risk management strategies, including using technology, to help legal teams to drive better collaboration on risk practices across organisations.

In this 2023 Australian General Counsel Risk Survey, you will find insights and strategies to navigate the intricacies of risk accountability, and understand better how others are closing the gap between vital but scarce skills and managing organisational risk.

Together, we can confront these challenges to create a stronger and more collaborative risk posture that is well-prepared to safeguard your organisation.

Philip Hardy
Partner, Head of Risk Advisory
Australia
T +61 3 9679 3155
M +61 411 104 250
philip.hardy@ashurst.com

Executive summary

Managing risk is becoming even more complex thanks to global economic and civil destabilisation; climate change, rapidly evolving digitalisation, cyber threats, and emboldened stakeholder groups.

To just keep up with the pace of change requires highly specialised expertise and skills that are in strong demand and still emerging; and therefore do not exist within many in-house teams.

Managing risk across an organisation is made even more difficult by structural barriers. Risk and Compliance functions don't often report to the General Counsel.

General Counsel must navigate complex internal structures and politics just to be able to influence "how" company-wide risk management is designed and executed.

We surveyed Australian legal teams across the country about their risk posture. We found organisations face formidable challenges:

- All of our respondents are struggling to keep up with the pace of change
- All feel significantly exposed in one or more areas of risk
- All have indicated that to some extent, they do not have the skills in house to cover all risk areas and acknowledge that it is impossible to hold all the skills in-house
- Many are seeking external support for new and emerging expertise areas to close the skills gap.

Our survey highlights the most critical areas of risk that organisations need to address.

Here are 5 questions to ask your legal advisers to ensure you are covered in the new and emerging areas of risk:

1. ESG

What are the potential legal risks associated with ESG related claims disclosures, and how can I ensure we are not making misleading statements about the company's ESG initiatives? What should I do if we are accused of "greenwashing?"

2. Cyber

What are the legal implications of a data breach, and how can the legal team assess and improve our cyber security posture, incident response and breach recovery efforts? To what extent is our Board and Executive team truly "resilience ready" and what can we do to address gaps?

3. Psychosocial risk

What are the legal obligations regarding psychosocial risk in the workplace, and how can we identify, assess and mitigate psychosocial risks within the organisation?

4. Digitisation and data governance

How can we best establish robust data governance frameworks in the context of a more digitised corporate infrastructure? What are the legal considerations when adopting new technologies that process or analyse data? What are the implications of current and likely reforms?

5. Financial crime

Are our risk assessment methodologies robust enough with respect to financial crime, and what are the specific risks an organisation like ours should consider?

Our findings reveal there is often a gap between legal application and operational practice. Legal leaders need to have a clear understanding of critical risk domains that can be managed in-house, and those that require external expertise. But across all of these risks, legal teams need to be able to work with their Risk and Compliance teams to apply the law and manage risk in their organisations.

This report highlights "risk in real life" scenarios to help bring to life some of the challenges faced by legal and risk teams as they collaborate to protect organisations. They are designed to show how a fully connected legal and operational response is the best way to manage these emerging risks.

Key Findings

Insight #1

Across the board, legal teams are under pressure to respond to rising instances of risk

Our research revealed that legal teams across Australia are under the pump, with 65% of respondents saying that their teams were either working “flat out” just to keep up, or falling behind due to increasing workload and demands for specialist knowledge.

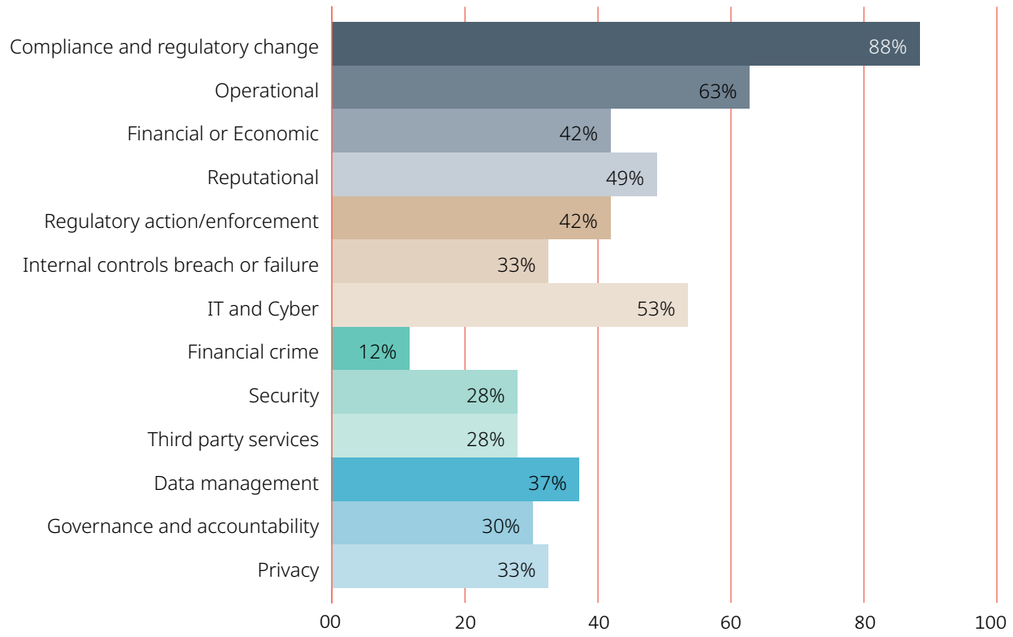
Coupled with this, across 13 broad categories of risk surveyed (see Fig. 1), there was not a single category of risk that professionals are not concerned about, with key areas of concern being:

- Compliance and regulatory change
- IT inadequacies / vulnerabilities
- Cyber threats

This concern is based on mounting levels of risk incidents within their business. At least 1 in every 3 companies who responded had experienced risk in an astounding 10 of these 13 categories, with significant negative consequences. More than 1 in 4 legal professionals reported that these risk incidents damaged their company’s reputation, brand value or revenue.

Approximately 20% of those surveyed reported that the risk incidents impacted the company’s clients and just under this number reported that the company’s value or market cap was affected.

Fig. 1: Percentage of companies who have experienced risk incidents in Australia across 13 key risk categories over the past 12 months.



Risk in real life

The rising complexity and impact of risk

Our findings clearly demonstrate the rising complexity and interdependencies between distinct aspects of risk. Data security and protection, for example, is often managed through third party services or in-house IT and cyber teams, requiring a peripheral approach to risk management that considers everything else that influences a particular risk outcome.

Yet, data security is more than just one component of the technology risk and control environment. It relates to regulatory compliance (i.e. privacy compliance), customer perceptions of brand and trust, as well as other legal issues such as appropriate data collection and use requirements.

There is no single risk owner for data risks, but the complexity of organisations can make it difficult to ascertain the aggregate risk and control environment.

Risks such as these need a ‘whole of organisation’ approach that considers legal, regulatory, people, operational, reputational, and financial implications through the risk lifecycles. Governance of these risks should drive this behaviour and clarify accountability so that risk issues do not ‘fall through the cracks’.

Insight #2

Legal teams often feel disempowered and face significant organisational barriers in terms of their ability to manage company-wide risk

Our research also uncovered that despite their heightened awareness around risk, legal teams feel they do not have adequate information, and therefore insight, to effectively manage it.

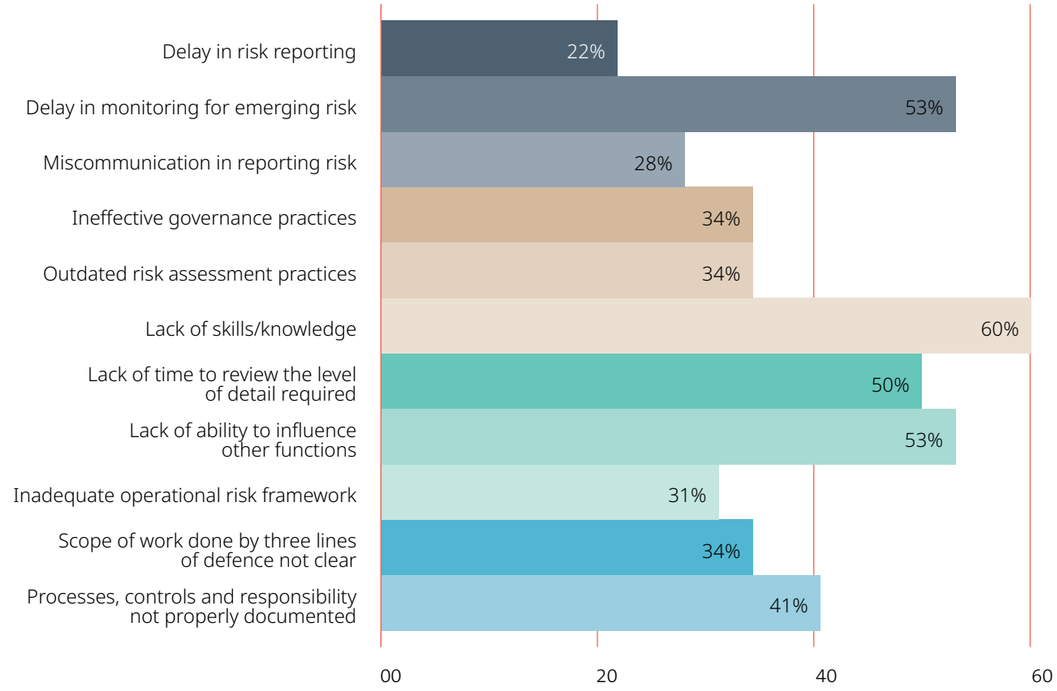
Over half of in-house legal professionals feel there is not enough transparency within their company for effective risk management. Almost 60% feel management information within their company is inadequate and does not objectively provide a view of risk.

Over half of companies surveyed felt that significant barriers to managing risk include a delay in monitoring for emerging risk, a lack of skills / knowledge, a lack of time to review the level of detail required, and a lack of ability to influence other functions (see Fig. 2).

Legal teams were also concerned around having to rely on other teams and bearing responsibility for things that are outside of their control. 56% admitted they feel exposed by responsibilities they must delegate across other functions.

Surprisingly, only 44% feel the legal team is consulted on their company's operational resilience and financial resilience plans, testing approach and conclusions and in roughly 1 out of 5 instances, the legal team is not consulted when an incident occurs.

Fig. 2: Percentage of companies who have experienced key barriers to managing risk in Australia.



Risk in real life

The widening void between legal application and operational practice

Our findings reveal there is often a large divide between 'legal application' and 'operational practice.' Legal teams often understand 'what' should happen to mitigate and manage risk in certain areas, but in reality, those areas are outside of their direct control.

Similarly, organisations face an elevated WHS risk due to the very public rise and safety regulatory focus of 'psychosocial risk' and increased safety action owing to a workforce that is more informed and empowered than ever before. But psychosocial hazards are most often owned by HR teams who are at the front line of responding to the outcomes. Examples of these hazards include bullying, sexual harassment, work demands and lack of control.

As such, legal teams often feel they have little control over WHS risk outcomes.

Insight #3

Gaps in in-house skills to manage key areas of concern and actual risk mitigation is lower than desired

Legal professionals today face a growing number of risks that did not exist a few years ago. New areas of risk are proliferating as the pace of digital growth accelerates and ways of working change. Across the board, there are significant gaps in terms of the in-house skills to manage risk. In 10 key areas of risk (see Fig. 3), there were only 4 areas in which over half of all in-house teams identified that they had expertise.

Fig. 3: Areas in which companies in Australia have in-house expertise as a percentage.

Across 10 key areas of risk (see Fig. 4), there were areas in which almost all legal professionals admitted to managing risks either reactively or not at all. We uncovered that only 1 in 3 legal professionals feel they are keeping up with their workload and have capacity to be proactive on issues.

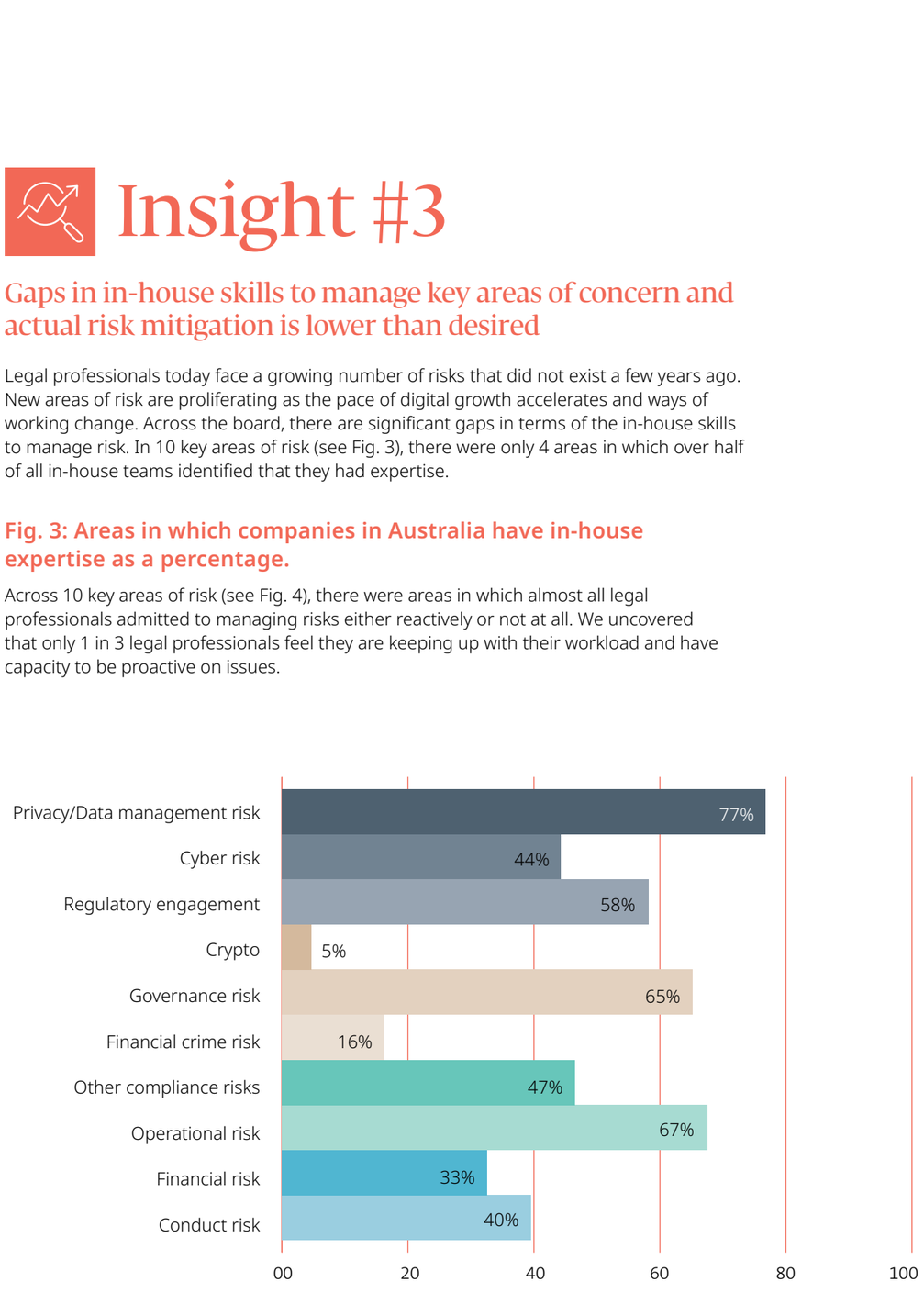
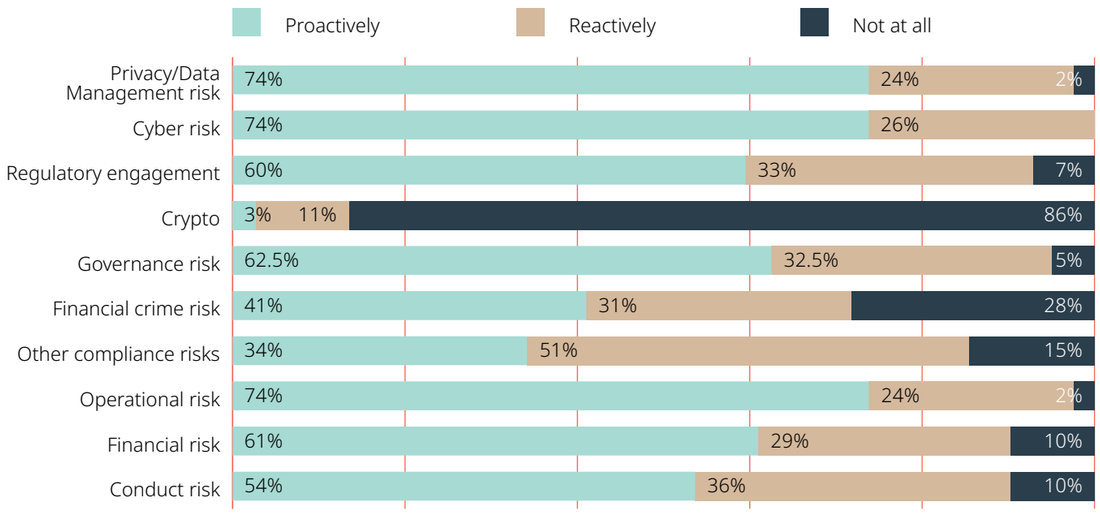


Fig. 4: How companies are managing risk across 10 key areas in Australia.



The need for supplementary expertise in emerging areas of risk

Financial crime, cyber risk and cryptocurrency are key areas of emerging concern when it comes to risk. Yet, expertise is not keeping pace with the requirements for specialist knowledge around managing these risks.

- Only 2 out of 5 companies reported that they have in-house skills in mitigating cyber-attack response, while 2 out of 5 reported having no in-house skills in mitigating cyber risks. An overwhelming number of companies reported that they are not adequately prepared for cyber risk or attacks, with almost 40% admitting they are not comfortable with their company's defences against cyber risk.
- Over 60% of teams have concerns about their company's ability to keep up with the evolving and sophisticated methods of financial crime. What is more, over 45% of in-house legal teams feel financial crime is not prioritised as a significant risk within their company, although 41% of professionals are concerned about it.
- Approximately 40% of legal professionals felt that conduct risk expertise was available within their teams, at a time of heightened scrutiny by regulators.
- Almost a third of professionals feel Australia's legislative framework is insufficient with respect to crypto, while almost half feel that financial crime risk and fraud is continually evolving and becoming more sophisticated in respect to crypto.

Risk in real life

The knowledge gap – capability gaps for risk and the significant legal implications

With Australia being targeted by cyber criminals, organisations are seeking to rapidly uplift capability. However, despite the significant legal issues attached to cybercrime, such as mandatory notifications, the legality of ransom payments, the legal obligation to protect personal data, and customer remediation, less than half of legal teams felt they had the requisite in-house expertise.

In-house legal teams will need to ensure cyber response plans are integrated across all parts of their organisation, proactively upskill their teams and retain specialist advisers to ensure sufficient expertise is at hand for the organisation to access in case of an attack.

Insight #4

Legal teams are reaching out for help

Today, in-house legal teams are becoming more reliant on outside expertise to manage an increasingly complex business landscape and are utilising external experts on specific subject matter areas that were once more niche, but are becoming mainstream such as regulatory convergence, reform, co-opetition globally and digitisation.

- Less than 2% of legal teams do all their Australian legal work in-house, with 60% of participants outsourcing 20% or more of this work.
- Almost 1 in 5 legal professionals outsource 30% of their work, while over 80% of participants expect this amount of outsourcing to either stay the same or increase over the next year.

The key areas in which legal teams require outside / outsourced help and insights include:

- **Regulatory convergence, reform, and co-opetition globally:** Teams are seeking help with regulatory engagement (43%), governance risk (26%) and compliance risk (23%).
- **Digitisation:** Teams are seeking help with privacy and data management risk (43%), and cyber risk (31%).
- **Shifts in how teams organise themselves to work:** Teams are seeking help with new business initiatives (35%), third party contracts (33%) or client contacts (25%), and disputes (69%).

Risk in real life

Getting the balance right between in-house and external expertise

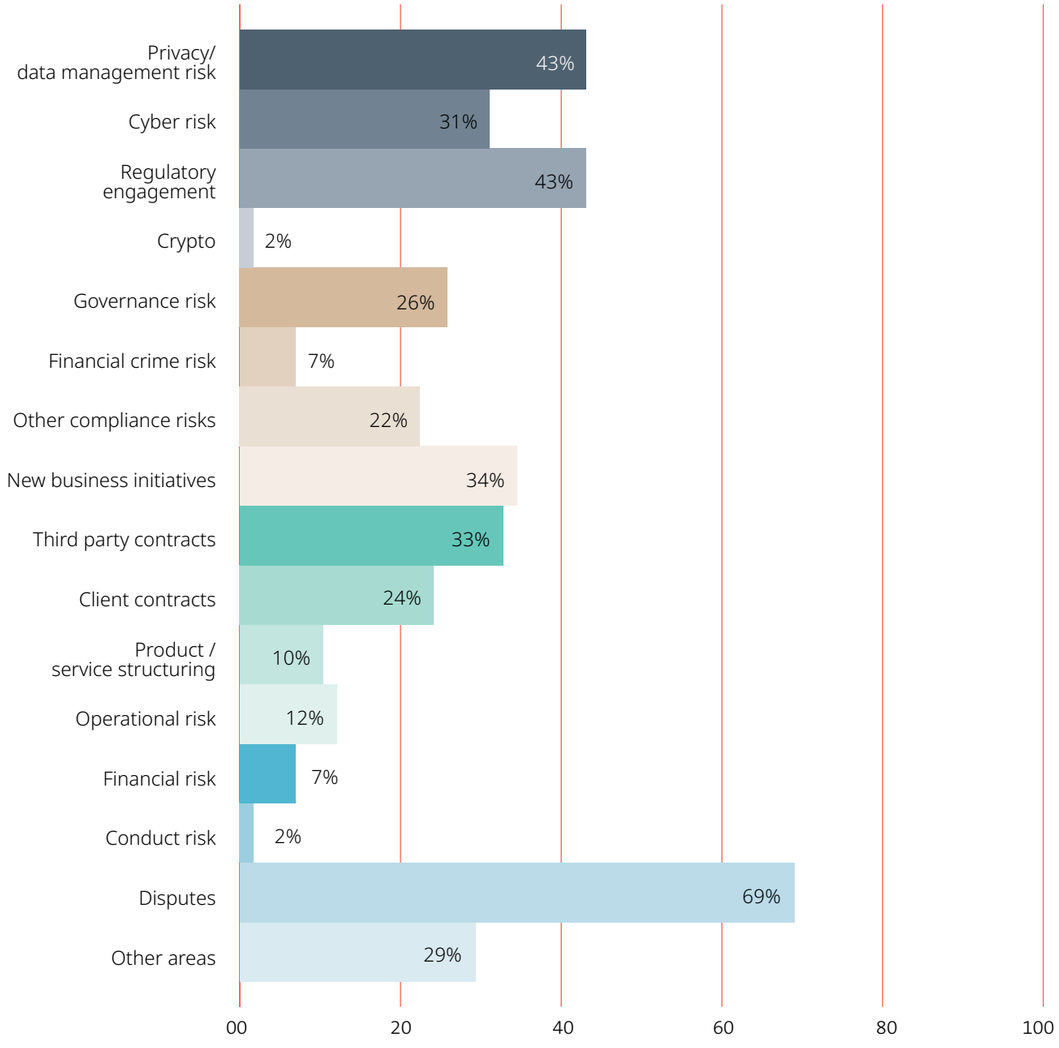
Legal teams cannot necessarily be expected to house all required expertise internally – the cost and oversight for niche areas would likely be prohibitive.

Instead, legal leaders should identify critical risk domains in which small teams can develop and grow their expertise. This will enable maximum value for the investment and empower teams to draw on external support for other areas.

ESG litigation is a critical risk. The current landscape of climate change and net zero related regulations, frameworks, standards and guidelines is complex. To address this complexity the operationalisation of commitments, transparent and rigorously demonstrated progress, measurement and validation should underpin disclosures.

Legal teams will need a core team of experts who understand the risk of ESG litigation in their disclosures and public commitments. However, they will need to supplement this with external expertise in implementing strategic ESG risk management approaches to navigate the complexities of ESG disclosure-related disputes and litigation.

Fig. 5: Areas in which teams expect to have Australian legal support outsourced over the next 12 months.



Conclusion

Mind the gap

The insights from our survey have practical implications for legal teams wanting to move from ‘awareness’ and ‘worry’ around risk, to overcoming the challenges that inhibit their ability to assist their organisations from actively managing it. This needs to be done in collaboration with other teams and with the understanding that ultimate responsibility lies at an executive level.

Owning the disconnect between responsibility and oversight

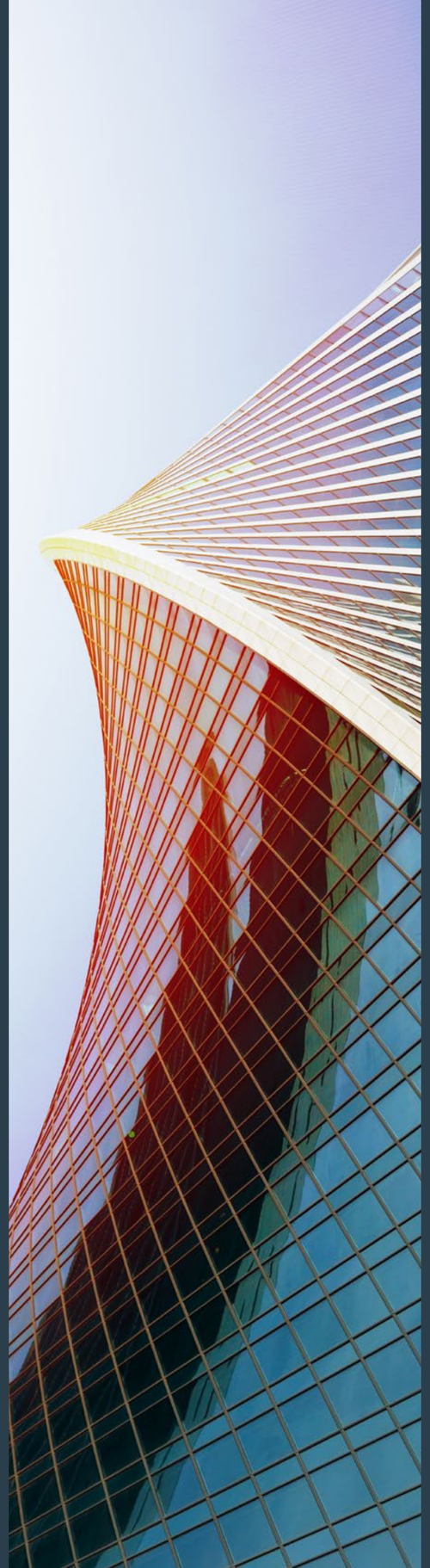
In-house legal teams often bear a large amount of responsibility when it comes to organisational risk, although the view that these teams are responsible for all risk is dangerous when we consider that quite often, function-specific risk is outside their immediate areas of expertise or remit.

Although they are often ‘accountable’ for mitigation, their ability to influence the operational functions responsible for risk management processes on a daily basis is low. These functions are not accountable to them, and as such, legal teams often feel less empowered than they need to be to influence risk management outcomes.

Bridging the gap

Organisations need to bridge the divide between legal teams and the implementation of risk management processes and procedures. This requires a range of changes, including:

- Clarifying expectations for risk owners to consult with legal experts
- Developing risk reporting to Executive Teams and Boards that specifically incorporates legal perspectives into the analysis of risk events relative to risk appetite
- Providing forums for legal experts to contribute to risk assessments, and the development of mitigants and controls
- Identifying barriers to effective collaboration and putting in place safeguards that ensure all voices are considered when developing risk mitigants.



Getting ahead of even more change

In the coming years, we see that there will be meaningful change – competitively, operationally, and legally. We believe the most prepared legal teams will benefit from early investment in the following areas:

Cyber incidents

Lifting crisis resilience, particularly at the Executive Team and Board levels, and increasing the speed and capacity to recover is critical for competitive advantage and operational resilience.

Regulatory change

Forthcoming major data and privacy reform will stress availability of appropriate talent, but failure to properly implement effective compliance arrangements will be costly both reputationally and legally. Teams that move early and take a ‘whole of customer’ approach will be much better prepared.

Data risk management

At the core of the above areas, will be the need for effective end-to-end data risk management arrangements. This requires a range of risk and legal owners to work together to ensure embedded data risks are properly scenario tested and effective mitigation strategies developed.

Regulatory intensity

Almost all regulatory litigation cases in the past two years have focused on allegations of failures in risk and compliance arrangements. Now more than ever, risk and legal leaders need to work together to ensure the suitability of these arrangements in an environment of more litigious regulators.

Third party risks

Properly assessing all risks in third (and fourth party) arrangements and developing internal mitigants that go beyond traditional contractual risk allocation is essential. This means assessing vendor arrangements across the lifecycle, properly assessing risks of failures by third (and fourth parties) and ensuring there are appropriate monitoring and governance arrangements in place.

ESG litigation risks

ESG litigation risks are centred on disclosures – both in terms of accuracy and capacity to execute against public commitments. Organisations need to properly risk assess all their public disclosures and ensure robust systems are in place to achieve them.

Workplace risks

The alarming increase in psychosocial risk factors in workplace arrangements requires a more fulsome risk assessment and accompanying set of mitigants. This will mean properly understanding modern psychosocial risk factors, assessing the sources and impacts of these risks and then modernising safety systems to ensure these are properly managed.

Ashurst Risk Advisory