Legal risk 2.0: Show you’re in control
Foreword

Legal losses continue to make headlines in financial services. Sanctions imposed on firms by regulators have risen to a level that is creating real behavioural change. And the focus on conduct risk in particular is causing risk teams to review existing frameworks and identify data points to inform conduct risk dashboards. But how does this affect legal risk?

In 2015, the European Banking Authority put ethical conduct in scope of legal risk, and outlined how legal risk should be incorporated into operational risk capital calculations. Risk capital calculations are likely to change again, through the introduction of a new standardized measurement approach towards the end of 2016, but the fact that you need to include legal risk beyond the scope of litigation losses and expenses should by now be beyond question. And to add to that pressure, in the UK in January 2016 the Financial Conduct Authority (FCA) announced they would consult into the role of the General Counsel to clarify their position within the Senior Managers Regime (SMR). That paper is due to be available in the summer of 2016 and if, as we expect, the FCA explicitly states that General Counsels will be included within the SMR, they will be subject to increased scrutiny, and be required to evidence that they are in control of legal risk.

In light of the heightened scrutiny since 2015 and continuing into 2016, we wanted to look again at in-house attitudes to legal risk not just within in-house legal teams, but across operational risk teams and the C-suite. We canvassed responses from a wide-range of companies across US, EMEA, and Asia Pacific that operate predominantly within the financial services sector including retail banking, wealth management, insurance and global banking and capital markets.

We particularly wanted to explore questions around ownership of legal risk, how well integrated legal risk is within broader risk management activities, and the ability of General Counsel to show that they are in control of legal risk. To complete the picture, we asked about the level of support General Counsel receive (from their organizations and from regulators), and what are the priorities and challenges for legal risk management in the immediate future. We hope you will find the analysis interesting, and do please get in touch if you would like to discuss any aspect of this report.

Legal risk 2.0: Show you’re in control
Legal risk benchmarking survey: results and analysis

Our legal risk industry survey explores current working practices around legal risk management, how well legal risk is understood throughout the financial services (FS) sector, the top priorities for businesses, and the challenges that organizations face in their efforts to show that they are in control of legal risk. We were able to draw three broad conclusions from the results, which we discuss in more detail throughout this report, and support with further analysis and details of our own legal risk management methodology.

1. Legal risk is owned by the General Counsel/In-house legal department

Lawyers’ subject management expertise make them (on the face of it) the natural owners for legal risk. But legal risk is such a broad area that you need to create a structured set of supervisory controls to help you meet your risk management responsibilities.

2. Legal risk isn’t well integrated into operational risk frameworks

Because legal risk overlaps with other risk areas, and organizations in FS are usually very complex, to manage it effectively you need to integrate with operational risk frameworks. And support the development of dashboards, predictive legal risk models and near real-time Key Risk Indicators from current operational risk data sets.

3. There is broad agreement on legal risk priorities and challenges

Legislative/regulatory compliance is still a key priority for most respondents, but duty-of-care or “conduct” related risks were a top priority for a significant number of respondents.

These three conclusions lead to several calls to action for firms in financial services in particular. The advent of the SMR and need to evidence that you are in control of legal risk is going to lead to new investment in integration of working practices, alignment of risk data-sets and greater influence over business decisions for the legal function.

“[There is] little point talking about legal risk without defining what it is before the conversation begins.”

Before we get into the details of the analysis, we will clarify what we mean by legal risk. Legal risk has been ill-defined over the last ten years, which has in part led to the lack of understanding that is evident in the results of this report. At a policy level, we define legal risk as follows:

Legal risk is the risk of financial or reputational loss that can result from lack of awareness or misunderstanding of, ambiguity in, or reckless indifference to, the way law and regulation apply to your business, its relationships, processes, products and services.

This is a deliberately broad definition and maps directly to human understanding and behaviour of the way your business (its relationships, processes, products and services) interact with law and regulation.

You will read how to refine this definition into a set of manageable responsibilities in the next section of this report, and consider where the ownership of legal risk sits within your own organization.
Seven out of ten respondents agreed that legal risk is owned by the General Counsel/In-house legal function in their organization. As the obvious subject matter experts in the law, this seems to make sense. And of the respondent role groups (see Appendix 1), in-house counsel were by far the most confident in their level of understanding. Almost 65% of in-house counsel were confident in their understanding of legal risk. But outside of that group, confidence levels drop to just 50%. But the legal department isn’t the only candidate for ownership.

Other candidates were the CRO/COO function (12%), the Board (8%) and the Chief Compliance Officer function (6%). All these groups are potentially valid owners of legal risk, dependent on how ‘ownership’ is framed. If ownership is framed in terms of controls, then CRO/COO would be a natural choice. Or if it is framed in terms of corporate governance, then the Board would be the obvious candidate. But if ownership is framed within the need to identify and quantify exposure, as a crucial first step, then you would expect the General Counsel’s Office to take the lead, due to their legal expertise.

The role of in-house legal teams within the three-lines-of-defence is much debated. In-house lawyers have a natural alliance to the first line, typically acting in a management or advisory role within that first line. Figure 1 shows a simplified version of the three-lines-of-defence and the roles that in-house lawyers take across each line.

To manage legal risk consistently across a complex organization, you need your legal team to adopt a second-line-of-defence role, in addition to their first line responsibilities, proactively assess potential exposure and advise the business at a macro level how to reduce exposure. The results of this survey leave no doubt that in-house teams need to better integrate into the three-lines-of-defence and apply operational risk management techniques to meet their second-line-of-defence duties.

Figure 1: The varied roles of a lawyer within three-lines-of-defence

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First line</td>
<td>Many businesses employ lawyers specifically to advise, for example, on business transactions, or commercial contract negotiations. Depending on the specifics of the work they do, this will be considered as either “1a” (front-line) or “1b” (management of front line) activities.</td>
</tr>
<tr>
<td>Second line</td>
<td>In-house legal teams have a responsibility to identify, aggregate and advise the business how to proactively manage legal risk. This area has been the focus of regulators and is where many legal functions now need to improve their approach.</td>
</tr>
<tr>
<td>Third line</td>
<td>In a very few instances, lawyers will assume 3rd line internal audit responsibilities. They may review the work of other legal teams to assure that they are managing legal risk appropriately. And when they act on internal investigations - fraud or regulatory - they quite naturally adopt a pseudo third-line audit role.</td>
</tr>
</tbody>
</table>

Regulators could do more to support legal risk management initiatives

One of the issues faced by General Counsel is the lack of clarity around what is expected by regulators. There is overwhelming agreement (80%) that regulators need to be clearer in their expectations, which we believe aligns to the need for legal to receive clarification of their role. Legal teams are small and although training is available (60% of respondents say specialist training is available should they need it), legal risks are so broadly integrated throughout various business processes that as General Counsel you need to be absolutely clear about your responsibilities.

One way to achieve this clarity is to map legal risks to a General Counsel Supervisory Control Framework (GCSF). Your GCSF outlines the risks you are directly responsible for, the risks you have supervisory responsibility for, and the risks you have delegated fully; and tracks the controls of those risks throughout the organization. This enables you as a core risk owner to track your exposure, monitor the effectiveness of controls and identify control owners to contact if their risks are flagged as heightened.

“Regulators are more confused than businesses and this adds to the management difficulty.”
<table>
<thead>
<tr>
<th>Risk Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract risk</td>
<td>The risk that you will fail to keep track of and meet or enforce your contractual obligations or rights, or enter into contracts with terms that are either inadequate, unfair or unenforceable.</td>
</tr>
<tr>
<td>Dispute risk</td>
<td>The risk that your behaviour leading up to and within a legal dispute could negatively impact the quantum of loss.</td>
</tr>
<tr>
<td>Non-contractual obligations risk</td>
<td>Risks that corporate behaviour and individual decision-making could result in a failure in non-legislated duty-of-care (or civil duty) to third parties.</td>
</tr>
<tr>
<td>Legislative/ regulatory risk</td>
<td>Legislative awareness, impact assessment and ongoing compliance frameworks. Not just compliance, but also the ability to take advantage of business opportunities that arise through heightened awareness of the legislative/regulatory environment.</td>
</tr>
</tbody>
</table>

2. Legal risk isn’t well integrated into organizational risk management practices

There is inevitable overlap between legal risk and other risk types. The degree of legacy integration means that to deliver good legal risk management, and evidence that you are in control of legal risk, you need to leverage existing risk management efforts and data.

Compliance risk, for example, is an area where legal teams could add significant value in the horizon scanning and impact assessment. Conduct risk is another area where lawyers’ insight into legal and ethical interpretations of action can help guide business decisions in a direction that meets regulator expectations.

A large proportion of your risk management processes will incorporate legal documentation as a form of risk control. One of the most interesting overlaps is the link between operational risk and non-contractual obligations (or duty-of-care). Up to 75% of your operational risk controls, for example, could well be in place to manage non-contractual obligations risk. The level of loss being imposed by regulators for operational failures in duty-of-care (or duty-of-care) has been identified as a significant area of risk that needs to be managed.

Because legal risk results from day-to-day business decisions and working practices technology is essential to gather and report the data that speaks to the current state of controls, operational losses that relate to a legal risk, the status of your Key Risk Indicators, and to feed predictive models that will point to where the next big legal risk exposure could come from. At the moment, more than half of respondents aren’t confident in their knowledge of where their biggest legal risk exposure is. And 70% of GC/CLO respondents aren’t confident that they can identify and quantify potential sources of legal loss. Although there is much greater confidence in the ability to predict short-term legal risk events (60% don’t expect to suffer a material loss in the next 12 months) the ability to look beyond the next 12 months needs to be developed.

Figure 3: FSA, FCA, PRA and SEC fines 2007-2016

Source: www.fca.org.uk and www.sec.gov

“Legal departments still often work as classical counsel, question asked, question answered. The problem is [to] efficiently involve legal in operational workflows.”
We asked respondents to rate their priorities between the five risk categories (see Figure 3). After analyzing responses, we found that Legislative/Regulatory Compliance risks are a top priority for 66% of respondents. The legislative regulatory landscape is voluminous and complex, and the varied application of the law across multiple jurisdictions poses many problems for international financial services organizations.

A recent development is the increased prioritization of non-contractual obligations. Non-contractual risks (compliance with duty-of-care/civil duty) were the number two priority for 40% of respondents. This is partly due to the growth of Conduct risk as a risk discipline and the involvement that legal teams have to manage exposure, but also due to the continued priority of regulators in FS to prioritize tort through their enforcement actions (see Figure 3), and the threat of individual criminal accountability looming large through SMR.

Contract risk was third in the overall priority list. There are two sides to contractual risk. On the one is the quality of the wording within your contracts, to confirm not just that the appropriate language required by regulators is included, but that terms are enforceable, fair and accurately represent the expectations of each party. But on the other side is the role of the contract as a key control document. This is being explored throughout the sector as legal departments begin to engage in risk management discussions, and in particular around front-office control risks.

3. There is broad agreement on legal risk priorities and challenges

We asked respondents to prioritize the five risk categories listed in Figure 2, and to prioritize a list of challenges that could affect their ability to deliver robust, proactive legal risk management. There was broad agreement across both priorities and challenges.

Top three legal risk priorities in 2016

"Legislative and contractual have been on the top risk list for some time (and will probably remain high on the list). Conduct/duty-of-care is currently the priority."

"[Legislation/regulation] is the licence for us to do business. I regard the legal/reg risk alongside duty to the customer as the priority risk."

Recent litigation expenses dwarf legal fees and expenses in 2012

Litigation expenses begin to outpace legal fees and expenses in 2012

Litigation expenses now 12 times more than legal fees and expenses

"Litigation expenses exceed legal fees and expenses by $27bn over five years"

"Recent litigation expenses dwarf legal fees and expenses"

"Litigation expenses now 12 times more than legal fees and expenses"

"Litigation expenses exceed legal fees and expenses by $27bn over five years"

Source: From FR_Y-9C submissions (www.federalreserve.gov)

8 | Legal risk 2.0: Show you’re in control
The lowest priority is intellectual property risk, although this was a top priority for three respondents and one respondent made the point that neither Contract nor IP risks are actually “low”. We believe that the ongoing impact of digitalization on the financial services industry, for example through investment in FinTech and the development of the FCA Sandbox in the UK, will give greater emphasis to strong and trusted brands. The legal risks involved with engaging effectively with customers via digital channels will become a core challenge for in-house teams in the coming years.

Challenges
Respondents identified Organizational complexity, Availability of data and Available budget as the top three challenges they face in their implementation of legal risk management (see Q9). Leadership focus also came through as a concern.

1. Organizational complexity
Our respondents come from predominantly large financial services organizations. When you have tens (or hundreds) of thousands of staff, to identify the individual behaviours and standard working practices that could bubble-up into a legal risk is incredibly difficult. It is one of the key reasons behind our conclusion that it is imperative to integrate legal risk management with broader operational risk management.

2. Availability of data
The complexity of organizations and the relatively low resource levels within legal teams (as owners of legal risk) mean that a manual approach to legal risk monitoring and assessment won’t work. Firms need to supplement the human expertise with technology and systems that can collate data points from current organizational processes, align them to legal risk analysis and so generate clear management information to support risk-based decisions.

3. Leadership focus/available budget
Legal risk management programs require strong leadership and adequate budget, as well as the necessary skills and expertise to deliver. Given the lack of current integration and poor use of data, it would seem the time is right for General Counsel to put legal risk at the top of their agenda, invest in their legal risk management frameworks and work proactively to reduce their exposure to multi-million dollar losses and widespread global headlines.
Questions and Answers

About the respondents
The majority of respondents have a legal background and work within the in-house legal team. We also had good coverage at the risk function (CRO, CCO et al) and board/business delivery. This provided good insight to the differences in opinion between the functions - in particular with relation to the level of integration between legal risk and operational risk frameworks.

Industry/sector

<table>
<thead>
<tr>
<th>Area</th>
<th>Public services</th>
<th>Legal services</th>
<th>IT, media and telecoms</th>
<th>Retail banking wealth management</th>
<th>Insurance</th>
<th>Global banking &amp; markets</th>
<th>Asset/fund management</th>
<th>Energy</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>9.52</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
</tr>
<tr>
<td>Asia-pacific</td>
<td>15.87</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
</tr>
<tr>
<td>EMEA</td>
<td>78.60</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
<td>1.56</td>
</tr>
</tbody>
</table>

1. Who has primary responsibility for legal risk management in your organization?

- Other: 3.08%
- Operational risk/CRO or COO: 12.31%
- Legal/general counsel: 4.69%
- Compliance/Chief compliance officer: 6.15%
- Board-level/CEO: 7.69%

2. We use operational data to monitor and model legal risk.

- Neither agree nor disagree: 6.15%
- Disagree: 12.31%
- Agree: 78.77%

3. I know which business, jurisdiction, product line or internal function is most exposed to legal risk.

- Neither agree nor disagree: 6.15%
- Disagree: 12.31%
- Agree: 78.77%

4. I am confident in my understanding of legal risk.

- Neither agree nor disagree: 6.15%
- Disagree: 12.31%
- Agree: 78.77%

This showed a slight improvement on previous surveys covering multiple sectors, possibly indicating that legal risk is better understood within FS that in other sectors.
5. Legal risk is well integrated into our operational risk management framework.

6. Our approach to legal risk compares favourably to that of similar businesses.

7. I am confident in my ability to identify and quantify potential sources of legal loss.

8. Please prioritize the importance of the legal risk areas below, from 1-5 where 1 is your top legal risk priority and 5 is your lowest priority.

9. Please prioritize your biggest challenge in managing legal risk in your business from 1-5 where 1 is your top challenge and 5 is your lowest challenge.

10. My organization makes specialist legal risk training and know-how available to me if I need it.

11. Regulators are clear in their expectations towards legal risk management.

12. I expect to suffer a material loss due to legal risk in the next 12 months.

13. I use technology to increase efficiency in identifying and managing legal risk.

Tables 8 and 9 have been calculated based on a points system, where 5 points are awarded to each top priority, 4 for second, 3 for third, 2 for fourth and 1 for fifth. Totals were then added up to form overall prioritization.
How EY can help

We are a global leader in risk advisory services. Through our FS legal services and legal risk team, we are ideally placed to advise how to implement a robust legal risk management framework, integrate with broader enterprise risk programmes and pinpoint legal risk within your business.

For further information, please contact:

Matt Whalley
Director, Legal Risk, UK FSO
+44 20 7951 0296
+44 7342 021329
mwhalley1@uk.ey.com

Matthew Kellett
Partner, UK FSO
+44 20 7951 8085
+44 7973 763243
mkellett@uk.ey.com

Rod Campbell
Senior Manager, UK FSO
+44 20 7951 8970
+44 7748 932083
rcampbell1@uk.ey.com

Steven Francis
Executive Director, UK FSO
+44 20 7806 9021
+44 7925 148548
sfrancis@uk.ey.com

James Gee
Executive Director, UK FSO
+44 20 7951 1959
+44 7538 988847
jgee@uk.ey.com

James Smith
Executive Director, UK FSO
+44 20 7951 7811
jsmith6@uk.ey.com
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2016 EYGM Limited.
All Rights Reserved.

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com