Deloitte.
Legal

Legal Risk Management

A heightened focus for the General Counsel

Contents

Foreword	3
What is legal risk?	5
Accountability	6
Assess and control	8
Monitor and report	11
Technology	12
Interaction with regulators	14
In time...	15
Contact	17

Foreword

Companies, their boards and General Counsels (GCs) face a constantly evolving landscape with exposure to financial and reputational losses if legal risks develop. This has created an expectation that in-house Legal teams will do more to identify, manage and mitigate the legal risks in their organizations. In the financial services sector, there is increased regulatory interest, particularly looking at how Legal fits into the wider organizational risk framework. These combined pressures are causing organizations to identify and manage more effectively the overlaps and gaps between Legal and the business (including other functions).

GCs are re-evaluating their operating models as discussed in our paper 'Optimizing your organization's in-house legal operating model.' In-house Legal teams are also making greater use of technology, both enterprise-wide systems and legal-specific ones, which we explored in 'What's Your Problem? Legal Technology.' As the Legal function transforms, so does the way in which it contributes to the organization's risk management, playing a greater and more proactive role than has historically been the case. This has resulted in more explicit consideration of what constitutes legal risk, how it should be managed and by who.

This point of view looks at the key considerations in approaching legal risk management and examines the steps being taken in getting to grips with legal risk management. As part of our research, we surveyed a large number of businesses in multiple sectors to compare and contrast their relative maturity levels*, and provide our view of what the future holds in relation to the management of legal risk.

Luis Fernando Guerra
Global Leader, Deloitte Legal

* See page 18 for more information about our survey and methodology.

Legal Risk Management

What is legal risk?

Mind-set change

Legal risk management as a discipline is a relatively new way of thinking for many in-house legal teams. The growing expectation in the financial services industry from other departments and regulators is that Legal gets explicitly involved in formal risk management processes. When defining legal risk – which has been framed as reputational impact, operating or financial losses and issues affecting the organization's ability to do business – it is clear that Legal needs to do more than the "day job" to identify, manage and mitigate legal risks.

A narrow or broad definition?

Some organizations apply a narrow definition in which legal risks are solely those arising from Legal's operations such as resourcing decisions (in-house provision versus use of law firms), the quality of the advice provided by Legal and the conduct of its lawyers. Such a definition fails to take account of the many other risks that an organization faces which have a legal component, for example financial crime, conduct and legal risks arising from an organization's operations ranging from contractual to intellectual property disputes. The underlying activities may be owned by other parts of the business. Yet to deny some Legal function responsibility for managing the legal risk inherent in those activities doesn't make sense and could result in responsibilities falling through the gap between Legal and the business. Hence, many organizations apply a broad definition of legal risk which encompasses any risk faced by the business which has a legal component. Surprisingly, our surveys found that there are still a number of organizations—41% of non-banking and 14% of banking respondents—with no definition of legal risk. Where a definition was in place, this still varied widely in definition and focus, reflecting the lack of a legal industry standard definition for legal risk.

A separate risk

In the past, GCs and organizations have often not considered legal risk as a category in its own right and it has been subsumed within other risks rather than being explicitly identified in risk management frameworks managed by Operational Risk, Compliance or Internal Audit. This may have been the case for financial services because Basel II defined legal risk as being a part of operational risk. Another reason for this lack of identification of legal risk in its own right could be because of its comparative lower profile when compared to other risks arising from financial crime, conduct and duty of care, IT and cyber security which can have a much larger impact on the viability or capital adequacy of an organization. However, the level of fines for many businesses over recent years has driven significant changes in the profile of legal risk in those organizations and peer group companies.

Of more importance than definition is identifying the risks, legal and otherwise, that the organization faces and establishing an effective framework for their management so that responsibility can be allocated between Legal, other functional areas and the business.

At Deloitte, we have developed a legal risk taxonomy to help both in-house Legal functions and those responsible for the organization's risk management system to better understand the legal risk landscape. The key risk areas we have identified encompass both narrow components owned by the Legal function; and broad ones – such as contractual, intellectual property, legislative changes and legal advice into other risk areas such as financial crime, conduct, employment and technology. It is clear from this that understanding legal risk is as much about understanding the organization's rights and obligations as it is about understanding the letter of the law.

Surprisingly, our surveys found that there are still a number of organizations—41% of non-banking and 14% of banking respondents—with no definition of legal risk.

Accountability

On a narrow definition of legal risk, it is clear that the GC and the Legal function are accountable for identifying and managing those risks which arise from Legal's operations. In the three lines of defense model, a commonly used risk management framework across the survey participants (70%), the Legal function is the first line and others (typically Risk and Compliance) need to fill a second line role in relation to these risks.

However, the consensus is that a broader definition of legal risk should get more focus from the Legal function. Every operation and function of an organization runs risks which need to be controlled or avoided. Many of those risks have a legal component. Legal needs to work across the organization to identify those legal risks, set the appetite for each risk and agree the roles and responsibilities for legal risk management including accountability and the controls or other mitigation measures to implement. GCs and risk specialists will need to collaborate to develop an effective framework that captures the multitude of legal risks that exist in organizations and design controls to mitigate the most critical.

Who owns the risk?

Ownership of risk will be determined by the structure of the organization and where the expertise sits to manage it. On a broader definition, business management own legal risk (including the GC in respect of legal operational risk) and Legal and other functions provide support and advice. Where business functions have first line responsibility for legal risk management, Legal's role is to establish policies, raise awareness, advise and monitor the effectiveness of controls and mitigations. Legal needs to educate business management so that they are better able to manage legal risk – what to do, what not to do and the implications if specific legal risks are not properly managed.

Global implications

In multinational corporations, there is a significant coordination and horizon-scanning role for Legal. Across the organization's geographical footprint, Legal needs to understand the legal risks arising in each country and how some risks may cross borders, potentially creating a double or multiple exposure if the risk materialises. Understanding the consequences of a breach for the organization, its directors or individual employees is essential in determining the risk appetite and the efforts which should be deployed in managing or avoiding the risk. Where significant penalties are involved, such as for failures in relation to the GDPR, or criminal sanctions, as can be the case where corrupt practices are uncovered, Legal will need to work with other specialists and in-country teams to raise awareness of the corporate and individual consequences of particular risks crystallizing. For some groups, this has involved shutting down operations in certain jurisdictions or not trading with them, managing the risk by avoiding it.

Independence

It is accepted that the GC and the Legal function need to maintain a degree of independence from the organization they serve to maintain their objectivity in providing advice. Where Legal is filling a first line of defense risk management role, a robust second line would ideally be in place to avoid the potential (real or perception) that Legal's objectivity is compromised. This is best achieved when those acting as the second line sit outside the Legal function. However, this is when problems emerge as it is difficult for non-lawyers to check the work of the Legal function. This is discussed further in the section entitled "Monitoring".

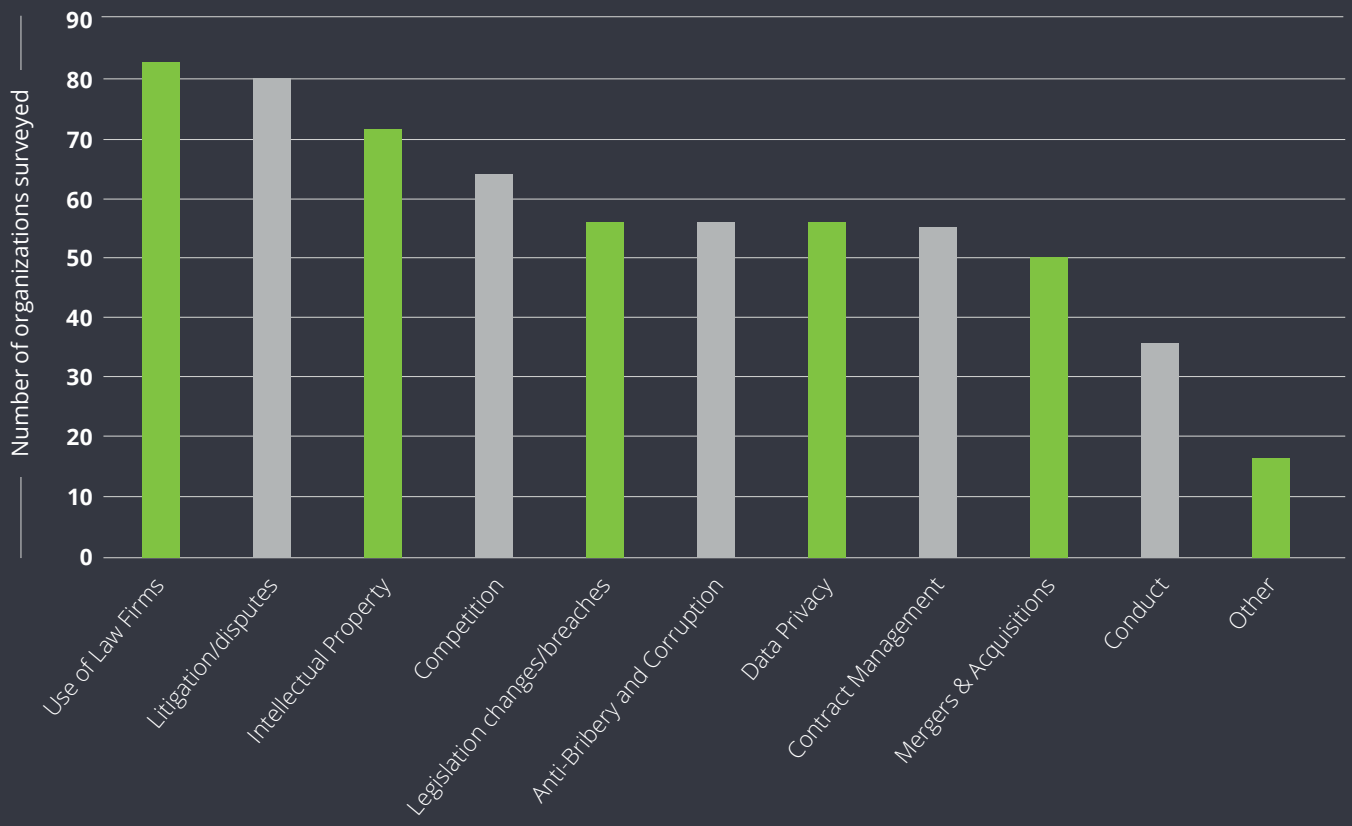
Policy ownership

Policies are a common approach to driving clear accountability for management of risks across an organization. Many Legal functions have policies concerning their use of law firms/other third parties, for when a mandatory referral to the Legal function is required and some will have policies for specialist areas.

The survey results illustrate Legal is not usually accountable for all areas that give rise to legal risk; for example, Conduct and Anti-bribery will often sit under Compliance. This highlights the importance of clear accountability and agreed roles and responsibilities between Legal, other functional areas and the business to ensure that legal risk does not "fall between the cracks".

In the three lines of defense model, a commonly used risk management framework across the survey participants (70%), the Legal function will most often play a combination of a first and second line role depending on the activities

Key policy areas owned by the Legal function*



* See page 18 for more information about our survey and methodology.

Assess and control

Having established the more prevalent broad definition of legal risk, risk management responsibilities will be owned both within the Legal function and by the business, how does the GC understand the level of legal risk across their organization? What structure and skills need to be in place to achieve effective management of legal risk? This will depend on a variety of factors, including the industry in which the organization operates and the level of regulation to which it is subject, whether the organization is centralized or decentralized and its strategy in areas such as intellectual property development or growth through acquisition.

Assessing legal risk

An assessment of legal risk exposure across an organization should be undertaken for each area of legal risk. This can be a highly subjective exercise, however, we find that using a common framework of risk factors such as regulatory, customer, financial and reputational implications, historical loss data (where available) and considering different risk event scenarios provide structure to this process. With operational risk's support, Legal is able to leverage the organization's experience and 'lift and shift' concepts from other risk functions, with words and methodology tailored to the types of risk identified.

Risk appetite

In addition to defining what is meant by legal risk, some organizations (38% of the respondents in our survey) have in place/are developing a legal risk appetite statement. This should not be a blanket approach, applying one appetite level to all risks. Instead it should be more nuanced with differing appetites depending on the type of risk involved and potentially the different jurisdictions and operating entities in which the risks arise.

Clearly, all organizations will want to identify any significant risks and some will decide to eliminate them. For example, the legal risks associated with a particular product launch may be so high as to result in the launch being terminated. Other risks may be transferred, for example, by the use of insurance.

Some risks may be tolerated and dealt with reactively if they arise. Other risks may be managed or treated proactively either to mitigate the risk of them occurring or to operate measures to manage them within certain tolerances.

Control

Once legal risks, risk owners and risk appetite are identified, the organization can set about considering the level of control to put in place to manage different legal risks. Controls will vary from risk to risk. Where legal risks are low, the risk may be tolerated where the Legal team deals with issues as they occur with minimal investment in controls. An example of this: a consumer business with low intellectual property risk that decides to manage intellectual property issues only when they arise. For higher legal risk such as competition risk, more resource and investment in control could be appropriate to proactively bring the risk within risk appetite. For example, this could require policy setting, comprehensive training programs across the organization and more active review and involvement from lawyers embedded in business processes to address competition risks proactively.

Controls to address legal risk may be owned and operated outside the Legal function, however, they are an important part of the legal risk management framework. An example is the use of contract templates to manage contractual risk, with responsibility for using and complying with these templates the responsibility of business teams, not Legal. Legal still needs to consider whether the controls in place are managing the contractual risk to an acceptable level for the organization and whether more, or conversely less, control is required. Where contract risk is owned by the business, controls may require that any contract over a certain value is reviewed by the Legal function. Moreover, what checks are in place to make sure this happens? If referred to Legal, is their review checked by another lawyer, or is the organization happy that someone outside of Legal just checks that the review has occurred? All of these steps form part of the legal risk management framework which the organization establishes, based on mapped processes and implemented controls.

Strategy and operating model implications

Assessment of legal risk and where legal resource should be invested and focused should be a key driver in deciding the strategy and legal operating model for an organization. Which activities Legal will continue to own and which will be managed elsewhere, the nature of legal expertise required, the balance of in-house resource and external counsel and the use of technology are all decisions that should be influenced by the legal risk profile of an organization.

Work with experts

Legal should not be expected to do it alone when developing a more mature approach to legal risk management. It is essential that organizations adopt a multidisciplinary approach which leverages the skills of the Legal Chief Operating Officer (if they have one), legal project management specialists, risk experts who are able to advise on the best controls and mitigations on a risk-by-risk basis and technologists to advise on the best technology to use for legal risk management purposes. These risk and technology specialists can also help Legal to identify new risks in new technologies which the organization is either selling or purchasing. Across the respondents to our surveys, legal risks are generally managed using the organization's own company-wide, operational risk system. Fewer than 10% of respondents to both our surveys use a legal specific risk management system.

Some organizations see the discipline of legal risk management as a key area of expertise for future leaders of the Legal function. In others, responsibility for managing legal risk is rotated around different lawyers in the team to further build expertise and develop career paths. We discuss this further in the section "Monitoring".

Three lines of defense

Many organizations—two thirds of non-banking respondents and all apart from one of the banks we surveyed—apply the three lines of defense model in the management of legal risk. Unsurprisingly, given that a broad definition of legal risks dominates, Legal often operates in a mix of first line and second line risk management roles. The most important consideration is to make sure the legal risks are comprehensively managed and ensuring that Legal maintains its independence and doesn't "mark its own homework" by filling first and second line roles in relation to the same risk. The three lines of defense model can also be a useful framework to define what monitoring requirements should be put in place to manage legal risk.

Awareness raising

Legal's advisory function is critically important to helping other parts of the organization to understand the legal risks involved in their activities, mitigating risk through awareness raising rather than leaving non-legal colleagues to manage legal risks or to apply controls by rote without understanding the risk which the control is designed to mitigate. This upskilling can be achieved without making everyone in the organization a legal expert. In the same way, risk and technology specialists can raise awareness within Legal of best practice approaches to risk management and help Legal to understand new technologies. That way, legal risks inherent in them can be identified and managed.

Monitor and report

The measurement challenge

Legal risk is often seen as hard to track, measure and report. This is either because it is absorbed into primary operational risks or the risk is qualitative rather than quantitative. Even where a risk develops, such as litigation, this would result in a financial loss, putting a number on that exposure involves a number of variables including the often subjective likelihood of success or failure, the potential costs incurred by both parties in getting to a resolution, the degree to which the defendent is responsible for the claimant's costs, the extent to which any losses are addressed by insurance cover and what happens in court on the day. Where the exposure relates to reputational loss, it is harder to measure.

Monitoring

With the legal risk framework in place, a monitoring and reporting regime can be established covering both the effectiveness of the legal risk management framework and flagging emerging exposures and the remediation of failures.

The most effective monitoring uses technology to supervise risks and controls, however, this is currently more widespread for operational risk management than for legal risk. In the contract arena, a contract management technology solution can provide ongoing monitoring of variations from key contract clauses across an organization to determine the level of legal risk being carried across a contract population. Whether monitoring and reporting is enabled by technology or not, Legal needs to understand what it wants to monitor upfront.

In multinational organizations, monitoring works best when it happens close to, yet independent of, the business. That way, those undertaking the monitoring have the best understanding of the local context and can react immediately in a more appropriate and nuanced way. By contrast, where monitoring happens from the center this can result in time delays, missing what is important or focusing on non-issues. That said, there are also benefits to centralization which include ensuring standardized and consistent advice across the organization or to reflect high levels of risk and sensitivity in areas such as competition.

Reviewing whether lawyers' responsibilities have been discharged effectively is a difficult area to monitor. Where there is more of a standardized process with clear stages and control points such as contract drafting and negotiation, it is possible to introduce more typical controls testing and assurance activity. This is much more difficult where legal professional judgement is being applied. Approaches from other professions, such as auditing, that are being used in some Legal functions are peer review within a legal team, as well assurance teams made up of lawyers to provide independent review of lawyers' work.

Assurance principles from other organizational areas are also being applied to legal risk by taking a risk-based approach to monitoring and assurance activities focusing effort on the areas of highest legal risk. Development of controls testing and assurance programmes is an example of this which is becoming more common place. This involves reviewing the design adequacy of key controls to address legal risk, and where proportionate, also testing the operating effectiveness through risk-based sample testing.

Reporting

The fruits of this legal risk management should be regularly reported to risk or audit committees and the board. The Legal function should also have an appropriate escalation route for urgent risk matters. In many organizations today, this may consist largely of reporting litigation risks and open cases to the audit committee throughout the year. In a more mature legal risk management environment, all the other categories of legal risk such as contractual, intellectual property, competition or anti-trust, data privacy, legislation and operational risks, will be monitored and reported where appropriate.

The most effective reporting frameworks will include key risk indicators (KRIs) as automatic reporting triggers to reduce reliance on subjective decisions by risk and control owners as to what they report. In our surveys, the majority of respondents have some sort of reporting and a subset of those use KRIs. However, the best monitoring and reporting relies on high quality data to drive risk management metrics and many organizations continue to struggle with where this data is held and how to get access to it and to report on it real-time. Again, Legal should draw on the experience of risk and technology specialists to assist in getting hold of this data and interpreting and presenting it in a way which helps both risk owners and those charged with governance to understand its implications.

Technology

The use of technology to enable better management of legal risk is a developing area. In our survey, the most common use of technology was organization-wide operational risk systems to help identify, assess and report on legal risk and control across the organization. However, outside of this, there was very little use of technology to manage legal risk. As technology matures in the legal sector, this is an area we anticipate will evolve significantly.

A changing skills mix

As legal risk management moves up the corporate agenda and Legal functions refine their operating models, technology is receiving increased focus. This is reflected in the recruitment by some of the technologists and data scientists, and the use of technology to automate some tasks and provide insightful reporting. Legal's needs are likely to be met through a combination of risk management-specific tooling and the incorporation of legal risk parameters into other technologies. For example, contract management technology could analyze contracts to identify higher risk clauses or include prohibitory controls which reflect the organization's legal risk appetite to prevent the execution of a contract which falls outside the appetite. An organization might have certain categories of assets that it was prepared to accept or pledge as collateral for a contract. If the operations department attempted to complete a contract with unacceptable collateral, the system would reject the contract.

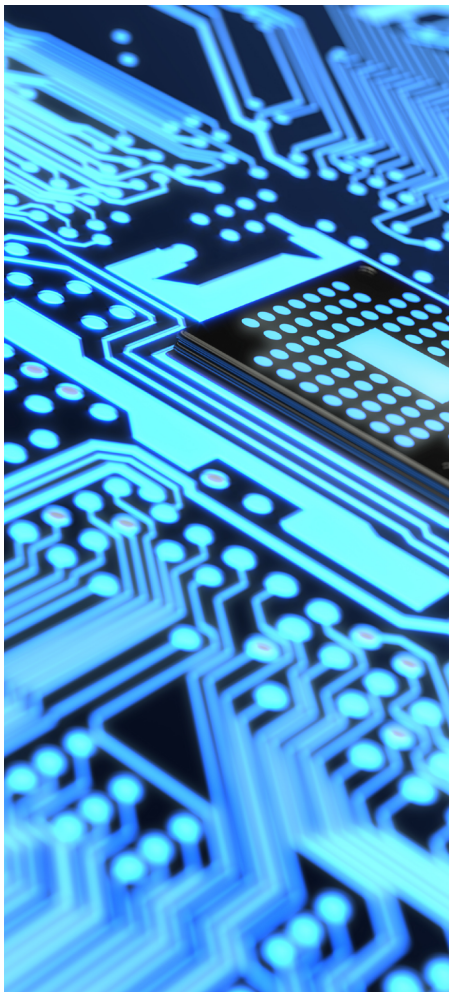
Quality data

Technology can also support monitoring and reporting by enabling an auditable environment, allowing access to data and improving reaction times for both proactively mitigating legal risks and effectively managing those legal risks which have crystallized. Resource allocation technology allows Legal to profile its workload and make sure it is focused on the right things. For example, tooling could help to identify the number of incidents across the organization in relation to specific risks so that effort can be directed to monitoring and potentially identifying the root causes of areas of heightened legal risk. In this way, technology increases risk oversight and control providing Legal with greater visibility across an organization. It provides increased coverage of business activities than would be possible through a purely manual, people-based approach.

Use cases

Other areas in which technology is increasingly being used as a component of legal risk management include:

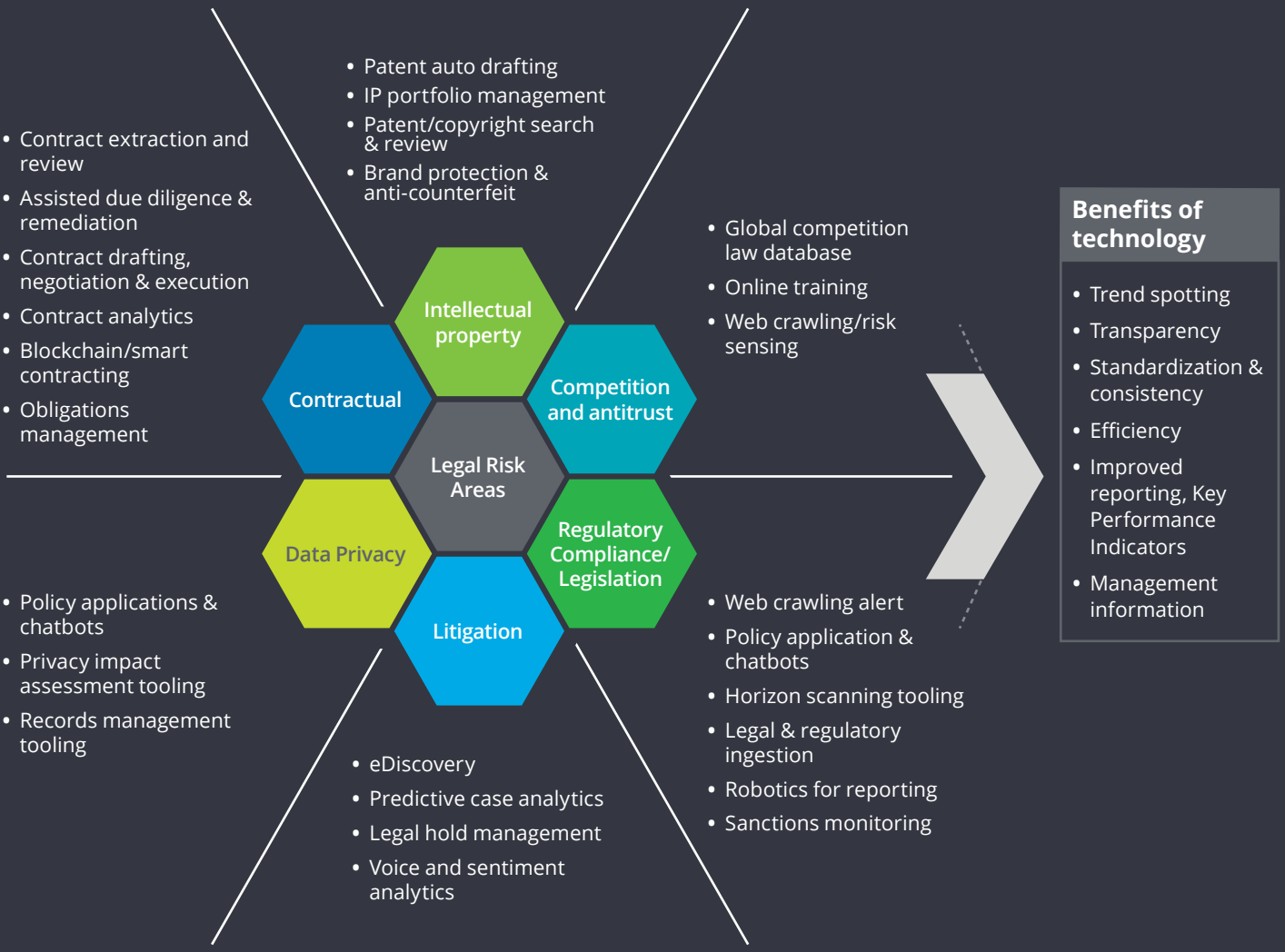
- Non-compliant event reporting. Although dependent on access to data, through the use of technology this can be turned into insights to help strengthen legal risk management
- The creation of management information (MI) which ensures that the whole organization has visibility on risk areas and can plan for and mitigate these risks effectively
- Exchanging information with regulators to demonstrate that measures are in place to improve compliance
- Fraud monitoring and detection, and call monitoring especially in environments which combine huge transaction volumes with the need for rapid reporting
- eDiscovery
- Case management tooling allowing for cases to be risk-rated
- Horizon scanning of large volumes of internet data and websites to identify legislative changes
- Litigation predictive analytics using large volumes of case precedents to better inform legal decisions to settle or fight
- Chatbots covering legal policy areas providing greater management information and insight to the type of questions coming into the Legal function and trends/potential risk areas
- Whistleblowing



Technology Enabling Legal Risk Management

Cross-departmental technology	
Identification, assessment and reporting of risks and controls	Enterprise risk management systems
Transparency and reporting of legal activity and risk profile	Matter management & eBilling
Managing legal instructions and business self service	Workflow
Managing documentary information	Document management system
Maintaining knowledge, insight and precedent	Knowledge management database

Here are some examples of technology use cases available to improve the management of legal risk



Interaction with regulators

Primary responsibility

The GC typically has a role in interacting with regulators, although more often than not specifically in relation to legal risk. In large regulated organizations which separate ownership of legal risk, regulatory risk and compliance risk into different teams, this may be less frequent as interaction is shared between the GC, the Chief Compliance Officer and the Chief Risk Officer. In smaller or less regulated organizations, all three areas may sit within the Legal department under the overall responsibility of the GC. The extent of interaction by the GC with regulators (and how proactive this is) will be dictated in large part by how regulated the industry is in which the organization operates.

A changing landscape

Keeping abreast of emerging regulations which carry legal risk is essential, including those regulations which primarily relate to operations. This includes horizon-scanning at both group and subsidiary or country levels and considering the impact of the increasing number of regulations which operate across borders. As regulations have an increasingly transnational impact, developing strong and transparent relationships with regulators may be a good way of managing legal risk and, in the event of a breach or compliance failure, securing a pragmatic outcome that doesn't result in penalties in multiple jurisdictions for the same issue.

Many organizations expect that monitoring and reporting will include some description of emerging regulations and their associated risks, together with identified breaches and their likely outcome. A fit for purpose reporting regime should include some narrative around interactions with regulators and what this means for the organization. We have seen increasing interest from financial services regulators to understand how organizations approach legal risk management in the context of a broader risk framework review.

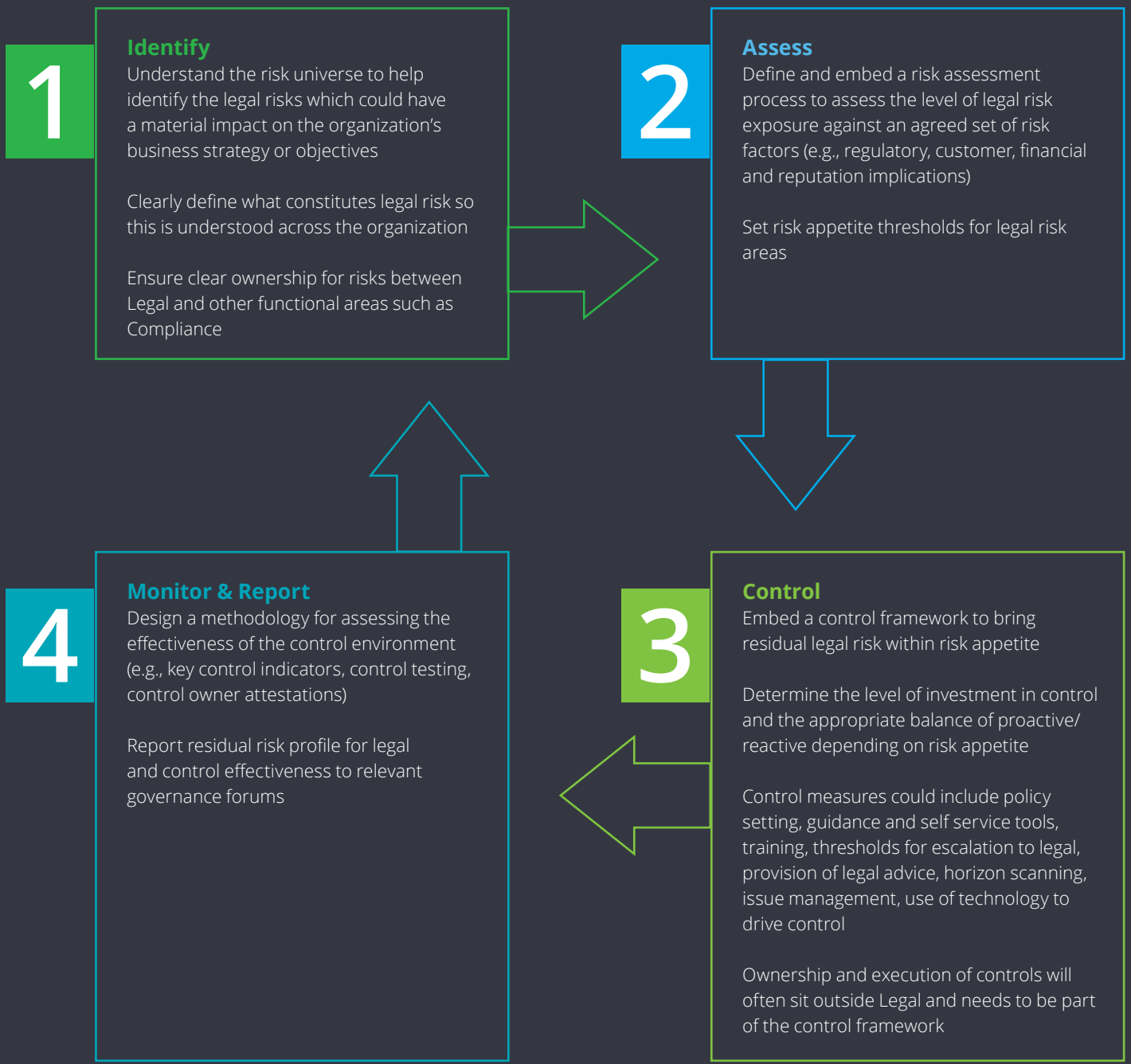
In time...

As organizations become increasingly mature in their identification and management of legal risk, we can expect to see legal risks separately identified and included in an enterprise's Risk Management Framework. This change of approach and mindset will enable Legal to respond more effectively to increased expectations and contribute to competitive advantage by controlling legal risks arising across the organization's operations.

Lessons will be learned from today's approach to monitoring and reporting of litigation risk, market risk and for financial services companies, credit risk. Monitoring, measurement and reporting will become more formulaic, with the use of key risk indicators to reduce the degree of subjectivity in what should be reported. The measurement of legal risk will become increasingly prevalent as legal operating models leverage technology to capture the underlying data and present it together with insights into root causes and recommendations that make legal risk management increasingly robust.

Fit for the future legal risk management will:
• Define legal risk and its boundaries with other risk areas
• Assess legal risk using a robust framework informed by data and scenario planning
• Define legal risk appetite at an individual risk and organization-wide level prioritizing and focusing resources on risk management activities effectively
• Apply the three lines of defense model to ensure appropriate accountability, independence and assurance over legal risks
• Report legal risks and the effectiveness of controls to the board and appropriate committees against a clear risk framework
• Include objective key risk indicators in their reporting
• Use technology in the management of legal risk to provide broader risk and control oversight and visibility across the organization.

Deloitte's Legal Risk Management Framework



Contact

At Deloitte, we have a broad range of skills to assist you in evaluating your current approach to legal risk management and identifying focus areas to minimize the threat of legal risks crystallizing. We use multifunctional teams with expertise in Legal Operations, Risk Management, Technology and Change to equip your organization for the future.

Luis Fernando Guerra
Deloitte Global Leader,
Legal Services
+34 91 514 5000
luguerra@deloitte.es

Karina Mowbray
Deloitte UK
+44 20 7007 6573
kamowbray@deloitte.co.uk

Tom Brunt
Deloitte UK
+44 20 7007 4891
tbrunt@deloitte.co.uk

Alexander Schemmel
Deloitte Germany
+49 89 290368948
alschemmel@deloitte.de

Candice Holland
Deloitte South Africa
+27 112098598
canholland@deloitte.co.za

Begona Fernandez Rodriguez
Deloitte Spain
+34 914381587
bfernandezrodriguez@deloitte.es

About the survey

Between September and October 2018, we polled over 100 General Counsel and senior in-house lawyers to benchmark approaches to legal risk management. This poll took the form of two surveys – one focused on the UK banking sector, the other, in conjunction with RSG Consulting, focused on companies across Europe, North America, and Asia-Pacific outside the banking sector.

All survey participants work in large companies (FTSE, FORTUNE 500, EUR350, or similar). The participants hold senior ranks (senior in-house lawyer or general counsel) in their organization. The corporate respondents represent more than 10 sectors; financial services, industrials and consumer account for more than half the total organizations. More than three quarters of respondents were based in the UK, Europe or Asia-Pacific.

Deloitte.
Legal