

REPRINT

R&C risk & compliance

RISK AND COMPLIANCE ISSUES ARISING FROM THIRD-PARTY BUSINESS RELATIONSHIPS

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
OCT-DEC 2013 ISSUE



www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine



Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com
© 2013 Financier Worldwide Ltd. All rights reserved.


www.kpmg.com

EDITORIAL PARTNER

KPMG

KPMG is a global network of professional firms providing Audit, Tax, and Advisory services. We operate in 156 countries and have more than 152,000 people working in member firms around the world. KPMG LLP, the United States member firm of KPMG International, traces its origins back to 1897 and since 1994 has been a limited liability partnership registered in the state of Delaware. With more than 24,000 employees and partners, KPMG LLP is a leader among professional services firms.

KEY CONTACTS

**John Ivanoski**

Partner

New York, NY, United States

T: +1 212 954 2484

E: jivanoski@kpmg.com**Graham Murphy**

Principal

Chicago, IL, United States

T: +1 312 665 1840

grahammurphy@kpmg.com**Jeffery Hulett**

Managing Director

McLean, VA, United States

T: +1 703 286 6695

E: jhulett@kpmg.com

HOT TOPIC

RISK AND COMPLIANCE ISSUES ARISING FROM THIRD-PARTY BUSINESS RELATIONSHIPS



PANEL EXPERTS

**John Hurrell**

Chief Executive

Airmic

T: +44 (0)20 7680 3088

E: john.hurrell@airmic.co.uk

John Hurrell was appointed as Chief Executive of Airmic in January 2008 following a career of almost 30 years in the Marsh and McLennan Group of Companies. Prior to joining Airmic, Mr Hurrell was the Chief Executive of Marsh's Risk Consulting business throughout Europe and the Middle East. Having been educated in London, Mr Hurrell entered the insurance industry in 1968 and qualified as a Fellow of The Chartered Insurance Institute.

**Karina Bjelland**

Senior Managing Consultant

Berkeley Research Group

T: +1 202 480 2720

E: kbjelland@brg-expert.com

Karina Bjelland is a senior managing consultant in the Financial Institutions Practice at Berkeley Research Group, LLC. The Financial Institutions Practice advises clients and their counsel in the areas of operational risk, regulation, accounting and finance and serves the needs of hedge funds, funds of funds, private equity funds, alternative investment funds, investment advisers, broker-dealers, insurance companies and banks. Prior to joining BRG, Ms Bjelland held various positions in the areas of financial institution supervision and regulation, and securities litigation consulting.

**John Ivanoski**

Partner

KPMG

T: +1 212 954 2484

E: jivanoski@kpmg.com

John Ivanoski serves as the Leader for KPMG's Regulatory practice. He has over 25 years experience providing audit and risk advisory services to global organisations. Mr Ivanoski has extensive experience in managing large global projects related to regulatory and risk transformation, third-party risk management, enterprise risk management, operational risk including third-party vendor management, and target operating models. He also served as a US Peace Corps Volunteer in Malawi, Africa assisting in the development of a credit cooperative system.

RC: Could you provide a general overview of the potential risk exposures that may arise when dealing with third-party business partners and vendors?

Bjelland: The list of potential risk exposures is quite extensive. There are privacy risks, transaction risks, technology risks, credit risks, compliance risks and risks to reputation. In addition, there are numerous other specific issues to consider that fall under the more general categories such as copyright and patent laws, and concerns related to ownership, liability, consumer protection and compliance monitoring and records retention. Finally, there are risks specific to an industry or type of business. Third-party risk exposure is relevant to all industries, not just financial, and each one of these has their own additional industry-specific risk issues to consider. For example, an oil company has to consider the additional risk of pollution-related liabilities in their contracts with third-parties, such as drilling contracts.

Hurrell: Recent research would suggest that the majority of the value chain in most companies is now provided by outside entities such as subcontractors, suppliers and distribution networks. This means that more than half the risk to the brand or reputation of a company is outside its direct control and often operating in countries which are relatively unfamiliar to the principal. This will

have been very different only a few years ago, and some companies have been better at making the adjustments to risk management strategy demanded by their changed business models than others.

Ivanoski: Third parties such as service providers, alliance members, consultants and suppliers can expose their business partners to a range of risks. While specifics depend on the industry, service or product being offered, potential third-party risks include the following. First, reputational risk from delivery of substandard products and services, disruption of services, and failure to meet the expectations of customers. Second, compliance risk from violations of laws and regulations such as consumer protection, securities filings, anti-bribery and corruption (ABC) and anti-money laundering (AML), or nonconformance with internal policies. Third, operational risk related to the potential failure of people, processes or systems. Fourth, credit risk related to services and transactions involving extension of credit such as origination, underwriting, servicing and processing. Finally, strategic risk from failure to implement business decisions or poor execution of those decisions.

RC: In what ways can third-party violations and misconduct negatively impact a company's brand and reputation? Have there been any notable examples in recent years?

Hurrell: There are multiple examples in the consumer clothing and food industries, such as dangerous sweat shops and horse meat. The challenge here is the prevalence of all forms of social media closely connected with traditional news media which potentially turns every human being on the planet into a news reporter. The traditional media will seek brand connections and the impact will be instant – often faster than any company's contingency plan can respond.

Ivanoski: A company's reputation can be affected negatively if its third parties do not deliver products and services at the right level of quality, and in line with contracts, policies and customer expectations. This failure can produce a variety of negative effects for the company, including reputational risk through brand impact and unfavorable press, as well as regulatory inquiries, fines and other enforcement actions. In the financial services industry, the Consumer Financial Protection Bureau (CFPB) has handed out enforcement actions to several banks whose third parties were, in the eyes of regulators, causing consumer harm due to sales of add-on products that did not benefit the customer or where customers were incorrectly foreclosed on. A critical point to note is that, along with the reputational impact of the enforcement actions, there were significant monetary penalties.

As a result of notable high-profile issues, banks have made significant enhancements in third-party risk management.

Bjelland: The public assumes that you have vetted a vendor or service provider when you choose to enter a business relationship with them. They become an extension of your company or image and you may become associated with

"A company's reputation can be affected negatively if its third parties do not deliver products and services at the right level of quality, and in line with contracts, policies and customer expectations."

*John Ivanoski,
KPMG*

their conduct, whether positive or negative, even if you were even aware of it prior to the event occurring. Recently, a group of banks sued a third-party payment company after the customers' personal data was breached. Unfortunately, this has happened quite often over the last few years and has damaged companies' brands because customers lose faith that their information will be protected, and customers may then choose not to continue the business relationship. In addition

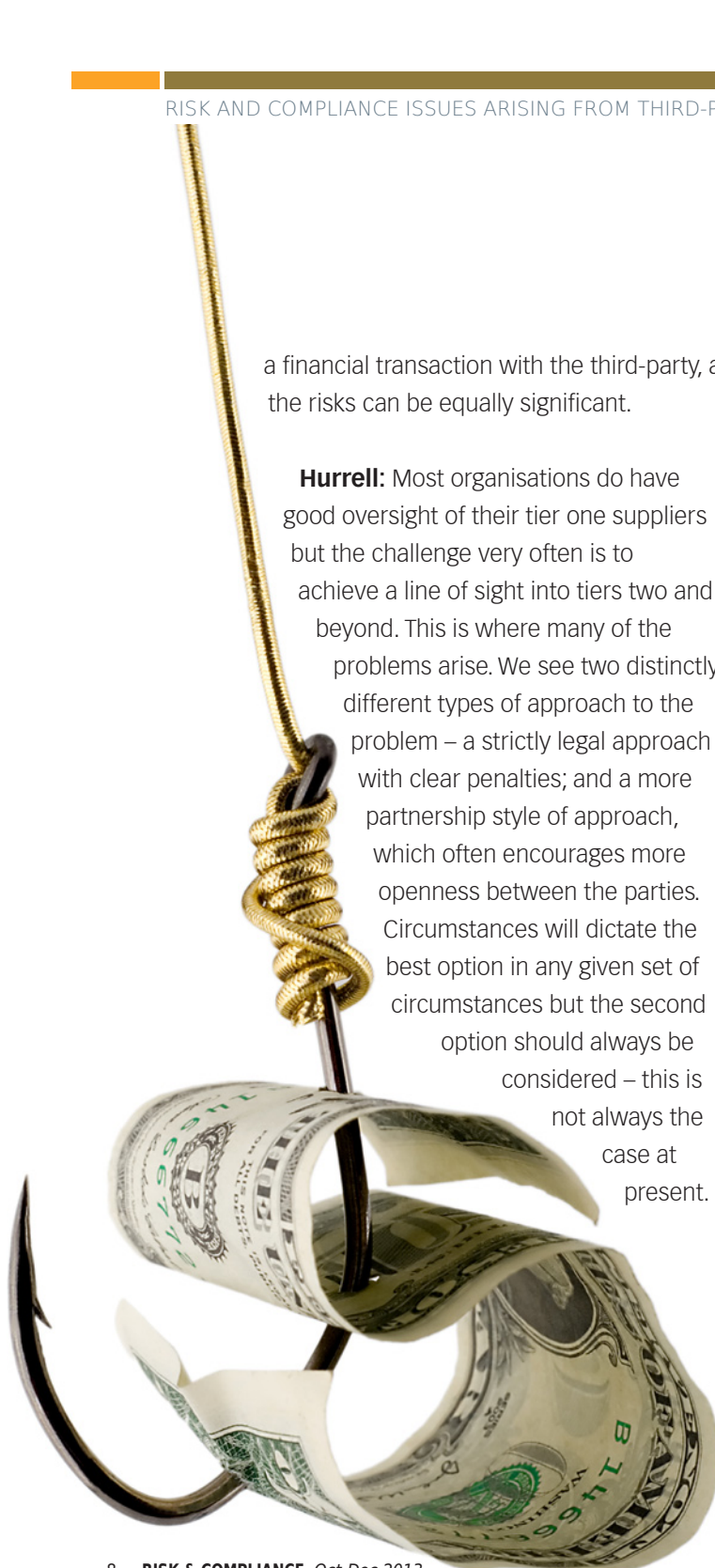
to reputational damage, there can be significant financial costs associated with this sort of incident, including litigation costs and reimbursement costs to customers. Currently, the Office of Comptroller of the Currency (OCC) and Consumer Financial Protection Bureau (CFPB) are looking into concerns that JP Morgan may have misled customers who purchased credit cards with identity theft protection through a third-party vendor.

RC: Audits, inspections, and other processes enable companies to evaluate third-party controls and compliance measures. What steps can a company take to strengthen the due diligence it performs on third-parties?

Ivanoski: Inventorying and assessing third parties based on the risks they expose the business to allows for a risk-based approach to management of third parties, which is vital given limited resources. A due diligence process that quickly identifies the risks a third-party exposes the organisation to, and directs the appropriate oversight function to exercise-focused control, is essential to avoid information overload. Each third-party may have a different combination of risks, requiring an appropriate blend of risk management activities from the oversight functions. Clarifying roles and responsibilities across the oversight functions, business lines and internal audit assists

with ensuring the appropriate risk management functions are aware of the risk and managing it accordingly. Executing contracts that clearly set out requirements, expectations and responsibilities, and provide the ability to conduct on-site reviews, collect relevant risk and performance information, are key to managing the risk third parties expose the organisation to. The focus of on-site reviews should include understanding how well the third-party's risk management functions work, how it monitors and manages compliance risk and how well it is performing.

Bjelland: A company should thoroughly evaluate third-party service providers prior to entering into a business relationship, and should also continue to regularly monitor controls and compliance measures throughout the relationship, and ensure that the third-party shares the same goals and adheres to the same policies. Due diligence on the third-party should include researching their reputation, checking references, and using all available resources of information such as state attorneys general or the better business bureau. If a third-party organisation is new, a company should exercise additional caution. It is also critical to review a third-party's financial information and insurance coverage. Audit and regulatory reports should be reviewed, such as an SAS-70, if one is available. The evaluation should be just as thorough as if the company were to enter



a financial transaction with the third-party, as the risks can be equally significant.

Hurrell: Most organisations do have good oversight of their tier one suppliers but the challenge very often is to achieve a line of sight into tiers two and beyond. This is where many of the problems arise. We see two distinctly different types of approach to the problem – a strictly legal approach with clear penalties; and a more partnership style of approach, which often encourages more openness between the parties. Circumstances will dictate the best option in any given set of circumstances but the second option should always be considered – this is not always the case at present.

RC: Employees at third-party organisations should be encouraged to report compliance or ethics violations. What processes can firms put in place to ensure this occurs, and to remedy any shortcomings at third-party organisations?

Bjelland: Make sure that reporting policies are clearly and regularly communicated to third-parties and employees through training and other measures, and establish a channel for employees to easily escalate any issues or ask questions, such as a confidential hotline devoted to answering questions related to potential issues and for reporting issues, such as a whistleblower hotline. Companies should encourage employees to timely and accurately report concerns, and ask questions early on. It is also important to provide protection against employee retaliation as this can discourage employees from speaking up. If there are shortcomings at a third-party, perhaps the company has resources that can be utilised by the third-party, whether technological resources or staff resources. However, if a third-party is not adequately equipped to handle the increased business or services required of them in the proposed business

arrangement, the company should seriously consider whether they should really be entering into that business partnership.

Ivanoski: Depending on the sophistication of the risk management infrastructure at the third-party, there may or may not be a mechanism, such as a hotline, to report compliance or ethics violations. This should be considered during the due diligence review. Third parties should, where appropriate, be required to implement ethics and compliance hotlines, for example, in line with better practices to ensure that there is a reporting mechanism for employees. Training the third parties' employees on the client's internal policies and procedures, expectations, and requirements drives an understanding of what is expected, keeps employees abreast of changes, and allows them to assess and decide on violations and shortcomings. An appropriate monitoring problem should ensure employees are adhering to internal policies and procedures.

RC: Do any particular risks emerge when working with third-parties in the emerging markets? What steps can firms take to reduce potentially damaging exposures in these regions?

Hurrell: The starting point is to understand the likely differences in approach locally on critical issues such as ethics, employment practices such as health and safety, respect for intellectual property, the legal system and local infrastructure. Many firms will work through a strong local partner rather than simply trying to impose 'head office' standards and procedures locally. The challenge is to operate according to local best practice whilst recognising

"Many firms will work through a strong local partner rather than simply trying to impose 'head office' standards and procedures locally. "

*John Hurrell,
Airmic*

that western media will always apply a western lens to their reporting of any failures. In particular this will always take place where a big consumer brand is involved.

Ivanoski: Operating in emerging markets exposes companies to country risk – the risk that economic, social and political conditions and events in a foreign country will adversely affect the company's financial interests. In today's environment, the most

notable risk facing organisations operating outside the United States include violations of anti-bribery and corruption (ABC) laws, and requirements under the Foreign Corrupt Practices Act (FCPA). Given the complexity of US laws and regulations, a growing number of US companies are retaining the regulatory and compliance responsibility in outsourcing/offshoring relationships, and pricing the requisite oversight activities into their agreements because the risk of non-compliance is perceived to be too great. Steps that can be taken to manage this risk include: incorporating specific risk assessment criteria for offshore characteristics; retaining knowledgeable skilled resources to draft contract provisions and understand the legal jurisdictions where the third-party is based; conducting on-site reviews to determine quality of management and staff, and gaining a firsthand understanding of the culture and business operating conditions.

Bjelland: The laws and ways of conducting business are clearly different in other regions, especially emerging markets, where some regulations may not have even been established yet or are not clearly defined. It is hard to avoid using a third-party when entering a new market because a company should hire or consult with individuals who have experience in that region and are familiar with the laws and potential problems that could occur by doing business there. There are many issues to consider in these markets. Foreign

Corrupt Practices Act (FCPA), money laundering concerns, and employee safety are just a few of the issues to consider. FCPA and other legislation require companies to perform due diligence on foreign third-party business partners, and the Department of Justice (DOJ) and the Securities & Exchange Commission (SEC) have fined US companies for not performing sufficient due diligence on these partners. Choice-of-law and jurisdictional issues – and the possibility of dealing with foreign courts – need to be considered when working with international third-parties and drafting contracts. Political and socio-economic factors can increase the difficulty of conducting business in certain regions. Additionally, a company needs to consider economic and trade sanctions, and potential concerns related to terrorist financing, bribery of government officials or commercial bribery, risk of child labour, and product safety concerns. A company should consider whether all of these risks outweigh the benefits of doing business in that region. Also, if the business model of the company and economies of scale permit, perhaps there should be a trial period or testing of only limited products or services before fully committing to that region. As an example, outsourcing to offshore contractors by financial institutions has increased in recent years because of savings due to lower wages and other reduced costs. However, instances of fraud and identity theft have increased. Offshore outsourcing of data services or call centers occurs

frequently and both pose risks to customer and other confidential information.

RC: Have you seen, or do you expect, any regulatory or legislative changes to affect third-party relationships in your region?

Ivanoski: In November 2012 the Securities and Exchange Commission (SEC) and Department of Justice (DOJ) released guidance on what is expected in developing and monitoring an effective ABC compliance program. Further, the SEC has established a unit focused on FCPA, and continues to pursue companies, officers and directors when violations are suspected. The US federal bank regulators have extensive examination guidance on third-party risk management and they conduct comprehensive examinations in this area. Further, they are planning to release updated guidance on the management of third parties in the near future. Initial expectations suggest they may expand the term 'third-party' to include a wider swath of entities, such as suppliers, alliances, joint-venture partners and vendors, as well as require more reporting on third-party risk to the board. In addition, under the Bank Service Company Act, the U.S federal bank regulators comprising the Federal Regulated Institutions Examination Council (FFIEC) have authority to examine banks' third-party service providers. In the financial services industry, public

consent orders and other enforcement actions related to regulatory violations have occurred with a resultant increase in regulatory scrutiny of these relationships. This focus has led to an increase in control and oversight of third parties by banks. Regulators have sent a clear message that banks can outsource operations, but can't outsource responsibility for the conduct of their third-party providers.

Bjelland: Both new regulations and increased enforcement of existing legislation will increase the importance of third-party oversight. A company's liability for the actions of their third-party relationships is becoming increasingly defined through actions by regulators and in litigation, and this process will be ongoing. Last year, a landmark \$25bn settlement was reached between five large banks and 49 state attorneys general which requires lenders to boost their oversight of third-party vendors. In addition, the CFPB has new mortgage rules that will become effective in January 2014 and will affect third-party business relationships. The news also reports the Federal Deposit Insurance Corporation (FDIC) and DOJ have been reaching out to banks over concerns related to certain online lenders. There have also been numerous recent legislative efforts related to protecting individuals' privacy, which becomes more of a risk when third-parties are involved.

RC: When working with a third-party, management should ensure that the specific expectations and obligations of both the firm and the third-party are outlined in a written contract. What risk-related issues should firms address when structuring such a contract?

Bjelland: This phase is crucial because poor planning and consideration of potential scenarios in the early phases of an agreement can lead to increased risk. The contract needs to address who is responsible for specific tasks, all rights and obligations for both parties, and also indemnification, business continuity planning, dispute resolution, locations, use of equipment, and ownership of data and IT contracts, for example. A company should review guidance from their relevant regulators, such as the FDIC or OCC in the case of financial institutions, on third-party business relationships. The contract should include a detailed business plan, service level agreements and sections on audits and monitoring and vulnerability assessments. The board and key management should be involved in the entire process. The contract should clearly define what the exit strategy is if the relationship does not work out, including the timeline and cost. A company should hire experienced staff, or make sure that

the third-party has experienced staff, in key areas such as IT and security. They may cost more but it could save money in the long run. The costs associated with maintenance of software and other items should be considered as well. An example of a potential concern is that a company could enter into a contract with a domestic third-party service provider without knowing that the third-party is in

“An example of a potential concern is that a company could enter into a contract with a domestic third-party service provider without knowing that the third-party is in fact subcontracting some of their services offshore.”

*Karina Bjelland,
Berkeley Research Group*

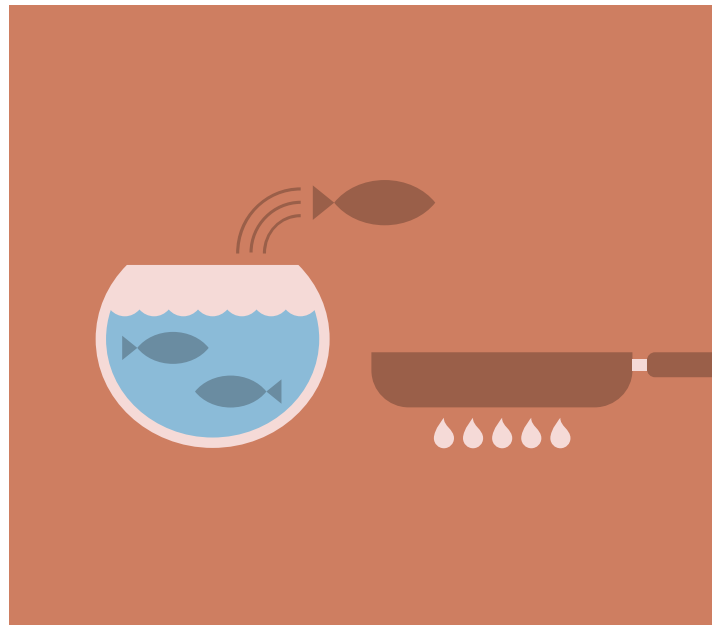
fact subcontracting some of their services offshore. This is one of the matters that should be considered when drafting an agreement and should be reviewed during audits.

Ivanoski: Current financial services regulatory guidance, for example, outlines a variety of topics banks should consider when entering into third-party contracts, including scope of the arrangement, responsibilities, performance measures and benchmarks, information confidentiality and security,

compliance with specified laws and regulations, access to information for performance and risk management, the right to audit third parties and their subcontractors, and business continuity. Companies in all industries need to be comfortable the initial perceived benefits of a proposed relationship will not be offset by reputational risks and non-compliance costs. Performance under the contract should be defined, but as noted, appropriate oversight and management controls should be established, including dispute resolution, indemnification, cost and compensation for non-compliance with contract and default and termination.

Hurrell: Contracts must focus on standards and quality and all other aspects which could impact on reputation. However, contracts should be drafted in a way that emphasises the partnership aspect and encourages open dialogue. For example, penalty clauses should usually only kick in if there has not been a voluntary disclosure of a problem within a prescribed period.

RC: Organisations should maintain adequate oversight of third-party activities and the quality control measures governing products and services provided. What features should be included in a firm's monitoring program?



Ivanoski: As a rule of thumb, third parties should be managed as if they were an internal department of the organisation. Assessing the quality of the products and services delivered by the third-party on a regular basis assists with understanding their performance relative to the contract. Monitoring the contract's specific terms and conditions is a way to ensure agreed-upon performance, control and risk management. Monitoring of controls through on-site reviews; assessing changes to the business; reviewing policies and training requirements; and assessing the resiliency of the third-party with regards to its financial health and its ability to withstand business disruption, are activities that drive effective risk management.

Bjelland: The first step is to fully understand the third-parties' business lines and products. If a company does not understand how a product or service works at the third-party, they need to make sure that they become educated prior to beginning the relationship because a company cannot monitor something they do not understand. An example could be how specific software works, or how confidential information is encrypted and stored, or where data is housed. A lack of knowledge could lead to customer complaints or worse scenarios down the road. The features that should be included in a monitoring program are operational audits, vulnerability assessments, fraud monitoring and quality checks and controls. The policies and procedures for monitoring should be consistent across the board. A company should ensure that training of employees is adequate and

experienced staff is employed, especially in key areas such as IT and security. These employees may cost more but it will save money in the long run. Examples of insufficient monitoring include recent cases where third-parties performing underwriting led to increases in delinquencies, or weaknesses in security led to information being hacked.

Hurrell: There needs to be clear terms in the contract between the parties stating that appropriate standards of quality – safety and environmental protection, for example – will be achieved by the contractor. This requirement should be stated as an expectation of the contractor, but the principal should ensure that it does not assume responsibility. The firm should obtain assurance from contractors that standards are being achieved. Also, there should be confidentiality requirements in the contract. **RC**