Risk management in the real world

When monitoring third party risks, it’s important that entities focus on value creation as well as value protection.

BY JIMMY CROWLEY

Outsourcing is increasingly a key strategic decision for many businesses allowing them to focus on core corporate activities. However, when things go wrong in third party relationships, companies may be exposed to significant reputational, regulatory, strategic and financial risks. There are two notable recent examples of high-profile third party failures in Ireland:

- The Central Bank of Ireland imposed fines on financial institutions in relation to the governance and control of outsourced services delivered by third parties; and
- In 2018, a restaurant chain in the UK was forced to close more than 560 of its 900 outlets as “operational issues” at a new distribution partner left deliveries “incomplete or delayed”. This is estimated to have cost the restaurant chain in question £1 million per day in lost sales.

In 2016, the Central Bank of Ireland warned that poor management of third party relationships is putting banks at risk, citing “very serious failings” in relation to the governance of these arrangements and brandishing some cases as “astonishing”. Specific criticism related to poor management of outsourced arrangements, lack of oversight and a lack of engagement and challenge from boards.

Extended enterprises

The operational environment of many companies has expanded to include outsourced arrangements, lack of governance and control of third party risks as they arise.

- Companies increasingly need to move toward a holistic approach to EERM that emphasises value creation as well as value protection.
- They are concentrating on firefighting rather than maximising the benefits that can arise from well-managed third party relationships.

Extended enterprise risk management (EERM) is the practice of anticipating and managing exposures associated with third parties across the full range of operations, as well as optimising the value delivered by the third party relationships. The risk management landscape is often fragmented and decentralised. Many companies have not agreed and documented their risk appetite. They may approach third party risk management on an ad hoc basis, addressing prominent areas such as cyber risk and regulatory compliance as they arise.

Crucially, many companies do not have a broad pan-company view of all current third party engagements and the associated risks. A common theme that emerges here is of a lack of ownership of risks across the company. For example, despite the increasing focus on risk management, some companies still do not have a dedicated risk officer. Additionally, many companies are not appropriately utilising the three lines of defence to manage risk and drive performance.

The first line of defence is the business unit, which owns the third party relationship and is accountable for managing associated risks in alignment with policies and procedures. The second line of defence is a centralised governance programme for extended enterprise risk management, which is responsible for establishing and enforcing policies/processes to ensure that third parties are managed consistently by the business. The third line of defence is internal audit, which is charged with administering a robust audit programme aligned to the most critical extended enterprise risks and controls as well as performing independent assessments.

In addition to underinvesting in the three lines of defence, many companies focus excessively on quantitative metrics – contract income and expenditure, for example – when engaging a third party. When assessing third parties, companies should always include appropriate qualitative metrics – vendor quality, technical capabilities, vendor risk profile, control environment, and ability to drive performance, for example.

By not having a defined EERM framework in place, many companies are concentrating on firefighting rather than maximising the benefits that can arise from well-managed third party relationships.

Driving value

Companies increasingly need to move toward a holistic approach to EERM that emphasises value creation as well as value protection. This typically involves establishing a systematic and proactive approach to managing risks across the third party lifecycle and, in so doing, unlocking value and improving business performance.

An operating model for implementing and integrating the various components of risk management across the third party relationship lifecycle forms the foundation of this approach. To be fully effective, such models must be aligned to the company’s overarching risk appetite and risk management framework. The model should link the individual components of risk management to agreed and documented business objectives and the company’s risk registers.

Four cornerstone capabilities

Many companies believe they cannot take an end-to-end approach to managing the extended enterprise because securing executive sponsorship and getting people to take ownership can be an uphill battle. Additionally, many businesses think the task is too vast and they do not have the expertise to implement and integrate the various components of risk management across the third party relationship lifecycle.
and resources to build, execute and sustain a comprehensive third party oversight programme.

In our experience, these barriers are more perception than reality. It is neither necessary nor possible to do everything at once. Companies should consider some practical steps to take toward establishing an EERM programme or evolving an existing one. Many companies can get a sense of what those steps might be by considering the extent to which they have developed the following cornerstone capabilities.

**Strategy and governance**

This involves the creation of an agile and flexible governance model.

- Is there a defined and documented strategy and governance model for managing third party risk?
- Is there a defined policy to assess third party requirements prior to entering into relationships?
- Are third party risk management activities linked to value drivers, agreed and documented?
- Have you identified, agreed and documented critical key performance indicators (KPIs) for all third party relationships?
- Have you agreed and documented how third party KPIs will be reported and monitored?
- Are there defined processes in place to identify new and emerging third party risks?

**Technology**

This involves using data and analytics to make informed decisions.

- What tools and technologies are employed to make informed decisions about third party performance?
- What transactional data are you entitled to access?
- Does the company’s IT and systems support KPI monitoring, reporting and performance assessment?

**Factors to consider in assessing your third party risks**

The complexity of the extended enterprise and resource constraints are no longer sufficient reasons to avoid taking an integrated approach to third party risk management. Wherever your company stands at present in relation to EERM, some practical steps can be taken now to establish an EERM programme or to move your existing risk management model to the next level. The following factors should be considered.

**Strategy and programme**

This involves the development of EERM solutions to assess, design and implement a strategically aligned extended enterprise programme. These may include:

- Conducting an enterprise-wide strategic third party risk assessment; and
- Developing the governance and operating model for EERM including KPIs, reporting and monitoring mechanisms.

**Evaluation and continuous monitoring**

This involves the selection and application of a suite of solutions to measure third party and proactively sense and respond to extended enterprise risks and opportunities. These may include:

- The selection of quantitative and qualitative metrics/KPIs;
- Third party risk assessment processes; and
- Contract compliance mechanisms.

**Technology enablement**

This involves the selection and application of technology solutions to transform and continuously enhance EERM. These may include:

- Systems design and deployment;
- Data analytics; and
- Reporting protocols.

**Conclusion**

Effective EERM programmes allow companies to align third party risk management to strategic objectives and deliver enhanced returns on investment by emphasising value creation as well as value protection.

Crucially, there is no ‘one size fits all’ EERM model or programme. Each company faces unique challenges and therefore, EERM programmes tend to be bespoke by their nature. Time spent on EERM programme design is rewarded in the longer term.

Finally, successful EERM programmes are continuously reassessed to ensure that the model being applied remains appropriate at all times.

---

**Spotlight**

Jimmy Crowley ACA

Jimmy is a Senior Manager in Risk Advisory in Deloitte Ireland.