riliance
Excellence in compliance

Amicus
LEGAL CONSULTANTS

ROYAL EXCHANGE FEEDBACK

JULY 2017

JULY 2017 **MEETING**

In July Amicus Legal Consultants and Riliance hosted a risk round table to discuss the changing risk and compliance landscape. The event was attended by representatives from a broad range of industries including; Pharmaceutical, Cloud Technology, Professional Services, Legal and Risk Consultancy.

The key topics discussed were:

- Regulators and legislation - are they getting it right?
- Reacting to crisis - how can staff make good decisions?
- GRC - Common elements of a successful GRC programme.

ARE THE REGULATORS GETTING IT RIGHT?

There has been a rise in the introduction of new regulations that affected all sectors represented. The group identified a string of new regulations including the 4th Money Laundering Directive, Senior Management Regime and GDPR, in addition to the existing regulatory burden faced by organisations. How organisations respond to this and the actions they take to comply varied, dependant on sector. However, one issue was common: the burden is increasing and is seen to be driven in some cases by politicians with an incomplete understanding of the regulations and their potential impacts.

THE IMPLEMENTATION GAP

The drivers behind recent regulatory changes were agreed to be positive and aimed at improving society, whether making it harder for terrorists to fund their activity, or enhancing and protecting an individual's data rights. In practice, the implementation of these regulations was unclear in areas, leaving organisations trying to figure out what regulators expect. This has led to organisations adopting a "no risk" approach, which may not be achieving the outcomes expected by regulators:

- **Wetherspoons Group** deleted its entire customer email data base, as a response to the new data protection regulation. The decision was made "on a risk basis", comparing the benefit of holding a marketing database with the risk of a potential breach that may attract financial penalties.
- **International banks** establishing and running de-risking programmes in a response to increased regulatory and compliance requirements. De-risking programmes aim to reduce risk by identifying and withdrawing services that could be high risk. These programmes have been seen to damage financial inclusion and left certain demographics without access to banking facilities.

http://www.wired.co.uk/article/wetherspoons-email-database-gdpr
http://www.globalcenter.org/wp-content/uploads/2014/12/14-Dec-19-Oxfam-project-description2.pdf

WHO TO LISTEN TO?

Large national and international organisations may be caught by multiple regulatory frameworks. Guests with experience of having "multiple regulatory masters" talked about how they would have to prioritise regulatory compliance based on the commercial impact to the organisation. Typically regulators with "sharper teeth" would be complied with first before "softer" regulators.

HANDLING CRISIS

When events do occur, such as a data breach or whistleblowing, the keeping of good records of the decisions made (and why they were made) was seen as critical to protecting the organisation. In pressured environments, decision making can suffer and the group questioned whether staff generally could make good decisions while working through a crisis. Feedback shows that an organisation can prepare for, and be ready to respond well to, a crisis or critical event; however it would need to invest in staff training and establish effective processes to ensure the impacts of risk events were mitigated as much as possible. The upside is that, for those that had been in crisis situations, the investment in training led to staff being able to make better decisions in response to critical events. Keeping good contemporaneous decision logs also led to a more productive relationship with regulators and a much quicker recovery in the aftermath.

CRISES IN THE NEWS IN 2017

- **WannaCry** - Cyber Attack leading to mass disruption of the NHS.
- **United Airlines** - Reputational Damage after passenger mistreatment video went viral.
- **Fyre Festival** - Operational Failure as luxury festival goers turned up to a bare campsite and no music acts.
- **PwC & The Academy Awards** - Reputational Damage as the wrong Oscar winning envelope was handed over by a PwC accountant.
- **Uber Driver Revolt** - Ongoing PR issues as Uber's relationship with its drivers and regulators worsens.

RIGHT FIRST TIME

Responding to crises/incidents quickly and effectively was seen as a key aspect of governance however, there was a general consensus that more proactive initiatives before an event occurs were equally as important. If crisis management and training reduces the impact of risk events, good risk management can help to reduce the likelihood of the event even happening. No matter what the risk or compliance challenge, getting it right first time was agreed to be the best approach.

In practice this is challenging as General Counsels, Risk Managers and Senior Management all face the same challenge to understand what risks they face, how best to manage them, and then how to get the wider organisation on-board to embed effective risk management. The group all had experience of implementing a Governance, Risk and Compliance (GRC) programme, with varying degrees of success, and identified themes to help build engagement:

- **Show the cost** - Investing in risk management can demonstrate tangible ROIs when comparing the cost of mitigation with the cost of a crisis.
- **Make it relevant** - Organisations don't respond well to "Tick Boxing" GRC programs. Make risk management relevant by linking it back to the organisations objectives and goals.
- **Empower staff** - GRC needs to be lived throughout the organisation to be effective, and in some cases such as responding to a crisis, the best staff to be involved are not senior management.

GDPR

Any discussion about risk management would not be complete without mentioning GDPR. Guests all agreed that preparing for GDPR was a major focus in 2017. Sectors with a history of handling sensitive data (such as Pharma) were more prepared; whereas sectors not subject to stringent data protection regulations, or not used to handling sensitive data, had more to do.

The same challenges were raised by the group in relation to GDPR as with other regulatory demands: What will the regulator expect in 2018, how will the subjective areas of the regulation be interpreted and how prevalent will fines be? While questions remain about what the GDPR will mean when it comes into force, the group were all preparing to be compliant and making sure they were not the first to find out!

AMICUS LEGAL CONSULTANTS

Amicus works across most global regions, combining legal expertise, highly practical corporate procedure 'stress testing' and an approach to risk management that is decision-making focused. Amicus provides governments with advice on treaty and legislative implementation and corporate General Counsel and their external lawyers with preventive and mitigating strategies.

RILIANCE

Riliance is a leading Risk and Compliance service provider operating across multiple industries and predominantly in regulated sectors. Riliance provides risk management platforms, training services and consultancy services to help organisations implement and manage GRC effectively.

CONTACT

For more information on any of the topics discussed then please contact:

Arvinder Sambei
a.sambei@amicuslegalconsultants.com
07949 553 060

Richard Beech
richard.beech@riliance.co.uk
07528 300 359