MANAGING YOUR DATA

Transforming Risk with Better Information Governance

As regulated companies are required to manage ever growing amounts of data, and regulators are imposing increasingly severe fines, how can firms ensure they comply with this greater scrutiny?

Regulated firms are increasingly struggling to manage their risks related to Information Governance (IG). There is a need to manage growing amounts of information as a result of the increased use of, and reliance on, systems and platforms which are utilised by the business to store and control data, among other factors. This is being matched by a greater number of cyber attacks, increased regulation and a determination by authorities to implement regulations more strictly.

40% – 60%

The average year-on-year growth rate of corporate data.[2]

90%

The percentage of companies that have experienced customer data breaches.[3]

£240 Billion

The estimated amount of potential fines for consumer product organisations for failure to safeguard their data.[3]

The International Data Corporation (IDC) has predicted that the world's data will grow by 10 times by 2020.[1] Alongside this increase, regulation is becoming stricter and more comprehensive with initiatives such as the EU's General Data Protection Regulation (GDPR).

Regulators are taking a more assertive stance, launching more inquiries and imposing larger fines. One example of this was demonstrated by the Financial Conduct Authority which fined a large international bank just over £3million for failures in its systems and controls. In other cases of poor record keeping affecting major global financial services organisations, fines have ranged between £3million and £30million.

1 http://www.computerweekly.com/news/2240217788/Data-set-to-grow-10-fold-by-2020-as-internet-of-things-takes-off
2 Computerworld article: "Data Growth Remains IT's Biggest Challenge, Gartner Says" by Lucas Mearian, November 2010
3 Capgemini Consulting's Digital Transformation Institute, July 2016

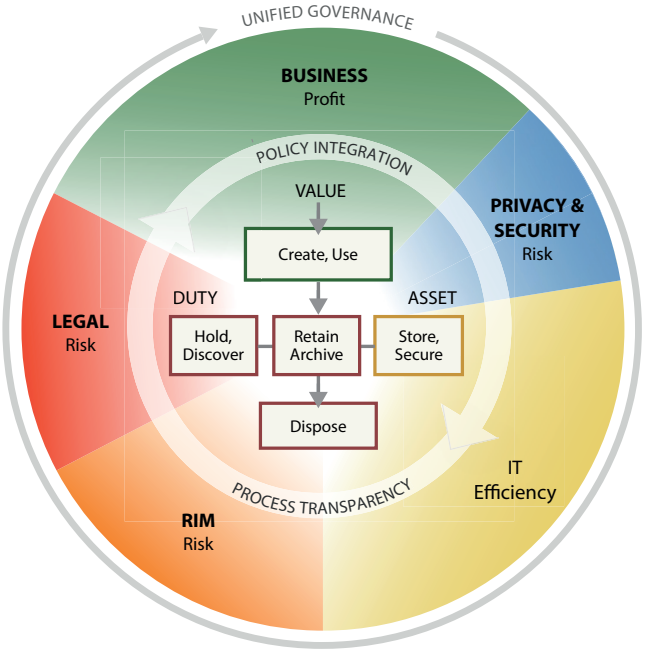
IG – no longer solely the responsibility of the IT department

The stakes for firms have never been higher and that is why IG is no longer a matter principally for the IT department. Instead, it needs to involve senior stakeholders from legal, compliance, security, privacy and the lines of businesses. The definition of IG by Gartner clearly shows how extensive this issue is becoming. IG is, according to Gartner: "The specification of decision rights and an accountability framework to ensure appropriate behaviour in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles, policies, standards and metrics that ensure the effective and efficient use of information in enabling an organisation to achieve its goals".

Information is being created at a faster pace and from increasingly diverse sources from file shares, SharePoint and applications to cloud and social media among many others.

Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management



Duty: Legal obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific containerof information

Information Governance Reference Model / © 2012 / v3.0 / edrm.net

The IGRM provides a framework for cross functional and executive dialogue and serves as a catalyst for defining a unified governance approach to information.

Three main sources of risk

Poor IG practice can expose firms to three primary sources of risk. First, there is **regulatory risk**. This includes regulations on record keeping requirements, confidential, financial information or patient records, mismanagement of which could result in legal liability. Failure to comply with the GDPR can result in fines of up to four percent of annual global turnover or €20million, whichever is greater.

Second is **litigation risk**. Firms that fail to preserve data appropriately in connection with a lawsuit or investigation might find sanctions issued against them as a result of insufficient legal records or potential spoliation of information.

The third area is **reputational risk**, in other words the negative impact on a firm in the eyes of shareholders, customers, the media and other audiences as a result of loss or misuse of information. This damage to reputation can result in revenue loss and a reduction of shareholder value.

IG risks should be managed as part of a broader Enterprise Risk Management programme which is most effective when bringing together the bottom up IG business processes, controls and reporting together with the top down approach from the board which sets strategic objectives, risk appetite and an overall corporate governance framework.

Firms must adopt a more integrated approach

The key to developing an effective IG risk mitigation system is integration. All too often, risk managers have had limited access to the board and strategic investment decisions are taken without their involvement. Similarly, risk managers, governance teams, compliance officers and other stakeholders frequently use a variety of frameworks and definitions. Additionally, IG projects are often tackled as a one off remediation or a disjointed activity. For example, firms today are pursuing aggressive migration to cloud applications like Office 365 or Box and often are doing so without fully considering the records, legal, privacy or security requirements of the data.

As threats from cyber attacks and more severe regulatory sanctions continue to increase, firms need to adopt a more holistic, integrated approach which

should be a board level issue with appropriate executive stakeholder support. In this way, it will receive the funding and prioritisation required to drive coordinated people, process and technology transformation across the company.

For instance, it is often required that a CIO, COO or similar level stakeholder must ultimately take ownership with the representation and engagement of stakeholders across legal, compliance, IT, security, privacy and the business. Once this integrated approach has been established the firm can appoint an IG champion who can start by initiating a comprehensive assessment of its data and associated business processes. This involves identifying where data sits within the organisation, how sensitive it is (employee and customer information rank highly here), which regulations apply to it and who has access to it.

The IG champion should work with other departments to put together a comprehensive, integrated governance structure that is appropriate to the firm's size, area of activity and locations in different jurisdictions around the world. They should take responsibility for developing a programme roadmap, including the definition of key remediation activities, allocation of resources, responsibilities and timelines, prioritised by risk, source, and/or jurisdiction. These risks should be tracked as part of a risk register which is visible to key stakeholders to ensure accountability for remedial actions.

Like other aspects of risk management, effective IG requires integrated Governance, Risk and Compliance (GRC) with both a top down and a bottom up approach as demonstrated in the diagram below. While the board provides the top down action, this strategic view must be integrated with the bottom up activities such as business processes, controls and reporting.

Consistency is essential. Policies and standards should be aligned throughout the organisation following global retention standards, with a minimum number of exceptions. There should also be alignment of enterprise IT processes such as system provisioning, decommissioning, migration of systems or storage management.

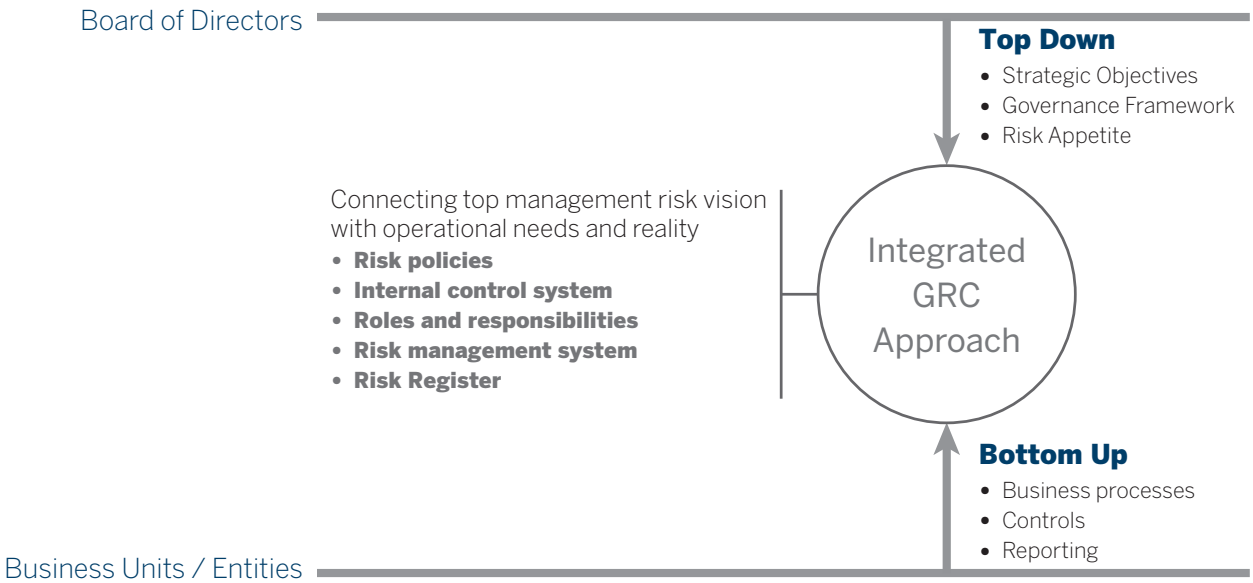
Global policies and one overall platform

The IG champion should ensure that the firm maintains global policies and a well defined target operating model whilst enabling local ownership and management of records which are compliant with regulations. They should also require all records to have a clearly defined owner and to be organised and classified so that they are easy to retrieve and retain for the appropriate periods. They must ensure that records are stored in compliant repositories and disposed of at the end of their lifecycle.

Working from a unified governance framework, all stakeholders must agree on a consistent set of policies and controls that are well defined to minimise ambiguities and misunderstandings. All stakeholders must be incentivised to take part and to cooperate with other stakeholders. They must be made fully aware of the excess cost and risk that poor IG presents, not only to the firm as a whole, but to them in particular.

The IG champion should make it clear that effective management of records and data can offer an opportunity to reduce the firm's risk and ultimately improve its position in the marketplace, placing it above the competition. This will give it a secure base from which to grow and make the most of new commercial opportunities.

Integrated GRC Approach



How one financial services firm reduced its IG risk

FTI Consulting worked with a global financial services firm to mitigate its risk on dark data and to help it to develop a strategic IG programme. Following an internal audit, the firm found that there was a significant volume of data on its systems, specifically fileshare content, which was being stored with inappropriate controls.

The company, which has around 50,000 employees globally, engaged FTI Consulting to analyse and remediate over 4.5 petabytes of its unstructured data. The FTI IG team interviewed over 250 staff across the company's compliance, legal, IT and information security teams.

"Collaborating with the firm's staff and utilising StoredIQ®, we classified questionable content to determine how critical it was and whether its storage method was appropriate," says Sonia Cheng, FTI Consulting's Information Governance and Compliance Services European Leader. "We also used our own proprietary e-discovery software Ringtail® to simplify the manual review of suspect data to ensure it was in compliance with its internal and external policies."

FTI discovered improper storage for regulated content, open security on unencrypted sensitive data, personal data in unsecured locations and improperly stored communication data as well as hundreds of terabytes of obsolete data. "All of these increased cost and risk for the company," says Sonia Cheng.

At the end of the engagement, FTI processed 4.5 petabytes of information, classified over 200,000 documents and remediated more than a petabyte of dark data to help the firm reduce its regulatory and operational risk exposure. Each file was tagged with a recommended action: migrate to properly managed storage, decommission, or leave in place. It was also given a priority based on its exposure to risk.

"In addition, our team also worked closely with the firm's IT and compliance teams to further refine its policies and procedures to ensure that the data would be managed more effectively in the future," says Sonia Cheng.

Key points to consider:

- The amount of data that firms have to manage is increasing exponentially
- Dark data presents particular risks
- Regulators are more assertive in their approach and are now imposing larger fines
- Given its growing importance IG is no longer solely a matter for the IT department
- Firms must take a holistic approach to IG. C-level executives need to take responsibility for it and engage an IG champion to lead this critical transformation.

This paper has been produced in collaboration with Nina Bryant, Unstructured Data Strategist at Deutsche Bank and Sarah Walker, VP & Global Chief Counsel at Aon Risk Solutions.

Sonia Cheng
Senior Director – Information Governance & Compliance Services
+44 (0)20 3727 1783
sonia.cheng@fticonsulting.com

FTI CONSULTING™