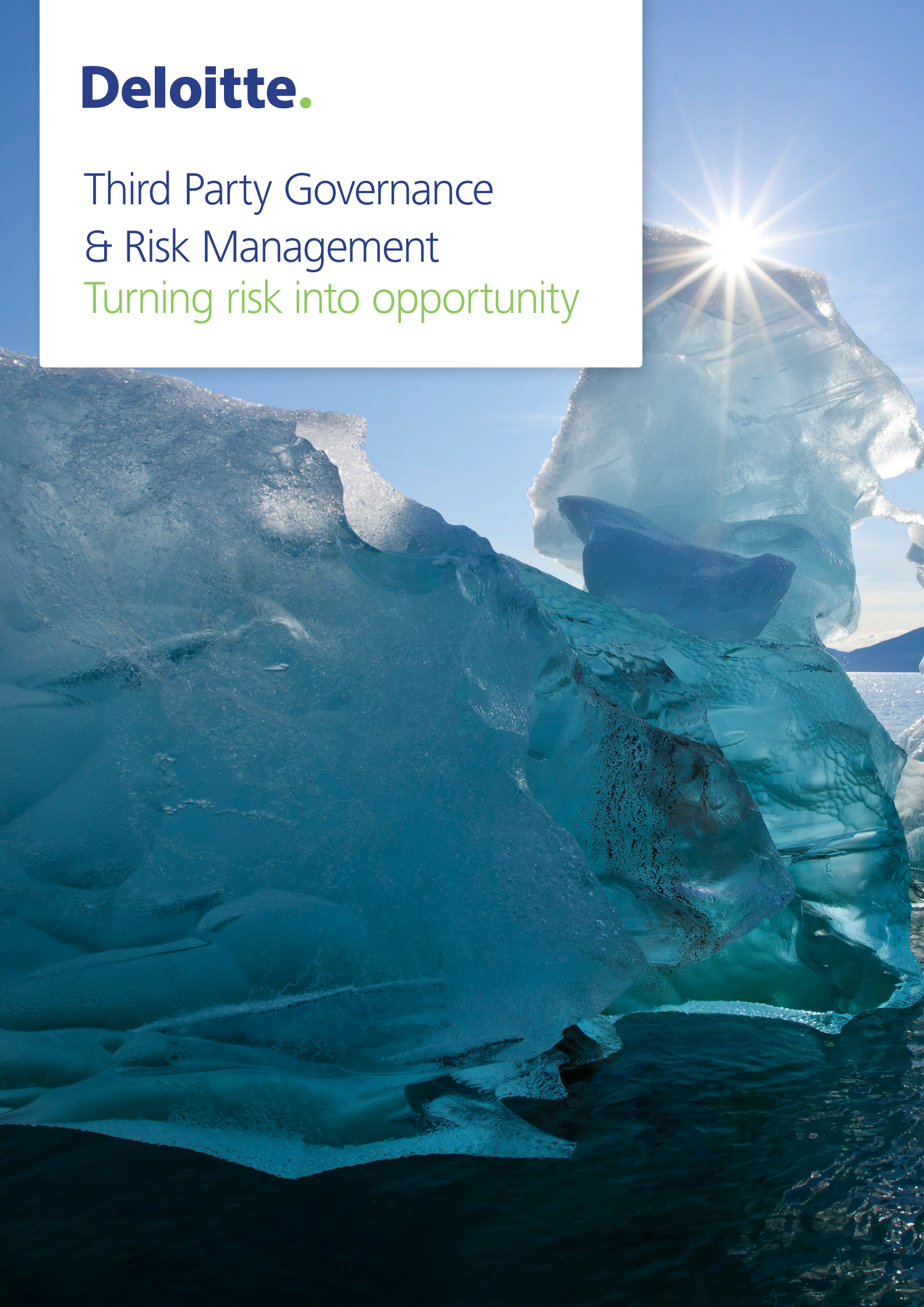
Deloitte.

Third Party Governance & Risk Management

Turning risk into opportunity



Contents

Foreword

For many businesses their global third party ecosystems (known as extended enterprises in some organisations) have in recent years become important sources of strategic advantage and business value. These organisations see their business partners as their second-most valuable organisational asset. Yet they are partners that bring risk. As reliance on third parties continues to grow, so does concern at the number of headline stories depicting regulatory action and reputational damage arising from third party actions. These are driving many organisations to reconsider how they approach the identification and management of the risks posed by third parties.

Third Party Governance & Risk Management ('TPGRM') is still in its infancy. Organisations are deploying a number of different approaches, some effective, others less so. For those that develop the most effective response there is significant opportunity: gaining holistic visibility of the risks that third parties bring to an organisation can enable that organisation to exploit, to the full, the opportunities that the extended enterprise presents.

In this paper, the first in a series of publications on this topic, we present our global experience on TPGRM and reveal the hard facts on this important issue. This paper will be followed up by additional papers focused on specific topics of interest, the first of which will cover the results of our Third Party Governance & Risk Management survey. We also offer tools and frameworks that will enable you to understand the rising need for effective Third Party Governance & Risk Management, enable you to assess your organisational maturity and determine a clear way forward for you. This is intended to help you not only manage third party risk, but also highlight the business case and the opportunity that third parties create for your organisation.

As reliance on third parties continues to grow, so does concern at the number of headline stories depicting regulatory action and reputational damage arising from third party actions. These are driving many organisations to reconsider how they approach the identification and management of the risks posed by third parties.

1. The rise of the extended enterprise

The notion of extending physical and virtual boundaries to garner the benefits of collaboration with third parties across the supply chain is not new. Management thinkers like Michael Hammer[1] have advocated the alignment and integration of businesses since the mid-nineties, and it has long been clear that, managed correctly, these extended enterprises can deliver organisational value and competitive advantage.

One of the top tier companies in the Fortune 500 has enjoyed a meteoric rise from obscurity to become one of the world's most known and loved brands. Astute use of overseas third parties has played a pivotal role in this rise.

More than one hundred million of the products that the company sells are assembled with components sourced from its extended ecosystem across countries like China, Japan, Taiwan and Korea. Research studies however show that the economic benefits of this accrue to the company in the U.S. rather than in the countries where the third parties are based.

The key benefits of such arrangements include cost advantage, which in turn drives dominance in price setting, best-in-class inputs and flexibility/scale that enables appropriate timing of product delivery.

Enhancing third party dependence is increasingly becoming a trend in highly innovative companies that wish to avoid high production costs. It also enables them to carry out higher value activities such as design, marketing and product management closer to home through the core organisation.

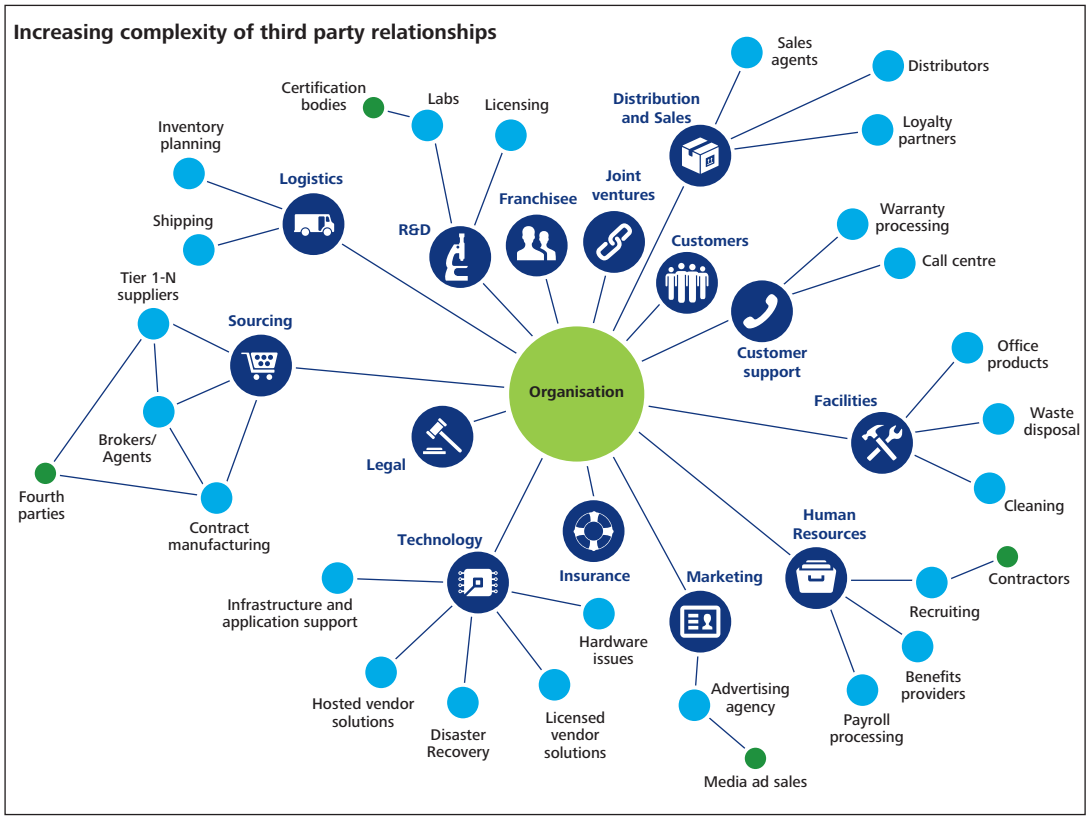
What is new is the degree to which this is now taking place, and the risks this is creating. Businesses have taken the concept of the extended enterprise to new levels. They are now facing risks such as the threat of high profile business failure, illegal third party actions being attributed to the organisation or regulatory enforcement action enforcing punitive fines in the more regulated industry sectors.

Deloitte estimates that the failure by large multinational businesses to appropriately identify and manage third parties (e.g. suppliers, distributors, franchises and joint venture partners) can lead to fines and direct compensation costs or other revenue losses in the range of US$ 2 – 50 million, while action under global legislation such as the US Foreign Corrupt Practices Act can be far higher, touching US$ 0.5 – 1 billion.

Whilst businesses have traditionally focused on management of third parties in their direct supply chain (suppliers and vendors), the benefits of extending the enterprise have increasingly also been realised on the sales and distribution side, in support services and with regard to alliance and joint venture partners.

The Institute of Collaborative Working (2014) estimates that up to 80% of direct and indirect operating costs of a business can come from third parties, while up to 100% of revenue can come from alliance partners, franchisees and sales agents.

1 Michael Hammer, Beyond Reengineering (New York: Harper Business, 1996)



Organisational focus on third party risk has traditionally been reactive and determined by who is driving the activity. This has typically been procurement teams focused on suppliers and vendors, or brand and intellectual property (IP) protection functions focused on distribution channels and non-authorised manufacturers. Such a decentralised approach to risk has led to micro-focus on risk areas that interest certain parts of a business or certain functions (for example, operational performance from a supply chain perspective or information security from a corporate security angle). Organisations are only now starting to take a holistic proactive approach to risk, covering all categories of third parties and all areas of risk.

Quantifying the risks 1: $772 million fines

A non-US headquartered multinational company, with interests in electricity generation and transmission as well as rail transport, was fined US$ 772 million in December 2014 for engaging in conduct in violation of the Foreign Corrupt Practices Act (FCPA). This has mainly resulted from the inappropriate conduct of third parties and ineffective due diligence and corporate controls over such third parties.

This new approach is a departure from the myopic method of considering risks in isolation and allows the organisation to consider *operational risk* factors (e.g. performance, quality standards, delivery times, KPI/SLA measurement) with *reputational/financial risk factors* (e.g. labour practices, an understanding of financial health, appropriate charging mechanisms and adherence to these) and *legal/regulatory risks* (e.g. compliance with bribery regulations, awareness of global industry standards as they apply to third parties, Environment and Health & Safety compliance) to obtain a comprehensive view of the level of risk across the extended enterprise.

The issue is particularly time-sensitive. The Deloitte Global CFO Survey reconfirms an unprecedented increase in global optimism and business perspective which is driving businesses to consider new sources of opportunity and organisational value.

When risk translates into rewards

With the rapid expansion of the extended enterprise, the risks associated with extending the enterprise continue to increase in proportion to the rewards. Recent examples of high profile business failures have demonstrated that Third Party Governance & Risk Management has not always been given the strategic attention it deserves.

Inappropriate action or failure of third parties has created new risks that have significantly impaired the achievement of strategic objectives (e.g. business model with regard to third party ecosystem failing to achieve growth and profitability targets in strategic plan). This has also compromised organisational reputation, broken down business continuity and resilience and even attracted substantial penalties and regulatory enforcement action.

Quantifying the risks 2: $400 million

A major supermarket chain in the USA faced a cyber-attack (November 2013) that resulted in the theft of 70 million items of data including details of their shoppers' addresses and phone numbers, and the theft of 40 million debit and credit card details.

The initial intrusion into its systems was traced back to network credentials stolen from a third party vendor, followed by a malware-laced email phishing attack sent to employees of that vendor organisation.

It is estimated that the organisation could be facing losses in excess of $400 million as a result of this breach, including reimbursement associated with banks recovering the costs of reissuing millions of cards; fines from the card brands for Payment Card Industry (PCI) non-compliance; and direct customer service costs, including legal fees and credit monitoring for tens of millions of customers impacted by the breach.

Regulators around the world, for instance in the financial services domain, are significantly increasing their attention on the third party risks faced by their regulated entities.

The US Office of the Controller of the Currency (OCC) Bulletin 2013-29 issued in October 2013 as well as the Board of Governors of the Federal Reserve System (Fed) in the US are explicit and extensive around clarifying who is included within the scope of a 'third party' and includes not just vendors but all third-party relationships within the entire extended enterprise.

Accordingly, the earlier focus on vendors as part of supply-chain management is now extended to outsourced/offshored providers of Information Technology and supporting business processes, all contractors, marketing partners and agents, brokers, franchisees and other parties operating under a collaboration agreement, joint venture partners and subsidiaries. It also extends to intercompany/inter affiliate services.

It is interesting to note that some of these third parties may also, in turn, outsource some of their processes to other subcontractors or service providers, giving rise to the concept of fourth parties. Regulatory guidance is starting to include these "fourth parties" if such parties are eventually responsible for supporting the third party business.

Elsewhere, recent cases of regulatory enforcement by the Financial Conduct Authority (FCA) in the United Kingdom have included a fine of approximately $67 million on a bank for IT failures (November 2014), which impaired the ability of its customers to access banking services. This, in turn, resulted from a software compatibility problem arising out of implementation of third party software, which remained undetected due to lack of adequate systems testing prior to going live, or broadly, the bank's failure to put in place adequate systems and controls to identify and manage their exposure to IT risks arising out of third party systems[2].

2 Financial Conduct Authority (FCA), Final Notice dated 19 November, 2014

Some industries are more mature than others in the use of third parties. For instance, manufacturing and consumer product organisations have long been focused on the extended enterprise in their supply-chain management and distribution network; retail organisations have traditionally leveraged third parties for greater sales penetration. Life sciences and healthcare companies have used third parties in their distribution network for a number of years, as well as contract manufacturers.

With the growth of Information Technology (IT) and business process outsourcing, banks and financial service companies have started leveraging third parties in this area, together with a large number of healthcare, manufacturing, distribution, retail and technology companies.

The new wave of virtual organisations such as online retailers or travel agents may choose to leverage third parties far more extensively to achieve higher strategic benefit than a more traditionally run business, with the related risks also increasing in proportion to the rewards. Accordingly, these businesses now need to consider more strategic risks such as reputation risk, together with legal, regulatory and other emerging risks, in addition to the usual operational risk of using third parties.

The increasing use of third party or extended enterprises is not about cost-reduction alone. Gaining strategic advantage, enhancing competitive edge and agility, are increasingly being innovatively focused upon to drive engagement with the ecosystem.

Capitalising on the opportunity and reaping the rewards

It is easy to focus exclusively on the risk, and forget the potential opportunity here. Deloitte experience indicates that effectively governed third party relationships can be a source of competitive advantage. For example, this can enable better product or service innovation, facilitate expansion to new markets and provide access to skills and capabilities not available internally, whilst the business continues to focus on its core business processes. As third parties bring in new knowledge and experience, some organisations are now also able to effectively use their third parties as knowledge partners or even as trusted advisors who are able to catalyse organisational innovation, provide strategic insights and feature on organisational Advisory Boards.

Deloitte believes those organisations that have a good handle on their third party business partners, can not only avoid the punitive costs and reputational damage, but stand to gain competitive advantage over their peers out performing them by an additional 4-5% ROE, which, in the case of Fortune 500 or FT500 companies can mean additional EBITA in the range of US$ 25-500 million.

Effective management and governance of the extended enterprise can drive performance by:

- Increasing revenue by identifying and recovering under-reported revenue streams.
- Minimising costs by selecting the right relationships that operate cost-effectively, limit regulatory issues and associated penalties.
- Enhancing the value of the third party by gaining efficiencies (for instance through technology-integration), improving service levels and better responding to fluctuations in market demand.

Academic researchers concur that best-in-class companies are establishing formal and comprehensive programmes that orchestrate their internal functions, suppliers, and customer operations, aligned to corporate goals[3]. Such strategic orientations have enabled some businesses to reduce product development times by as much as 40 percent and reduce the cost of purchased materials by between 15 and 35 percent[4].

Research by the Outsourcing Unit at the London School of Economics[5] shows that the announcement of a large outsourcing deal typically increases share prices, as investors view this announcement as a positive action, indicating tightening of cost control and "hands on" serious management.

Similarly, a study commissioned by Logica, (now CGI) entitled "The Outsourcing Effect on Stock Price" suggested that when companies announce an outsourcing or offshoring decision, their share price would go up. Benchmarked against other companies in their sector, the short-term benefit is estimated at performing around 1.7% better after an outsourcing announcement.

3 Berard, L. and York, M. (2013), Strategic Sourcing: The Future Is Now, In Analyst Insight Aberdeen Group, Boston, MA

4 Asmus, D. and Griffin, J. (2012), Strategic Sourcing: Best Practices, Innothink Group, Colorado Springs, CO

5 Willcocks, L. P., Cullen, S., & Craig, A. (2010). The outsourcing enterprise: from cost management to collaborative innovation. Palgrave Macmillan

This is supported by the findings of Stern Stewart Research in the USA, where a study of 27 companies undertaking large IT outsourcing initiatives indicates an average gain in shareholder value of 5.7% over and above the general market trend.

In 2013, three researchers from the University of Texas and the Indian School of Business[6] further demonstrated that firms pursuing large-scale, fixed price outsourcing, which are characterised by lower business uncertainty and simpler coordination requirements, realise higher market returns. Variable price contracts also realise positive long-term abnormal returns. These tend to occur in the longer term, at a point when the causes of outsourcing success – many of which appear are intangible – have become clearer. *However, the results also imply that firms which outsource complex functions without pertinent experience, prior association with the vendor or perceived lack of governance may eventually experience significant loss of shareholder value.*

In terms of risk management, more generally, a 2012 study by FERMA[7] found that firms with 'advanced' risk management practices exhibited stronger EBITDA and revenue results over five years than those with 'emerging' risk practices. This review of over 800 firms in 20 countries concluded that 75% of firms with 'advanced' risk management practices had EBITDA growth of more than 10% per annum.

The study validates that advanced risk practices and culture can directly correlate to stronger financial results, as the entire organisation becomes more aware and accountable for the significant obstacles standing in the way of success. This enterprise approach helps management see the connections between the risks, in essence, linking risk management with strategy in their decision-making.

The changing paradigm of third party risk

Traditional	Emerging
From a narrower focus on supply chain management	To leveraging the wider extended ecosystem, including third parties in sales, distribution and marketing; support services; business partners, strategic alliances and subsidiaries
From cost savings as the primary driver	To strategic agility, access to special skills and competitive advantage as the key drivers
From a source of risk	To a source of opportunity.
From a technology focus evolving from enabling connectivity	To virtual networking and collaboration
From accountability at an operational level	To greater accountability at the Boardroom and C-suite level
From limited stakeholder impact	To significant source of shareholder value

In a 2014 Deloitte global survey[8], increasing costs, enhanced regulation and concerns around cyber fraud, data security and privacy were expected to challenge organisations on outsourcing as a business model. Challenges are expected to increase in staffing the retained organisation and managing vendors and contractors, who in turn are expected to enhance the innovation, soft skills and generate greater value to the business.

6 Mani, D., Barua, A., & Whinston, A. B. (2013). Outsourcing Contracts and Equity Prices. Information Systems Research, 24(4), 1028-1049

7 http://www.ferma.eu/blog/2012/10/ferma-risk-management-benchmarking-survey-2012-the-results accessed on 5 May 2015

8 Deloitte. (2014). Global Outsourcing and Insourcing Survey Results. Available at http://www2.deloitte.com/content/dam/Deloitte/us/Documents/strategy/us-sdt-2014-global-outsourcingInsourcing-survey_051914.pdf; accessed on 6 May 2015

2. Taking this seriously: the hard facts

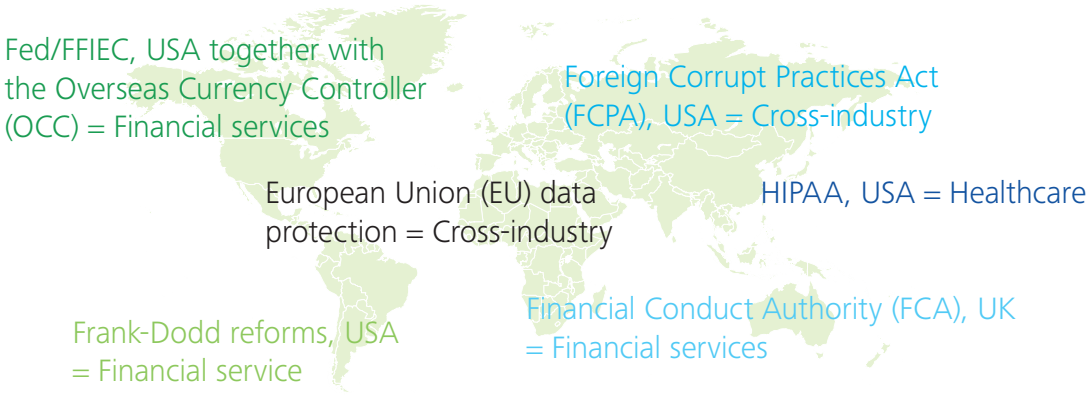
Why are regulators interested in third party governance and risk management?

Although the concept of making principals responsible for the actions of their agents is not new, legislators around the world are increasingly interested in how businesses manage their third parties. This is driven by the need to ensure that the operating structure and business models of their regulated entities do not adversely affect the end-customers of these entities. Given this fundamental regulatory objective, the related regulation has set out two key expectations:

- The need for businesses to continue to recognise that they are responsible for the acts of third parties in complying with their regulatory responsibilities. This is particularly important as they recognise the nature of new threats arising in the world of evolving technology-driven innovation.

- Making it clear that the use of third parties should not impair their ability to regulate businesses.

Sources of regulation with a global implication on third party risks



Financial Services: An industry leading the way in third party regulation

Around the world, industry-specific regulatory action with regard to the use of third parties is dominated by the financial services industry but as penalties become increasingly severe, so other sectors are catching up. We predict that other industries will continue to refine their regulations and activities to focus on the continued risk of third party entities.

Examples of regulatory action in the financial services industry

For instance, in the UK, the FCA has recently started implementing a revised penalty framework which seeks to remove the value of the entire financial benefit derived directly from the breach, with powers to further enhance the same to provide a "credible deterrent".

This resulted in total fines exceeding approximately US $1.6 billion between April 2012 and September 2014. Total fines to firms have increased from $94 million in 2011-12 to about $672 million in each of the last two full financial years. The typical fine is also getting larger with the median fine increasing from $2.24 million in 2011-12 to $8.9 million in 2013-14.[9]].

9 [Source] NERA Research, Patton, R. Trends in Regulatory Enforcement in UK Financial Markets 2014/15 Mid-Year Report

Examples of significant FCA action related to Third Parties in the last two years

- November 2014: US$ 67 million. "IT failures which occurred in June 2012 and meant that the Banks' customers could not access banking services". This, in turn, was due to a software compatibility problem arising out of implementation of third party software, which remained undetected due to lack of adequate systems testing prior to going live. More broadly it was concluded that it was a result of the Banks' failure to put in place adequate systems and controls to identify and manage their exposure to IT risks arising out of third party systems.
- September 2014: US$ 59 million. "Failing to take reasonable care to establish adequate and effective organisational, control and risk management systems in relation to the opening, on-going operation and monitoring of external accounts in which safe custody assets were held with sub-custodians outside the Banking Group ("third-party sub-custodians")".
- August 2014: US$ 13.4 million for "failing to treat customers fairly over the sales of accident insurance by outsourced service provider companies". The FCA said that the insurance company failed to provide customers with fair and balanced information and put up barriers to prevent customers from cancelling policies. The FCA added that these failings were made possible by poor systems and inadequate oversight of the outsourcing companies. The FCA found that the telesales scripts used did not provide clear information and emphasised the ability to cancel policies in order to drive sales. When customers tried to cancel, the process designed presented barriers to cancellation. Poor governance and monitoring of the outsourcing companies was blamed for the mistreatment of customers, along with an "aggressive" outsourcing timetable and an inadequately resourced compliance department.
- August 2014: US$ 7.5 million for "incorrectly reporting transactions between November 2007 and April 2013" caused by a coding error in software developed by contract staff which reversed the buy/sell indicator. As a result, the bank failed to properly report 29,411,494 Equity Swap CFD (contracts for difference) transactions.
- June 2014: US$ 3.7 million. Failure "to pay due regard to the information needs of its clients and communicate with them in a way which is clear, fair and not misleading" for financial products sold to retail investors through third party distributors.
- March 2014: US$ 504,000 for a "failure to take reasonable care to establish and maintain effective systems and controls for countering the risks of bribery and corruption". The FCA found that the general insurance broker, operated a weak control environment surrounding the sharing of commissions with third parties which gave rise to an unacceptable risk that they could be used for corrupt purposes.
- December 2013: Over US$2.8 million for failing to have in place appropriate checks and controls to guard against the risk of bribery or corruption when making payments to overseas third parties, breaching the FCA's principle on management and control. Between 19th February 2009 and 9th May 2012, the organisation received almost $33 million in gross commission from business provided by overseas introducers, and paid them over $18 million in return. Inadequate systems around these payments created an unacceptable risk that overseas introducers could use the payments made for corrupt purposes, including paying bribes to people connected with the insured clients and/or public officials.
- More than US$ 1.4 million for "failing to adequately protect client money". The organisation, an outsourced service provider of asset management and wealth management services. Under the FCA's client money rules, firms are required to keep client money separate from the firm's money in client bank accounts with trust status. Firms that undertake client transactions and hold client money should perform daily client money calculations (referred to in the FCA Client Asset Sourcebook (CASS) rules as internal reconciliations) to check that they are segregating the correct amount of client money so that in the event of the firm's insolvency, client money is returned to clients as quickly and easily as possible. Between November 2007 and October 2012, the organisation failed on several occasions to perform its internal reconciliations failed on several occasions to ensure that any shortfall or excess identified in its internal reconciliation of client money was paid into or withdrawn from the client bank account by close of business on the day of the internal reconciliation.

[Source: Various FCA Final Notices cited above]

In late 2013, the OCC became the first major U.S. banking regulator to issue updated guidance about third-party risks, noting eight specific areas where banks needed to make improvements to their vendor management programmes related to third parties. Among those recommendations were guidelines related to how banking institutions should terminate relationships with third parties if certain security criteria are not met.

At the time of writing, the OCC is focusing attention on card-payments risks and the role third parties often play in the exposure of card data when it is being processed. On April 25, 2014 a district court in North Carolina approved a settlement with a bank, which had allowed a third-party processor to originate approximately $2.4 billion in debit transactions for fraudulent merchants. The bank has been ordered to pay $1 million to the U.S. Treasury and to forfeit $200,000 to the U.S. Postal Inspection Service's Consumer Fraud Fund. The bank is also required to take steps to prevent future consumer fraud.

Regulatory action is not a US or UK phenomenon alone but is increasingly becoming a global issue. Regulatory thinking in the area of third party risks in some other jurisdictions is highlighted below:

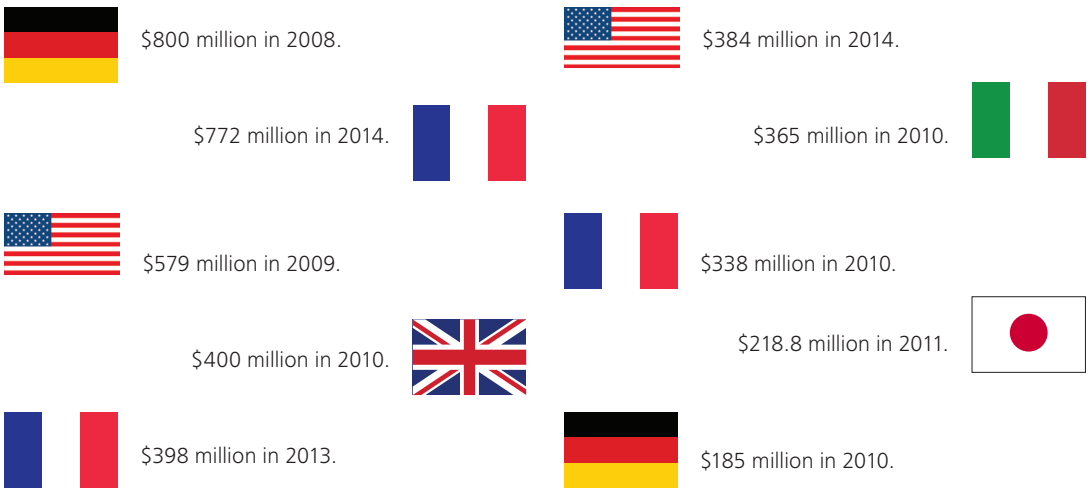
- **Singapore:** The Monetary Authority of Singapore (MAS) has stated that it "is particularly interested in material outsourcing which, if disrupted, has the potential to significantly impact an institution's business operations, reputation or profitability and which may have systemic implications."
- **Australia:** The Australian Prudential Regulatory Authority (APRA) aims to ensure that all outsourcing arrangements involving material business activities entered into by a regulated institution are subject to appropriate due diligence, approval, and ongoing monitoring.
- **Hong Kong:** The Hong Kong Monetary Authority (HKMA) states that institutions "should not enter into, or continue, any outsourcing arrangements [that] may result in their internal control systems or business conduct being compromised or weakened after the activity has been outsourced."

Cross-industry regulation impacting third parties globally

Several elements of legislation and regulation are industry-neutral and have a global impact. The US Foreign Corrupt Practices Act (FCPA) applies to all industries and affects multiple global jurisdictions. The "top 10" FCPA enforcement actions to date indicate that non-U.S. companies dominate the biggest FCPA cases[10]:

It is believed that non-U.S. headquartered companies are slower to recognise the risks of FCPA offences and enforcement.

Largest FCPA fines and penalties



10 Cited in The FCPA Blog, http://www.fcpablog.com/blog/tag/top-ten; accessed on 6 May 2015

Many of these companies operated significant long-term bribery schemes in several global locations outside the USA. With their limited appreciation of FCPA, the evidence of this was retained in explicit emails, false consulting agreements and related invoices, money transfer records etc.

Three of the largest cases in the last one year are analysed below:

$772 million for engaging in conduct in violation of the FCPA, in turn mainly resulting from the conduct of third parties and ineffective corporate controls over third parties. "The organisation did not perform any due diligence on the consultant even though the consultant had no knowledge about, or experience in, the relevant industry. Certain consultants were located in a country different than the project country. At other times, the consultants asked to be paid in a currency or in a bank account located in a country different than where the consultant and the project were located. In multiple instances, more than one consultant was retained on the same project, ostensibly to perform the very same services. Despite, these "red flags," the consultants were nevertheless retained without meaningful scrutiny."

$384 million: More than $110 million in corrupt payments were made to Bahraini officials with influence over contract negotiations between the organisation and a major government-operated aluminum plant. Its subsidiaries used a London-based consultant with connections to Bahrain's royal family as an intermediary to negotiate with government officials and funnel the illicit payments to retain its business as a supplier to the plant. The organisation lacked sufficient internal controls to prevent and detect the bribes, which were improperly recorded in its books and records as legitimate commissions or sales to a distributor.

$398 million: The organisation made more than $150 million in profits through the bribery scheme and attempted to cover up the true nature of the illegal payments by entering into sham consulting agreements with intermediaries of the Iranian official and mischaracterising the bribes in its books and records as legitimate "business development expenses" related to the consulting agreements. The organisation had inadequate systems to properly review the consulting agreements and lacked sufficient internal controls to comply with federal laws prohibiting bribery.

The UK Bribery Act came into force with effect from 1 July, 2011 and since then enforcement activity has primarily been on individuals rather than corporates.

However, in December, 2014, the UK Serious Fraud Office (SFO) secured its first conviction related to a $35 million biofuel scam, relating to promotion of biofuel investment products linked to jatropha tree plantations in south-east Asia. The former chief commercial officer, together with an agent used by the company, was found guilty of Bribery Act offences and conspiracy to provide false information.

Increasing impact of emerging regulation and regulatory enforcement beyond financial services

The focus on third parties is not a financial services phenomenon alone. Other regulators and stakeholders such as consumers and consumer protection groups, shareholders, activist groups, market analysts, for instance in various other industries including life sciences and healthcare, chemicals, food and drink, and retail, are being held accountable for improper action by third parties who act as their agents.

Based on Deloitte experience, we predict that industry regulation will significantly increase in the coming five years. This, together with the increasing dependence on the extended ecosystem by companies in these industries, will make Third Party Governance & Risk Management an even more strategic initiative. This is evidenced by the following recent developments:

- In one of the largest healthcare fraud settlements in U.S. history (November 2013), the US Department of Justice announced that a global healthcare giant and its subsidiaries will pay more than $2.2 billion to resolve criminal and civil liability arising from allegations relating to manufactured drugs, including promotion for uses not approved as safe and effective by the Food and Drug Administration (FDA) and payment of kickbacks intended to promote the use of these drugs in nursing homes. Although the consultant pharmacists who were involved purported to provide "independent" recommendations based on their clinical judgment, this civil settlement concluded that the organisation viewed the pharmacists as an "extension of their sales force", thus holding the organisation responsible for these actions.

- In the UK, the Medicines and Healthcare Products Regulatory Agency (MHRA) is the organisation that looks after the safety of prescribed medicines and other health devices and equipment. The MHRA works closely with the European regulator, the European Medicines Agency (EMA), which oversees the safety of medicines across Europe. With the recent expansion of enforcement responsibilities and powers of the MHRA[11], it appears that this organisation is rapidly strengthening itself to expand both its capability as well as the rigour of enforcement to follow the role model of the FCA in the financial services sector.

- In the food industry, the recent discovery of horsemeat in products labelled as beef at certain retailers in the UK in early 2013 has focused attention on the need to manage risks better with the supply chain. The Chartered Institute of Procurement and Supply[12], an international trade body and watchdog for buyers, suppliers, and the procurement industry, carried out a survey which indicates that 86% of supply chain managers do not believe that regulators understand supply chains, while more than a third, 36%, claim their CEO is not engaged about the potential risks in the supply chain. In addition, only 53% of companies have a strategy to mitigate risk in their supply chains[13].

- The chemical industry is another sector where regulatory compliance is vitally important, as the business viability of chemical products now depends on conformity with health and safety and environmental legislation. For example, REACH is a European Union regulation on the Registration, Evaluation, Authorisation and restriction of Chemicals, which was implemented in June 2007[14]. REACH has replaced a number of different chemical regulations with a single system, which aims to protect human health and the environment through improved identification of the properties of chemical substances. The European Chemicals Agency (ECHA) is expected to be very active in its implementation of the European Commission's Substances of Very High Concern (SVHC) Roadmap to 2020[15], which entails data gathering, screening and Risk Management Options (RMOs) for SVHCs. With a large number of contract manufacturers involved in this industry together with other third parties in supply chain and distribution, this is likely to enhance the strategic importance of Third Party Governance & Risk Management.

The increasing impact of new technology

The rapid emergence of new technology, as illustrated below, will stimulate further regulatory focus and increase the impact on third party risks.

Gartner[16] predicts that 2015 will be dominated by the adoption of hybrid cloud technologies. These will rapidly escalate the status of third party cloud-related technology providers to a critical level, a shift that will bring significant risks. Fundamental concerns about security, privacy and resilience of data and applications on the cloud will remain – with significantly enhanced ramifications of consequences of any breach or security incident. Data ownership and privacy will remain key concerns, together with lack of clarity on who exactly is the data owner and who is the data processor under various privacy enactments. Legal issues will include confusion over legal jurisdiction, which will become blurred and contract compliance will become even more complicated.

New regulation is continually emerging with a global basis or pan-European impact. For example, the recent European Payment Services Directive (PSD/2)[17], which enables the European Commission vision to create a single European payments market, includes a provision to regulate third party (so-called "third party payment service providers") access to payment account information, including the amount of funds in the account. The objective is to standardise and regulate access to financial information so that payment transactions can be made directly without the use of credit cards (and paying the related commission) or other intermediate service providers. It is expected that large retailers would consider becoming third party payment service providers themselves, enabling them to take payments directly from a customer's bank account. This brings in new risks around the protection of consumer data as well as the need to substitute traditional controls that existed within the traditional four-party payment system effectively and efficiently.

11 The Medicines and Healthcare Products Regulatory Agency, available at https://www.gov.uk/government/publications/report-a-non-compliant-medical-device-enforcement-process/how-mhra-ensures-the-safety-and-quality-of-medical-devices; accessed on 6 May 2015

12 The Chartered Institute of Procurement and Supply; www.cips.org; accessed on 6 May 2015

13 Cited in The Telegraph, 11 March 2013. Available at: http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/9922860/UK-supply-chains-need-overhaul-to-avoid-new-horse-meat-scandal-survey-warns.html; accessed on 6 May 2015

24 The European Chemicals Agency, http://echa.europa.eu/regulations/reach; accessed on 6 May 2015

15 Roadmap document available at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205867%202013%20INIT; accessed on 6 May 2015

16 Gartner, Top 10 Strategic Technology Trends for 2015. Available at: http://www.gartner.com/technology/research/top-10-technology-trends; accessed on 6 May 2015

17 European Commission, Directive on Payment Services (PSD), 24 July 2013. Available at: http://ec.europa.eu/finance/payments/framework/index_en.htm; accessed on 6 May 2015

Data privacy and protection continues to be an area of prime focus globally, particularly when personal data resides with third parties in the ordinary course of business and the contractual relationship with the third party. Under the new EU data protection law[18], fines for noncompliance can now be up to 2% of "annual worldwide turnover". These fines would be imposed on the data collector by the supervisory authority (the governmental body that handles data security within a member state) on a case-by-case basis and be "effective, proportionate and dissuasive".

Data backup and resilience has been an important consideration where data has resided with third parties. However, the recent EU Working Party guidance on the "Right to be forgotten" published at the end of November 2014[19] will drive action in the opposite direction to remove personal data when requested by the data subject, with penalties for not doing so across all global jurisdictions within an acceptable timeframe.

The explicit and the implicit cost of third party failure

1. 90% of top executives consider third party risk as a key business challenge.

2. Punishment by regulators causes losses to shareholders that are on average, 10 times the size of the fine itself.

3. Investing in reputation risk management can demonstrate expected additional 4.3 percent annual return on equity.

It is relatively easy to quantify the explicit impact of reputation loss caused by third party failure in terms of fines, compensation and any direct expenditure to mitigate the impact of the loss. However, the implicit loss caused by reputational damage, is often much higher and more difficult to quantify. In the words of Warren Buffet, "If you lose money for the firm I will be understanding. If you lose reputation I will be ruthless."

The 2014 Deloitte Reputation Risk survey continued to identify reputation risk as a strategic issue; almost 90% of top executives surveyed considered it a key business challenge. They recognise that any element of reputation risk that is not properly managed can quickly escalate into a major strategic crisis. The survey highlighted the following top business risks driving reputational damage, all of which can be put in third party context:

- Risks related to ethics and integrity such as fraud, bribery, and corruption involving third parties.
- Security risks, including both physical and cyber breaches compromising data held by third parties.
- Product and service risks, such as those related to safety, health, and the environment arising out of the action of third parties, suppliers and vendors.

Reputation loss is increasingly being measured by fall in share prices and market capitalisation, following the announcement of enforcement action or any other event triggering reputation damage.

Three academics from Oxford University[20] (John Armour, Colin Mayer and Andrea Polo) recently demonstrated that punishment by regulators causes losses to shareholders that are, on average, 10 times the size of the fine itself. Interestingly, this ten-fold proportion of impact did not increase with the size of the fine. Share prices, on average, were seen to fall by around 2.55% in the three days after the announcement, where direct harm to customers and investors was involved (after neutralising the effect of broader market trends). This was significantly higher than situations not directly harming customers or investors such as failing to file proper financial returns or transaction reports, behaviour adversely impacting trading partners or even failing to implement adequate process controls not impacting partners.

18 European Commission, Press Release Database: "Progress on EU data protection reform now irreversible following European Parliament vote" dated 12 March 2014. Available at: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm; accessed on 6 May 2015

19 European Commission, 26 November 2014, Article 29 Data Protection Working Party Press Release. Available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf; accessed on 6 May 2015

20 Armour, J., Mayer, C., & Polo, A. (2010). Regulatory sanctions and reputational damage in financial markets. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678028; accessed on 6 May 2015. Oxford University Centre for Corporate Reputation: http://www.sbs.ox.ac.uk/ideas-impact/reputation/events/regulatory-sanctions-and-reputational-damage-financial-markets; accessed on 6 May 2015

Nir Kossovsky, in his book "Reputation, Stock Prices and You"[21] demonstrates, through the use of forward-looking big data, how even the sceptics now have a clear and compelling business case to invest in reputation risk management. "For the median company, the upside measure of success is an expected additional 4.3 percent annual return on equity. This is the product of building value with both a strong defence and an effective offence". Another emerging concept is that of reputational continuity, which Kossovsky believes to be a product of good governance. Taking the strategy to the stakeholders can create value. When stakeholders can appreciate improvements in governance, controls and risk management that upgrade their long-term expectations, equity values will rise.

Quantifying the risk 3: Fines of $43 billion + 7% market capital erosion

A global petroleum giant is paying out US$10-$14 billion in fines (January 2015) related to one of the major oil spills in history. This is in addition to more than $28 billion in spill response, clean up and claims. It reached a $4.5 billion settlement of criminal allegations in 2012.

Share prices eroded in the region of 7% as markets expected the organisation to accept full accountability, despite its direct dependence on third parties. In its last financial statement, the organisation has taken a $43 billion charge against profits to cover all the costs, which are still subject to significant uncertainty.

Regulators around the world are realising that the impact of these fines, although disruptive, are sometimes still not sufficient to be credible deterrents of similar behaviour in future and are relooking at implementing newer mechanisms to calculate penalties that would have a greater impact on organisational behaviour going forward. The revised penalty framework, which the FCA has now started implementing, enables them to enhance fines significantly to provide this credible deterrent to inappropriate action, either by themselves or by their extended ecosystem going forward[22]. This is likely to enhance both the explicit and the implicit impact of the loss of their regulated entities.

21 Kossovsky, N. (2012). Reputation, Stock Price, and You: Why the Market Rewards Some Companies and Punishes Others. Apress

22 Hinton, P., & Patton, R. (2011). Trends in Regulatory Enforcement in UK Financial Markets. NERA Economic Consulting, London

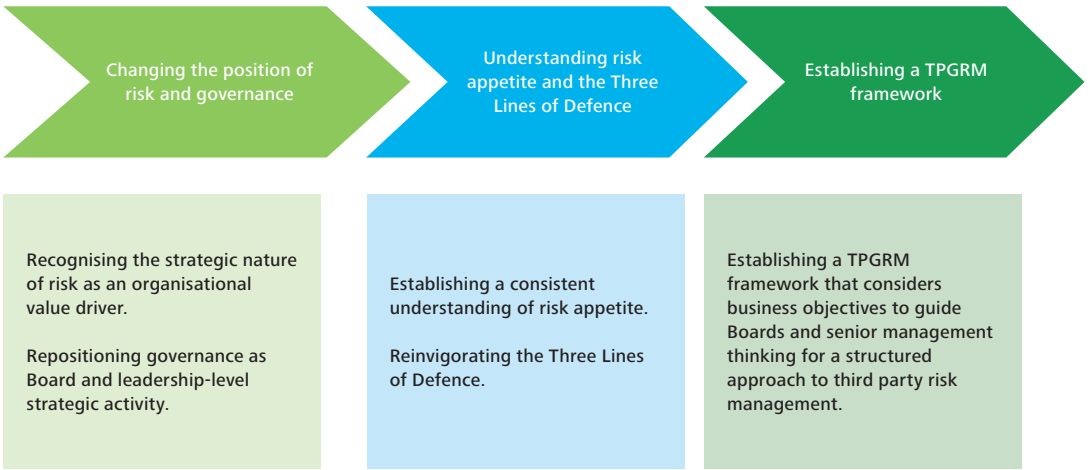
3. Perspectives and frameworks for TPGRM

This section sets out our perspective on the key concepts and developments that underpin the evolution of TPGRM from a defensive value-preservation activity to a much more strategic value-creation focused activity. These related concepts can provide a guiding framework to progressive businesses for creating a strategic opportunity from a well-governed extended enterprise. The following diagram summarises the relationship between risks, risk management and governance, which are discussed in the subsequent section.

Relationship between Risk, Risk Management and Governance

Good governance and risk management is not about eliminating risk, but rather managing it appropriately. Further, such governance and risk management mechanisms should not stifle the business. It should raise organisational awareness and competencies, remain simple and proportional to the overall risk to the organisation, whilst providing the right management information to the key stakeholders and accountable individuals.

The changing face of TPGRM



Changing the position of Risk and Governance

Risk management has long been associated with mitigating adverse financial consequences of "bad things happening". For instance, when most people think of TPGRM, they would immediately think about organisational interests and reputation being impaired through third party action or about fines, penalties and regulatory enforcement action.

However, the world continues to realise that risks must also be seen as a source of opportunity. To seize those opportunities it is not enough simply to avoid the risks; for an enterprise to optimise its value and achieve success it must manage risks. This is even more critical in the face of a volatile and uncertain macro-economic environment ahead[23]. Accordingly, the more progressive global organisations are now starting to demonstrate bimodal thinking around how to maximise the opportunities out of the third party extended ecosystem while managing the related risks at the same time.

Governance, which is a higher-level process involving directing and managing risk management and related activities to address stakeholder expectations, is therefore naturally starting to reinvent itself with a focus on maximising the opportunity while also managing the compliance requirements and the downside of risk.

In this new thinking, the explicit linkage of risk and strategy, starting at the Board and C-suite level of the organisation, is considered an integral part of the organisational strategy-setting process[24].

Although the regulators around the world are better known for their enforcement action, it is extremely relevant to note that most regulators around the world are not only endorsing but also driving this enhanced accountability for risk management at the Board and C-suite level. Accordingly, most progressive global organisations now have top-level accountability for third party risk.

Management thinkers including Michael Porter[25] have long advocated how strategically aligned governance can significantly enhance competitive advantage through differentiation and enhancing shareholder value. This can be done not just by pursuing opportunities that enhance shareholder value, but also being stronger in dealing with disruption when it hits everyone, and creating a resilient image[26].

Changing position of TPGRM

- ☑ Risk as a matter of choice not just a matter of chance
- ☑ Governance strategically aligned and starting at the Board
- ☑ Board and C-suite accountability for governance initiatives
- ☑ Expanding the thinking to broader set of risks and strategic assets
- ☑ Adopting an outside-in perspective to consider external forces that impact business
- ☑ Cross-functional collaboration and alignment
- ☑ Risk management competency development and CoEs
- ☑ Alignment with ethics and corporate social responsibility thinking

23 See also: Funston, F. and Wagner, S. (2010). Surviving and thriving in uncertainty [electronic resource] : creating the risk intelligent enterprise / Frederick Funston, Stephen Wagner. Hoboken, N.J. : Wiley, c2010

24 See also: Beasley, M.S. and Frigo, M. L. (2007). Strategic Risk Management: Creating And Protecting Value. (cover story). Strategic Finance, 88(11), 25-53

25 Porter, M.E. (1985). Competitive Advantage. The Free Press, New York, NY

26 Elahi, E. (2013). Risk management: the next source of competitive advantage. *Foresight, 15(2), 117-131*

A critical success factor in this is to consider a much broader set of risks and strategic assets which are more difficult to leverage, manage and protect, including people, intellectual property, customers, marketing efforts, and even, for example, "the crowd" in emerging phenomena like crowdsourcing. Additionally, companies should adopt more of an outside-in perspective by gathering data and appreciating external perspectives from external sources, including, for instance, customers, bloggers, information trendsetters, and marketplace and security analysts[27].

Another recent global survey[28] corroborates the view that risk management functions have indeed started taking a more strategic role leading to mature practices such as stronger interaction between risk functions and Boards; use of analytics for evolving strategic purposes; development of cross-functional collaboration through such means as risk committees; financial and operational skill-development in risk management personnel; and the evolution of organisational risk knowledge centres.

Following the financial crisis, Ethics and Corporate Social Responsibility are also becoming more important and integrated elements of the strategic governance responsibilities of the Board, and this is supported by an increasing recognition of the strategic and moral benefits of having a strong reputation[29].

Relating this changing position to your organisation:

- ☑ Do you see the significant use of third parties as an extended ecosystem in your organisation increasing your risk exposure only, or do you also see this as a source of strategic opportunity to enhance competitive advantage and strategic opportunity?
- ☑ Would you consider risk management and governance related to third parties to be an enabler in your organisational pursuit of value and strategic advantage and is this directly aligned to the strategy-setting process?
- ☑ Do your risk management and governance activities over third parties have Board or C-suite level accountability?
- ☑ Are you merely concerned about protecting any damage to your reputation arising from third party actions or are you focused on proactively enhancing reputation through the use of third parties?
- ☑ Are third parties in your extended ecosystem aware of and aligned to your organisational thinking and policies on ethics and corporate social responsibility?
- ☑ How are you leveraging risk management and governance to maximise the opportunities arising from Third Parties as your organisational asset?
- ☑ Does your communication to your stakeholders include your focus on risk management and governance as a source of value?

27 Deloitte. (2013). Exploring strategic risk. Available at http://www.deloitte.com/view/en_US/us/Services/additional-services/governance-risk-compliance/explore-strategic-risk/index.htm; accessed on 6 May 2015

28 Marsh. (2014). Excellence in Risk Management XI - Risk Management and Organizational Alignment: A Strategic Focus. Available at: http://usa.marsh.com/NewsInsights/MarshRiskManagementResearch/ID/38927/Excellence-in-Risk-Management-XI-Risk-Management-and-Organizational-Alignment-A-Strategic-Focus.aspx; accessed on 6 May 2015

29 See also: Hull, C. E., and Rothenberg, S. (2008). Firm performance: The interactions of corporate social performance with innovation and industry differentiation. Strategic Management Journal, 29(7), 781–789

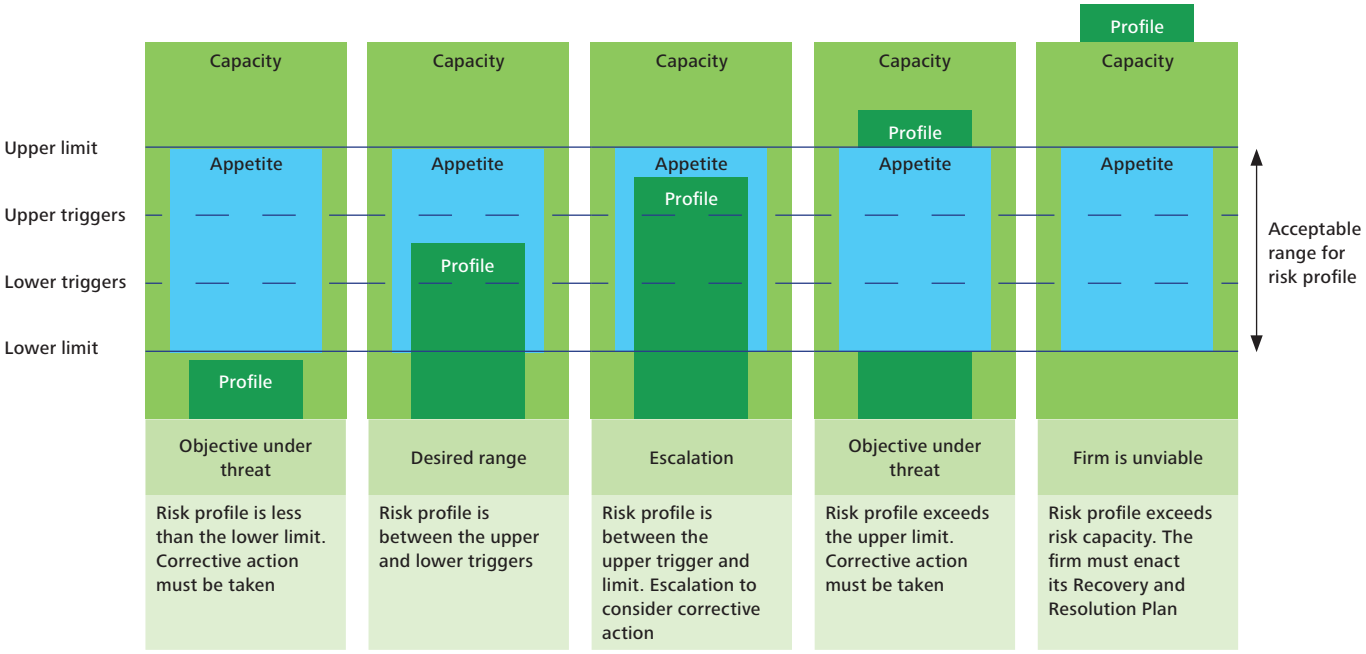
Understanding your risk appetite

Risk appetite is one of the essential concepts that must be understood and consistently applied to be able to reap the strategic benefits out of this emerging perspective on governance and risk management.

Simply stated, risk appetite is the amount and type of risk that an organisation is willing to pursue or retain (ISO/IEC guide 73:2009[30]). Similarly, the COSO's Enterprise Risk Management Framework[31] defines risk appetite as "the amount of risk an entity is willing to accept in pursuit of value" clearly recognising the opportunity dimension. The COSO Framework also recognises that is reflective of the entity's risk management philosophy, which in turn influences the entity's culture and operating style.

Risk appetite is thus about establishing a strategic boundary between the amount of risk that a business is willing and able to take as an integral part of its business model/profitability (risk seeking/upper limit) on the one hand and the level at which it wants to expose itself to "bad things happening" on the other (risk aversion/lower limit), together with a set of strategic, financial and operational risk parameters and related tolerances. These parameters and tolerances provide indicative triggers for management action and intervention according to the actual risk profile visa-vi risk appetite under various scenarios, as shown in the figure below.

Risk Appetite: Establishing the boundaries



30 Cited in Purdy, G. (2010). International Standards Organisation (ISO) 31000: 2009—setting a new standard for risk management. Risk analysis, 30(6), 881-886

31 Enterprise Risk Management: Integrated Framework. Committee of Sponsoring Organisations of the Treadway Commission, 2004

Set out below is an example of how a high-level risk appetite statement might look for an organisation which is not within financial services, but is seeking to strategically place higher dependence on its extended enterprise, supported by additional investments in TPGRM.

Sample Risk Appetite Statement

Strategic value drivers and risks	Sample assertions
Strategic value-drivers	**Market growth:** We will aggressively target a 15% growth in revenues and a 5% increase in market share through a three-pronged approach: • Expand to new markets in the MINT countries by investing in strategic alliances with established players in these new territories in our existing product range. • Innovate to develop new products related to focused markets through extensive research on emerging customer preferences. • Establish a franchisee network to enable marketing of company products more aggressively. **Profitability:** We propose two key focus areas to enhance profitability within a 1-3 year horizon: • Aggressively identify and invest in new supply-chain partners in emerging geographies with a potential to bring in strategic cost reduction, whilst looking for opportunities to revisit make or buy decisions taken in the past. • Rationalise overheads, enabled by finance and IT transformation through implementation of a shared services model and outsourcing of IT and business processes. The Board accepts the risks inherent in the above strategic initiatives, together with a planned enhancement in the level of governance and risk management to reduce the residual risks that the company would face by adopting this strategy.
Unacceptable risks	**Reputational damage and market capital erosion:** The Board has absolutely no risk appetite for any situation or action that can have a negative impact on the company's reputation, perception of company brands and/or cause market capital erosion. Should such an undesirable situation arise, the company is committed to addressing this as a strategic priority to contain any damage at the earliest opportunity and aggressively protect the company's reputation, brand perception and prevent any market capital erosion.
Strategic risks	**New markets and franchisee networks** The company has a higher risk appetite related to the above strategic objectives relating to market growth and is willing to accept higher losses in the pursuit of higher returns. While the Board expects a return of 18% on investment in each of the growth initiatives over a 1-3 year horizon, the Board is not willing to take more than a 25% chance that the investment leads to a loss of more than 50% of the capital investment in any new initiative. **Innovation and product development** The company however has a relatively lower risk appetite related to new product development. The Board will not accept more than a 5% risk that a new product will reduce our operating earnings in that overall product category by more than 5% over the next five years. **Supply chain partners** The company has a lower risk appetite related to the social and economic costs for sourced products from overseas locations that could be accused of promoting modern slavery or having unhealthy working conditions. In relation to procurement agents, the risk tolerance is set at near zero for materials and services that do not meet the Group's quality and sourcing requirements.

Strategic value drivers and risks	Sample assertions
Operational risks	**Product defects resulting from raw materials** The Board recognises the need for aggressive pricing to maintain its competitiveness, and in keeping with market expectations on similarly priced products, has adopted a higher risk appetite relating to product defects in accepting the cost savings from lower-quality raw materials. The company has set a target for production defects of one flaw per 1,000 units. Production staff may accept defect rates up to 50% above this target (i.e., 1.5 flaws per 1,000 units) if the cost savings from using lower-cost materials is at least 10%. **Inappropriate promotion** The risk of inappropriate promotion of company products by third parties only applies to third parties who provide services that result in information about company products being passed on to external parties and the public, and is highest where a third party sells, promotes or publishes material for public consumption in relation to the same. In addition, geographies with a lower Consumer Price Index represent a higher risk of inappropriate promotion. As such, detailed control activities will be focused on those providing sales services to the company in high risk geographies, whilst there will be contractual requirements on similar third parties in low risk geographies to comply with the Group code of practice for promotional activities.
Financial risks	**Free cash flow and working capital** We will limit investment in acquisitions or new investment initiatives to an amount that will enable the company to achieve its annual free cash flow target of US$ 600 million. Similarly, as we seek new business, we will maintain our working capital at 5-6% of net revenues. **Financial derivatives** The use of derivatives is restricted to hedging of financial risks only and the Board has no appetite for taking any speculative position on financial derivatives trading. Further, the company will limit its hedging activity to ordinary swaps only with counterparties rated AA and above. **Shared services and outsourcing initiatives** The company proposes to closely monitor financial metrics relating to the shared services and outsourcing initiatives around finance and IT to reduce these costs from 2% to 1% of gross revenue and from 5% to 3.5% of gross revenue respectively, over a 3-year timeframe.
Regulatory risks	**Adverse event reporting** The company has a regulatory requirement to report all adverse events relating to its products to the relevant regulator. As such, it will educate third parties but also expect timely reporting on adverse event information from such parties, enabled by signing a contractual requirement. Proactive controls will be weighted towards third parties that are most likely to come into contact with adverse event information.

A risk appetite framework thus sets a forward-looking view of the desired risk profile for the organisation and establishes a process for achieving that profile. As can be seen, the effectiveness of its design would directly determine how effectively an organisation is able to align its governance and risk management framework to corporate strategy to create strategic advantage.

Risk appetite statements, in order to be effective, must cover the full horizontal breadth of organisational activities and therefore the complete spectrum of risks. At the same time, they must have the vertical depth to granularise the implications to monitorable parameters and metrics with defined tolerances. Many of the smaller organisations at this stage have, however, chosen to keep it simple and to one high level statement.

However, larger organisations are starting to evolve multiple cascading risk appetite statements aligned to business divisions or even by risk type. For instance, an organisation pursuing an aggressive risk appetite with regard to the extended ecosystem may drill down its overall risk appetite statement to one specifically focused on third party risk. This detailed risk appetite statement in the lower level of the cascade should then, in turn, be supported by principles, policies and procedures and monitored through detailed metrics and performance measures.

Iterative discussion in the Boardroom, C-suite and amongst top executives is, in turn, key to ensuring the effectiveness of this design. Even regulators concur that it is the Board's responsibility to provide thoughtful, meaningful counsel to management and to exercise scepticism regarding the framework. The Board, together with the Risk Committee, if established, can do this by challenging the constituents of the framework and critically monitoring compliance, in an environment where the macro-economic environment, the foundation of business strategies and the impact of risks can all radically change very quickly[32]. Similarly, the independent Audit Committee would typically work with Internal Audit to holistically review this entire mechanism to ensure completeness, efficiency and effectiveness and provide independent assurance on its monitoring and management.

Establishing clarity with regard to organisational risk appetite brings many benefits:

- Providing a structured framework for understanding risk and risk performance.
- Framing discussions around business decisions in a consistent way.
- Fostering a common language and metrics that promote broad-based risk awareness and understanding across the business.
- Guiding the allocation of resources, specifically an organisation's infrastructure supporting its activities related to recognising, assessing, responding to, and monitoring risks in pursuit of organisational objectives[33].

The allocation of limited organisational resources in responding to and monitoring risks is a key consideration in today's business environment where a proportionate approach to each area of risk can help prioritise organisational actions. A robust and well-articulated risk appetite framework can bring in the organisational clarity to eliminate any subjectivity and bias in such decisions.

In order to be fully effective, the organisational risk appetite framework should be widely communicated to all relevant stakeholders across the business, rather than being held as a best-kept secret. It should align with the organisational Enterprise Risk Management (ERM) system to provide meaningful feedback on managing to the risk profile.

Risk appetite is easier to define in terms of measurable financial risks that can be monitored using specific quantitative metrics, for instance credit, market, and liquidity risks for the financial services industry. Limits can then be cascaded from top-down statements by business area and/or by and within risk type. Going forward, businesses are working on qualitative aspects, as illustrated in the example above, to include difficult-to-measure risks such as strategic, reputational, legal and business model risks through a more horizontal approach.

Relating risk appetite concepts to the use of third parties in your organisation:

- ☑ Has your Board and top leadership articulated a risk appetite statement that considers the use of third parties in your organisation?
- ☑ Are key members of your middle management and those responsible for management of third parties in your organisation aware of this organisational risk appetite?
- ☑ Have third parties been classified according to criticality and risk with regard to their strategic impact to your business to ensure proportionate focus and deployment of organisational resources to risk management and governance?
- ☑ Are specific types of risk, including strategic, reputational, operational, compliance and resilience risks drilled-down and articulated from the organisational risk appetite statement and is this reflected in documented third party responsibilities? Have you established the related metrics?
- ☑ Does your Board and members of senior leadership periodically review and challenge their view on the organisational risk appetite?
- ☑ Do accountable individuals charged with Third Party Governance & Risk Management have an active contribution to this discussion and challenge?

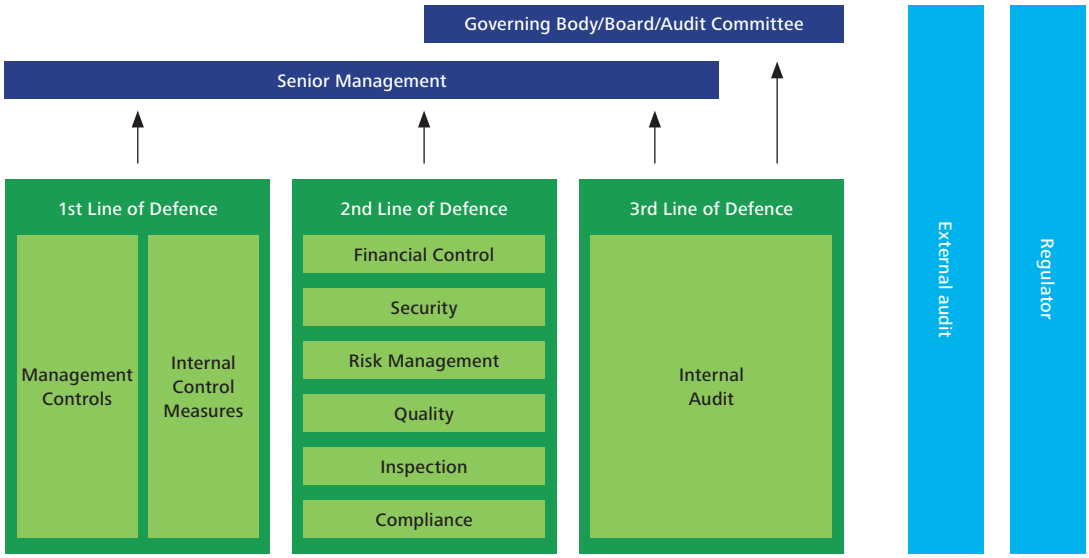
32 See also: Yoost, D.A. (2014). BOARD OVERSIGHT OF THE RISK APPETITE FRAMEWORK. The RMA Journal, 96(8), 16-23,11

33 Cited in Oliver Wyman and RMA: Conduct new survey on risk appetite. (2014). The RMA Journal, 96(9), 64-69

Reinvigorating the Three Lines of Defence:

As risk management and governance becomes an overarching strategic issue, aligned to business strategy and operations drilling down to individual business units, it is natural that people at various levels, functional areas and stakeholders will have a role to play.

The Three Line of Defence model



Adapted from EDIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41

The Three Lines of Defence distinguishes between three groups of such players:

- First Line of Defence: represents functions that own, manage and take corrective action for risks in their respective functional areas. They typically report to operating management, who in turn report up to executive leadership and are supervised by the Board.

- Second Line of Defence: represents functions that oversee and guide common risk management processes as a common organisational function, such as risk management or compliance or even the office of the Chief Financial Officer (CFO) and financial controllers. Once again, they report to executive leadership and the Board.

- Third Line of Defence provides independent assurance on risk management, typically represented by Internal Audit functions and teams, reporting typically to an independent Audit Committee.

Each of these players brings a unique set of perspectives and skill-sets to risk management and governance which can be an invaluable asset to every business, provided they are orchestrated to ensure that:

- There is complete clarity on who does what in the area of risk management.
- There are neither overlaps nor underlaps in who does what, in the context of the bigger picture.
- Limited risk management resources are deployed effectively across the organisation to address the most significant areas of concern and opportunity across the business.

The Institute of Internal Auditors (IIA) recognises that Boards, Audit Committees and C-suites are not only the primary stakeholders for the Three Lines of Defence but also best positioned and responsible for ensuring that this concept is effectively embedded across the depth and breadth of the organisation.

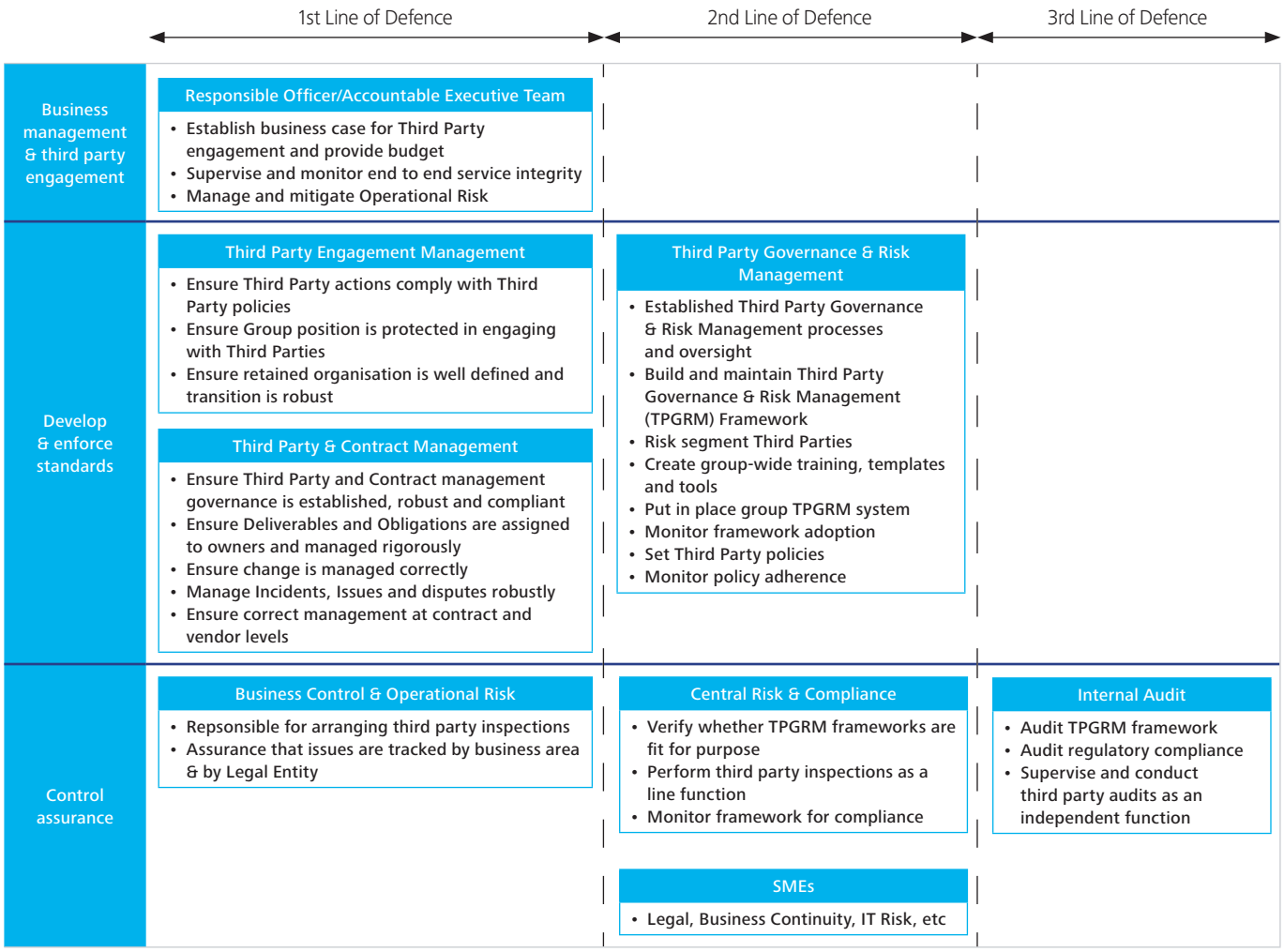
Coordination and knowledge/information-sharing across the Lines of Defence perhaps enabled through common technology and a "risk data warehouse", is a pre-requisite to establishing an effective risk management function.

If we apply the concept of the Three Lines of Defence to a risk appetite framework, the second line should provide the framework, policies, tools and standards through which risk appetite should be set and managed. The first line together with senior leadership should be responsible for setting the agenda for risk appetite discussions and implementing related decisions like monitoring of the same and triggering escalation. Internal audit, as the third line of defence should review the entire process for completeness, efficiency and effectiveness and provide independent assurance on its monitoring and management.

Set out below is an example of how the Three Lines of Defence could operate in case of Third Party Governance & Risk Management – this principle should be applied to each category of third party in the organisation to ensure good governance. This principle is increasingly being endorsed by regulators around the world, including financial regulators such as the FCA for their regulated entities being able to demonstrate the fulfilment of their regulatory obligations.

"The Three Lines of Defence principle is increasingly being endorsed by global professional bodies such as the Institute of Internal Auditors (IIA) and regulators around the world for organisations to achieve an appropriate level of governance and compliance."

Third Party Governance & Risk Management: Three Lines of Defence View



Relating the Three Lines of Defence to TPGRM in your organisation:

- How are you leveraging the concept of the Three Lines of Defence to establish and monitor your governance and risk management of third parties?
- Is there a defined coordinator or orchestrator role to ensure that the Three Lines of Defence are appropriately coordinated through periodic sharing of relevant knowledge and information?
- Are members of your operational teams aware of and trained in their responsibilities to effectively operate as the first line of defence?
- How are shared control responsibilities related to the first line of defence communicated to the related third parties, for instance through appropriate service level agreements or contractual clauses?
- Are the contracts with your third parties periodically reviewed to ensure that contractual terms are appropriate to organisational risk management and governance expectations?
- Do you have evidence of adoption of your organisational risk management strategies, policies and standards developed by your second line of defence by your third parties?
- Is your Internal Audit team equipped and trained to periodically carry out independent reviews and provide assurance over third parties?

Establishing a TPGRM framework

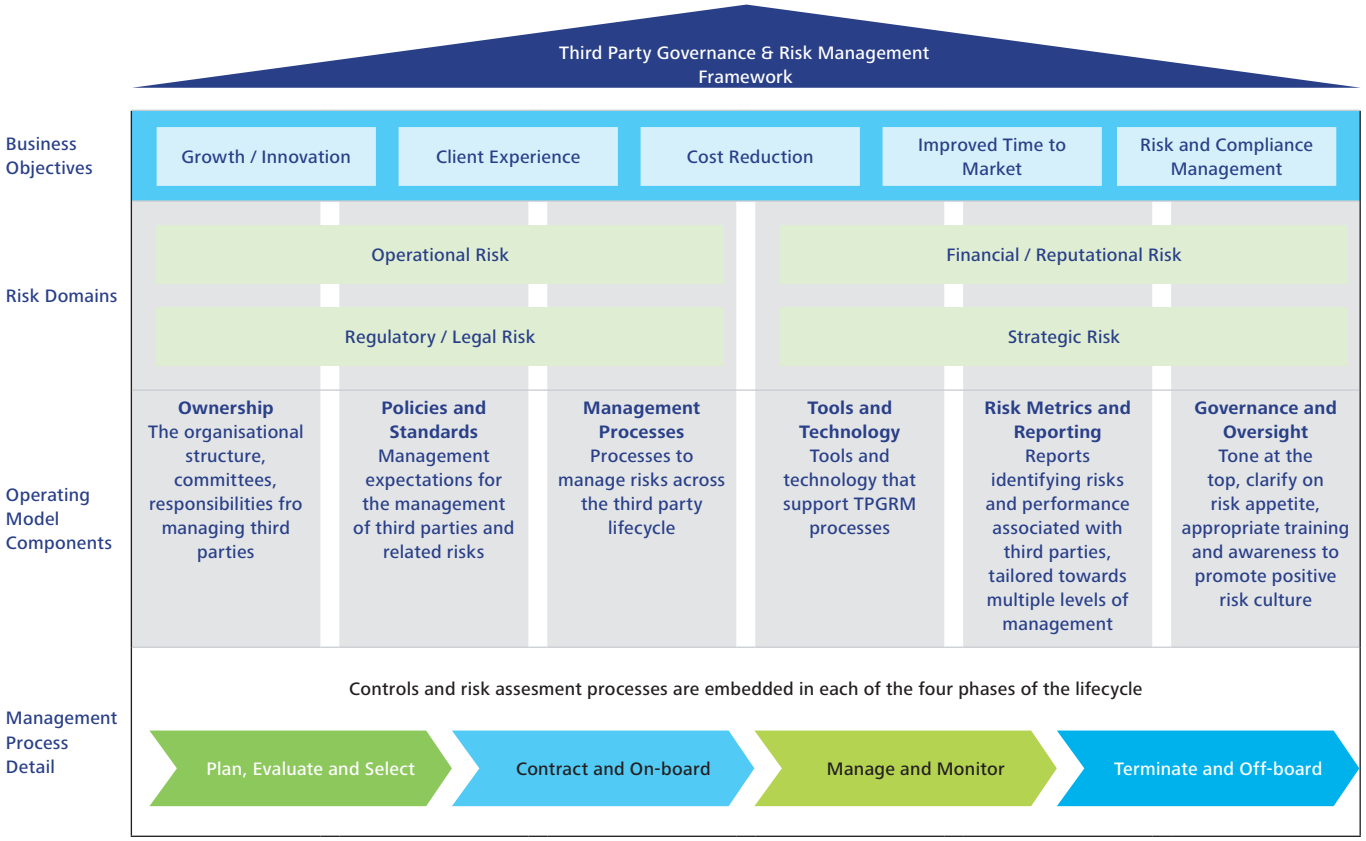
To help boards and senior management in the area of TPGRM, Deloitte has developed a framework, shown in the figure below. The framework is intended to guide management's thinking for designing a structured approach for third-party risk management, including aspects of the business objectives for using third parties; the associated risks of using third parties; the required operating model components for end-to-end risk management; and detailed management processes for enabling a sustainable, effective programme. Like many other risk domains, TPGRM requires enterprise-wide accountability, including support from the business, as well as procurement, legal, risk management, information technology, compliance, and other functions.

Although TPGRM programmes will differ for each institution, there is a common goal: to consistently and effectively evaluate and monitor third-party performance and risk. This requires good governance, as well as contributions from multiple business areas. In our view, effective businesses extend compliance and risk-management programmes to their supply chains and third-party relationships, leveraging compliance as an engine for creating and preserving organisational value.

Third Party Governance & Rick Management framework

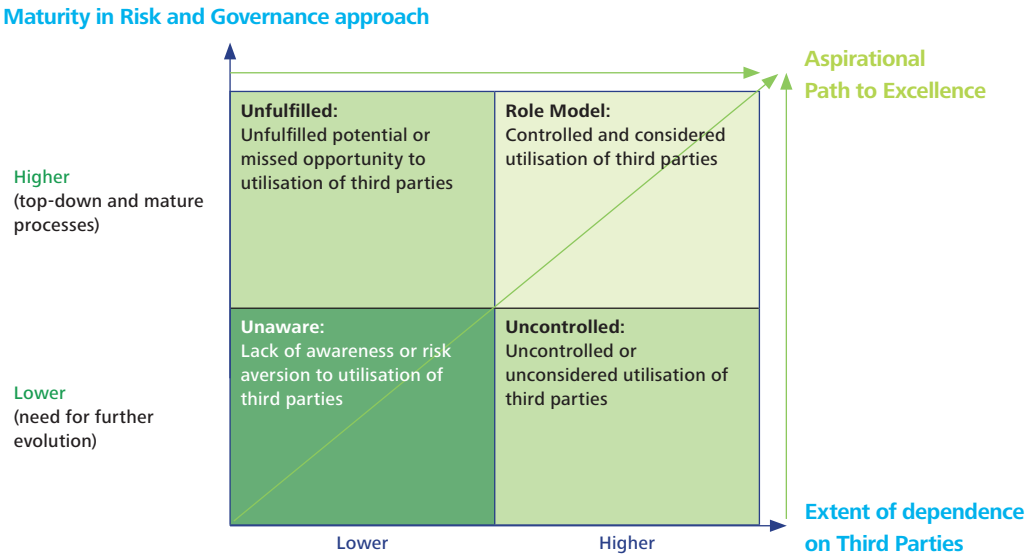
The TPGRM Framework highlights the business objectives of using third parties, the risk domains activated by using third parties, and the operating model components that must be in place for effective Third Party Governance & Risk Management. In a future paper in this series, we will explore the types of granular risk third parties may pose to organisations across different industries.

The Framework enables the assessment of the operating model components of an organisation's TPGRM Program against requirements and leading practices.



"Organisational focus on third party risk has traditionally been reactive and determined by who is driving the activity, typically procurement teams managing suppliers and vendors, or brand and IP protection teams concentrating on distribution teams and non-authorised manufacturers. Organisations are only now starting to take a holistic proactive approach to risk, covering all types of risk across all third party categories."

4. Organisational typologies and third party risk: which organisation are you?



Our experience shows that organisations can take different stances in their extent of extension of their enterprise, along a continuum ranging from lower to a higher level of dependence. On a second dimension, they may be at varying levels of maturity in their risk and governance approach to third parties.

Based on the above two criteria – the extent of dependence on third parties, and the maturity of governance processes – organisations can be mapped to a two-by-two grid set out in the figure above. This grid can be used by organisations to understand their current positioning as a first step to developing plans for reinventing themselves as the Role Models (upper right-hand quadrant) who, as explained below, are able to maximize the opportunities through the third party ecosystem, while managing the related risks.

The Role Models: The "best-in-class" organisations would clearly be those that are able to leverage their third party ecosystem more extensively with a higher planned dependence on them. They are also the organisations that are in a more mature stage of implementation of the related governance and risk management mechanisms, implemented top-down from the Board and C-suite. These organisations would be the best positioned to maximize the opportunities arising from the use of third parties, as the second most valuable organisational asset. It is likely that these organisations will involve third parties in higher value processes, considering and managing a greater level of risks in a dynamic, agile and innovative way in their pursuit of business value.

Diametrically opposite them would be the organisations that continue to have limited use of the third party ecosystem and have also not implemented or matured in their implementation of governance mechanisms and practices. Such organisations are likely to face the greatest potential challenges to erosion of organisational value and would be lucky to survive the future. Accordingly, they can be classed as the *Unaware*, who are likely to experience erosion in their profitability and organisational value, which may threaten eventual survival. For such organisations, it is likely that any limited use of third parties would be focused on lower value generating and less-risky activities and they may still face several threats and hazards in these limited pursuits of organisational value.

Organisations that have a higher dependence on third parties in their aspiration for higher organisational value, without the requisite evolution in governance mechanisms to give them the required control, are likely to be unable to manage the various threats they face as they engage with their third party ecosystem and can be considered *Uncontrolled*.

Finally, organisations that will continually remain *Unfulfilled* are those that that have limited leverage of third parties despite maturing in governance mechanisms and practices. They are likely to be perpetually facing significant opportunity loss, leading eventually to threats of value erosion and survival challenges.

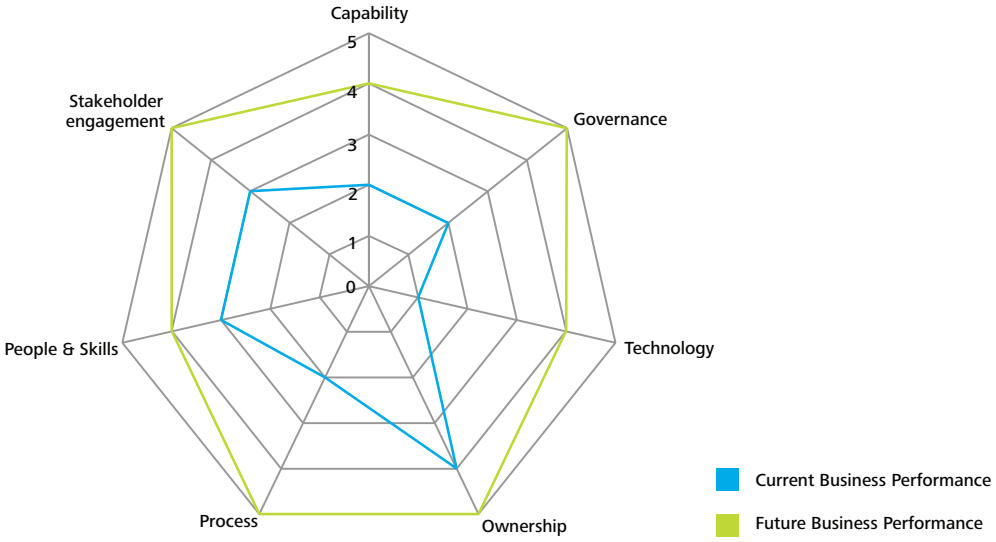
A consistent aspirational path to excellence can be seen by other organisational types aspiring to evolve as the Role Models.

5. A tool to assess your way forward

In this final section, we provide a simplified tool to enable you assess the maturity of seven key elements that, in our experience, are key to implementing a best-in-class Third Party Governance & Risk Management (TPGRM) system.

These seven elements are summarised below. Four of these seven elements relate to strategy and governance-related matters, which underpin the establishment of a mature TPGRM system, supported by appropriate technology, process and people.

Each of these seven key elements can be assessed in terms of current and target (future) ratings and presented in a diagram below to enable aspiring organisations plan out their path to excellence as they enhance the leverage from their extended enterprise.



Strategy and Governance:

- **Governance structure:** The extent to which robust governance structures are in place to manage third party risk at an enterprise wide level. Strong governance structures have dedicated teams in place at a senior level who are empowered to drive organisation wide behaviours.

- **Ownership (clarity of roles and responsibilities):** The extent to which ownership of activities for Third Party Governance & Risk Management is known by those tasked with performance and oversight of the framework. Activity ownership is kept up to date to avoid an inability to manage risk when individuals either leave the organisation or move to different roles.

- **Stakeholder engagement (awareness and commitment):** The extent to which the organisation's people are aware of Third Party Governance & Risk Management processes and to which those processes are followed. This also covers the quality of 'back-end monitoring' that is carried out to determine internal compliance with Third Party Governance & Risk Management policies. This includes both those tasked with activities and those who may become so in the future.

- **Capability:** The extent to which activity ownership is allocated to the appropriate individuals, and decision-making authority at both a transactional and framework level is allocated to individuals with the competencies and skills to apply judgement in line with business requirements and risk management needs.

People and Skills:

The extent to which the organisation's Third Party Governance & Risk Management governance structures are appropriately resourced. Individuals responsible for making decisions and setting the approach to Third Party Governance & Risk Management across the organisation have the skills, experience and seniority to do so.

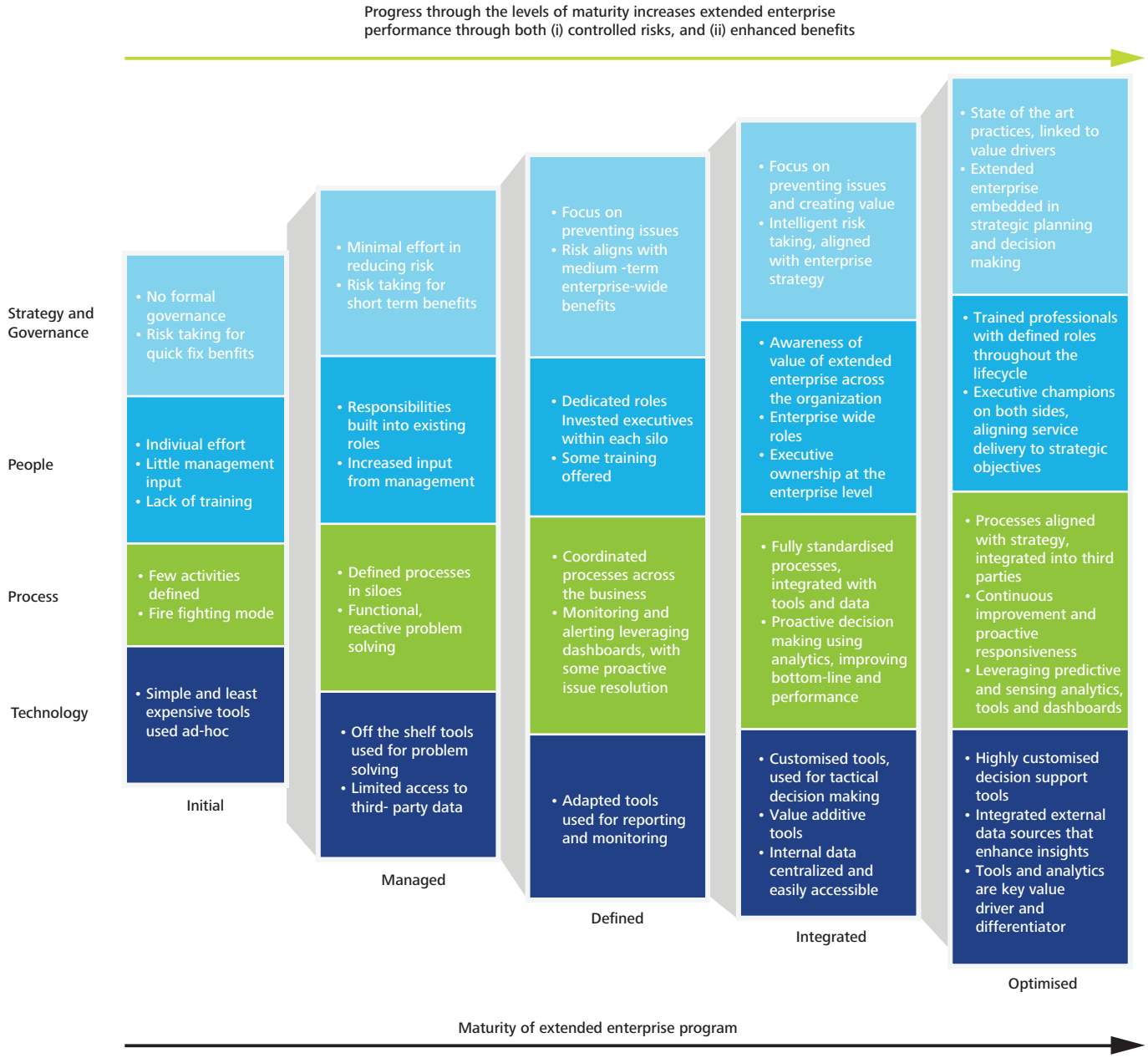
Process:

The extent to which the processes in place for management of third party risk are robust, clear and achievable. Good processes are in line with the organisation's stated risk appetite and provide a positive experience for Business Owners within the organisation, as well as for the third party.

Technology:

The extent to which the organisation has technology in place, across its operations, to facilitate the performance of the framework seamlessly from inception to exit of a third party relationship. At the very highest level, this would include the ability to manage third parties at both an engagement and relationship level. Systems are readily available and usable for those tasked with Third Party Governance & Risk Management activities.

In our experience, organisations enhance their performance in terms of being able to exploit the opportunities arising from the extended enterprise as well as managing risks better as they mature over the five stages.



About the authors

Kristian Park co-leads Deloitte's global Third Party Governance and Risk Management team as well as the Contract Risk & Compliance team in the Europe Middle East and Africa region, helping clients with third party risk, supply chain risk and contract risk. He has worked across all industry sectors, from Life Sciences, Financial Services, Energy, Sports, Technology to Media and Consumer Business. As a UK based partner, Kristian focuses on Third Party Governance & Risk Management, working with clients to develop governance frameworks to identify and manage all types of third party risks, looking at both process and technology solutions; performing inspections of third party business partners on behalf of a client; and assessing third party compliance with contractual terms and conditions. In addition, Kristian is responsible for Deloitte's UK Software Asset Management and Software Licensing teams and assists clients manage their software licensing obligations – driving efficiencies and savings.

Sanjoy Sen is a Doctoral Research Scholar at Aston Business School, UK, specialising in strategic governance related to third party risk, having earlier worked as a partner at Deloitte and another global professional services firm. He has over 26 years of experience in risk and governance in the UK, Gibraltar and various countries in the Middle East and in India. This includes assisting clients in strengthening their corporate governance mechanisms, establishing enterprise-wide risk management frameworks to support governance mechanisms and reviewing/addressing specific business and technology risks.

Danny Griffiths is a Senior Manager in our London based Contract Risk & Compliance team. He has 8 years of experience in providing assurance and advisory services to his clients. Danny leads the Contract Advisory proposition within our UK CRC team, supporting clients in the development of Third Party Governance & Risk Management frameworks. In addition, Danny specialises in leading contract compliance programmes on behalf of his clients, assessing third party compliance against contractual obligations. Danny has experience in performing third party compliance inspections across a range of third parties including suppliers, outsourcers, marketing agencies, distributors, resellers and licensees. He has experience working across a broad range of industries including Financial Services, Technology & Media, Consumer Business, Sports Business, Energy & Utilities, Real Estate and Public Sector. He has undertaken projects in multiple jurisdictions across Europe, the Middle East, Africa, the Americas and Asia.

Global Third Party Governance & Risk Management Contacts

Global Third Party Governance and Risk Management Contact			
Kristian Park		krpark@deloitte.co.uk	+44 20 7303 4110
Regional Contacts			
Americas	Kristina Davis	kbdavis@deloitte.com	+1 617 437 2648
APAC	Jimmy Wu	jimwu@deloitte.com.tw	+886(2)25459988
	Jansen Yap	jansonyap@deloitte.com	+65 6216 3119
EMEA	Kristian Park	krpark@deloitte.co.uk	+44 20 7303 4110
	Jan Corstens	jcorstens@deloitte.com	+3 22 800 2439
Country Contacts			
EMEA			
Austria	Alexander Ruzicka	aruzicka@deloitte.com	+43 1 537 00 3701
Belgium	Jan Corstens	jcorstens@deloitte.com	+3 22 800 2439
Croatia	Ivica Perica	iperica@deloittece.com	+385 (91) 6778 091
Denmark	Thomas Brun	tbrun@deloitte.dk	+4 53 610 3571
Finland	Katariina Perkkio	kperkkio@deloitte.com	+35 820 755 5301
France	Marc Duchevet	mduchevet@deloitte.fr	+33 6 77 38 24 81
Germany	Andreas Herzig	aherzig@deloitte.com	+49 711 165 5460
Greece	Alithia Diakatos	adiakatos@deloitte.gr	+302106781100
Hungary	Zoltan Szollosi	zszollosi@deloittece.com	+36 (20) 910 7644
Ireland	Eileen Healy	ehealy@deloitte.ie	+353 214 907 074
Italy	Andrea Musazzi	amusazzi@deloitte.it	+39 3466805017
Luxembourg	Jan Corstens	jcorstens@deloitte.com	+3 22 800 2439
Netherlands	Jina Calmaz	JCalmaz@deloitte.nl	+31882881871
Portugal	Joao Frade	jfrade@deloitte.pt	+351 966304388
Portugal	Miguel Cunha	micunha@deloitte.pt	+351 962744629
Southern Africa	Justine Mazzocco	jmazzocco@deloitte.co.za	+27825507521
Spain	Oscar Martín	omartinmoraleda@deloitte.es	+34 914432660
Sweden	Michael Bernhardtz	mbernhardtz@deloitte.se	+46 73-397 10 66
Switzerland	Philipp Lanz	planz@deloitte.ch	+41 44 42 16 469
Turkey	Cuneyt Kirlar	ckirlar@deloitte.com	+90 533 281 98 49
United Kingdom	Kristian Park	krpark@deloitte.co.uk	+44 20 7303 4110
	Mark Bethell	mabethell@deloitte.co.uk	+44 20 7007 5913

Asia Pacific			
Australia	Brian Bogardus	bbogardus@deloitte.com.au	+61 2 9322 7049
China	Yvonne Wu	yvwu@deloitte.com.cn	+862161411570
Hong Kong	Hugh Gozzard	huggozzard@deloitte.com.hk	+ (852) 97461695
India	Porus Doctor	podoctor@deloitte.com	+91 9820069949
Japan	Masahiko Sugiyama	masahiko.sugiyama@tohmatsu.co.jp	09 09 809 6885
Japan	Bruce Kikunaga	bruce.kikunaga@tohmatsu.co.jp	+819083477656
Korea	Min Youn Edward Cho	minycho@deloitte.com	+82-10-6361-2728
New Zealand	Aloysius Teh	ateh@deloitte.co.nz	64 21 544628
Philippines	Luisito Amper	lamper@deloitte.com	
Taiwan	Jimmy Wu	jimwu@deloitte.com.tw	+886(2)25459988
Singapore	Victor Keong	vkeong@deloitte.com	+6562248288
Indonesia	Deddy Setiady Koesmana	dkoesmana@deloitte.com	+62 21 29923100 x33555
Malaysia	Sin May Wong	sinwong@deloitte.com	+6012 212 6181
Thailand	Weerapong Krisadawat	wkrisadawat@deloitte.com	+66 26765700 x11706
Vietnam	Philip Chong	pchong@deloitte.com	+6562163113
Americas			
Argentina	Martin Carmuega	mcarmuega@deloitte.com	+54 11 4320 4003
Brazil	Patricia Muricy	pmuricy@deloitte.com	+55 21 3981 0526
Canada	Timothy Scott	tiscott@deloitte.ca	+1 416 643 8702
Chile	Christian Duran	chrduran@deloitte.com	+1 (562) 729-8286
LATCO	Maria Gabriela Castro	marcastro@deloitte.com	+58 212 2068570
LATCO	Esteban Enderle	eenderle@deloitte.com	+54 11 43202700
Mexico	Gema Moreno Vega	gmorenovega@deloittemx.com	+52 555 080 6324
United States	Walter Hoogmoed	whoogmoed@deloitte.com	+1 973 602 6517

Notes

Designed and produced by The Creative Studio at Deloitte, London. 45094A