Vendor risk management

Strategic and operational dependency on third parties is commonplace in organisations across all sectors. The question for chief audit executives (CAEs) is how to ensure that meaningful assurance is provided with often limited audit resource.

Organisations often use their own language as this topic is rich in terminology, so for clarity this briefing begins with a lexicon:

- **Vendor/supplier:** A person or organization that provides a product or service, vendor can be B2C (business to customer) or B2B (business to business) they are typically closest to the end customer in a supply chain, suppliers are B2B.
- **Outsourcing:** Obtain a service by contract from a supplier/contract out.
- **Procurement process:** Method of purchasing from ordering, receipt, review and approval.
- **Contract management:** Process of creating, executing and analysing contracts.

The following are largely interchangeable terms and definitions merge:

- **Vendor risk management:** Often focus on cost, quality and value.
- **Supplier relationship management:** Assessing contracts for strategic value, maximising interactions and renewal evaluation.
- **Third party management:** Monitor and manage interactions with external parties.

This paper uses the term third party to discuss themes related to the use of external party (vendor/supplier) to provide services, whether as a simple contractual arrangement for a service or fully outsourced.

In or Out

There are always two sides to a coin and there is an argument for keeping all activities in-house and avoiding third party risks. Regardless of when internal audit joins the party, by invitation or gate-crashing, this debate should be the starting point; understanding the rationale will provide risk insight and enable targeted assurance.

Internal audit should understand how the decision has been made by reviewing the business case, analysis of the costs and risks associated with the activity. Consideration should also be given to who made the decision and whether they had appropriate authority. The ability to exert demanding controls, maintain flexibility and protect knowledge may be of greater value than potential cost savings, particularly where highly confidential or sensitive data is involved. Ever increasing cost pressures, regulatory requirements, stakeholder expectations and innovations have meant that the use of third parties is a common occurrence. This is typically because providers can benefit from economies of scale that individual organisations are unable to achieve or specialise in particular skills, for example internal audit co-sourcing for IT skills.

This is a high fraud risk activity and care should be taken to ensure that conflicts of interest are declared.

Transparency is essential to ensure that contracts are awarded to appropriate parties, not to acquaintances or out of convenience having previously used a particular supplier. In 2017 critics questioned the decision by the Ministry of Justice to award a new contract to G4S when they were being investigated for fraud related to a previous contract, time will tell if they are the next Carillion or a valued strategic partner.

If the use of third parties is prevalent there may always be assurance gaps in this area. As chief audit executive (CAE) there may be creative opportunities to add value such as developing a decision matrix that ensured risk, control and governance was adequately addressed alongside commercial factors. An example of this is the gateway approach developed by the Office of Government Commerce (now Crown Commercial Services), with independent reviews at critical stages of the procurement lifecycle.

Due diligence

Typical due diligence would include financial performance and references from other clients depending on the nature/riskiness of the service. CAEs may consider engaging internal audit in a consultancy capacity at this stage if the business does not have the skills to do this effectively; care must be taken as auditors cannot then audit for assurance purposes within a year.

It is important that a comprehensive risk assessment is completed before the third party is engaged. Internal audit may be required to facilitate this if risk management is immature within the organisation. This enables the business to make informed decisions about their risk exposure, it may be that a preferred vendor has issues that need to be addressed and supported rather than excluding them from the selection process.

Internal audit can also exploit risk assessments to target activity during engagement planning and also to validate that risks have been refreshed ideally on a regular basis, at a minimum when changes occur that impact the service.

Appraisal of vendors using due diligence principles should extend beyond initial selection and be part of an ongoing management programme. Quarterly reviews to assess their financial position, performance, media activity, informal information and other pertinent factors could identify early indicators to problems enabling management to take action; issues such as movement on the board, restructuring, job losses, delays in new developments, taking on another large client or lax data security. In organisations where these multi-discipline meetings take place it may be useful for internal audit to attend as an observer to ensure risk evaluation is given sufficient attention.

Contracts

Contracts are often regarded as one of the most important tools in managing third parties. Audit findings that a service is being provided without a signed contract, or signed by someone without appropriate authority can lead to a flurry of activity but what actually changes, some legal standing if things go awry but does it lead to better risk management?

Much like the space suit an astronaut wears, contracts provide a level of protection to organisations, but they are fragile. There is a compromise between control and usability, imagine an astronaut so restricted that they couldn't perform a spacewalk.

Aside from the legal requirements and details of the service itself, it is important that a contract always

includes:

- Right of access clause ensures the right to audit or review the activities of the third party, their procedures, systems, premises and accounts in relation to open book arrangements – without this agreement any assurance work undertaken will be in a parallel universe compared to the reality for the third party.
- Service level agreements provide a definitive measurement of satisfaction that should be tied to payment schedules - assurance can be provided over the accuracy and timeliness of data used or a more informed review could evaluate their appropriateness and the robustness with which they are challenged - cosy relationship, targets always achieved, fraud opportunities?
- Relevant standards, such as ISO27001 (information security), ISO14001 (environmental management), ISO9001 (quality management) and service specific standards provide a platform for internal audit to provide assurance, requiring documented procedures and policies.

If not already available as business information, CAEs may consider undertaking an inventory of third parties to produce a risk profile from which to base internal audit activity. Vendors could be assessed based on risk factors such as the value of the contract, regulatory impact, criticality of task, anti-bribery and corruption potential, resilience plans, data sensitivity and financial security. Where an inventory is not available the business should be advised of the risks they are exposed to such as failing to adhere to renewal or termination notice periods and potential fines.

In order to comply with the Public Contracts Regulations 2015, procurement in the public sector is transparent by design and a paper mountain of policies, procedures and guidelines are readily available. Commentators argue that this has created a risk averse culture and a propensity to use incumbent suppliers to avoid protracted on-boarding processes. The Carillion insolvency debacle in January 2018 highlighted this as the public sector was left exposed on high profile projects and ongoing site management. A public inquiry was launched and auditors across sectors should review the scope and ask the same questions of their own organisations to mitigate where possible becoming a similar case study.

Risk themes

Organisations are exposed to an additional layer of risk when engaging with external parties to provide services. These are heightened when fully outsourced as responsibilities are transferred in addition to the provision of the service itself. For example a company may contract ABC Ltd to provide security staff for particular duties and shifts or may out outsource the management of physical security to ABC Ltd at which point they determine what is required, the shift patterns etc. CAEs must always be mindful to remind management that the risks associated with the service are never transferred; reputation, regulatory compliance, stakeholder experiences all remain with the organisation.

Whilst cyber risk is about the failure of IT systems such as loss of access or data breach, it is not simply a technology risk or for IT service providers. It is the medusa of risks reaching out in multiple directions with the ability to impact loss across financial, regulatory, operational and reputational categories in an instant. In addition to specific IT service providers, any third party with access into systems poses a cyber threat; document sharing, inventory management, accounts management. The third party systems potentially become the weakest link in any cyber defence as a hacker could use it as a portal into a more secure organisation. It is critical to have a persistent awareness of how cyber threats are being managed.

Board are typically engaged with the topic of cybersecurity, it has been a hot topic for many years and adverse incidents in all sectors have helped maintain its profile. Internal audit can use this to demonstrate the value of third party assurance as the management of many of these risks will now sit outside of the organisation.

Regardless of contractual arrangements an organisation remains accountable for its operations when transferring services to a third party. In many instances the legal risk can be mitigated to a degree but for issues such as bribery and data loss the penalties can be severe. Organisations must be satisfied that legal and regulatory compliance is maintained.

The collapse of global construction giant Carillion sent shockwaves through the public and private sector, a stark reminder that resilience risk can impact at any level. With ever increasing volatility in financial, political and environmental systems organisations must develop contingency arrangements. A fifth of respondents to a 2017 global survey had suffered complete failure of a third party. The report also showed that whilst dependency on external providers was increasing, the maturity of their governance and risk management was lagging behind. CAEs should consider the risk maturity of their organisations in relation to the use of third parties, is there room for improvement? How well prepared is the organisation to deal with external uncertainties? Is a key supplier located in an area prone to earthquakes?

Third parties also bring a new dimension to cultural risk and can adversely impact the overall control environment if there are material differences in approach to:

- **Ethical values:** Regulatory compliance, corporate integrity.
- **Management philosophy:** Risk attitude, data security, HR policies.
- **Authorities:** Decision making, accountability.
- **Competence:** Rewards, quality, experience.

A typical cultural conflict may be in attitude to the Prompt Payment Code, a supplier with tight cash flow controls may not see the reputational benefits of being on the applying rather than receiving end of the Code.

Assurance

Any organisation, regardless of size can find themselves with a significant reliance on third party activities. The extended enterprise refers to the depth and complexity of relationships that also extend to fourth and fifth parties; the sub-contractors and suppliers that an organisations third parties rely on. It is relatively straightforward to manage one or two but once they become multifarious internal audit should be expecting them to be managed in a holistic and co-ordinated manner using robust processes or a vendor management system.

To maximise the value of internal audit assurance, CAEs need to be aware of the full suite of controls, monitoring and assurances in place within the first and second line. An assurance map with clear accountabilities and responsibilities ensures that activities are not duplicated or assumed and fall between the cracks.

For each third party, the organisation will adopt one of three generic strategies that may evolve over time or be embraced from the outset. It could be useful for internal audit to devise its own assurance strategy mirroring the increasing complexity. CAEs may also consider overlaying the assurance activities of the 1st

and 2nd line against this to see where the different strategies are managed.

Frameworks

There are a plethora of vendor risk management and supplier relationship management frameworks available depending on whether your organisation has the capital to employ a big four consultancy, deploy software or needs a practical fix with the support of internal audit. While such tools may be too comprehensive for many organisations, internal audit can use them to prepare more pragmatic test plans during engagement planning or prepare for advisory meetings with stakeholders.

Examples include:

- Created by international professional association ISACA, COBIT 5 offers useful guidance for IT specific vendors.
- A detailed framework for outsourcing arrangements is available from the National Outsourcing Association, whilst too comprehensive for many organisations; internal audit can use it to prepare more pragmatic test plans during engagement planning.
- ISO44001 is concerned with collaborative business relationship management applicable to public and private sectors. The standard provides a relationship management plan, key elements include:
    - A robust rationale/business case for the relationship, including measures of success.
    - Appropriate policies, people and skills to support collaborative working.
    - Culture of working together and resolving conflicts at an operational level.
    - Commitment to continuous improvement, learning from mistakes not seeking blame.
    - Multiparty risk management process alongside day to day monitoring/management of the relationship.
    - An exit strategy, with the risks of separation fully understood.

Closing thoughts

The trend for processes and functions rather than tasks to be transferred to third parties may develop further with whole organisations being operated by third parties. Specialist skills and economies of scale may drive this or the ability to capitalise on innovations. As seen with cloud computing and hosted software, developments take place in a think tank environment and applied to all clients rather than each client having their own projects to generate improvements. Conversely the reputation risk of data loss may become so great that organisations bring activities back in house.

Assurance over individual suppliers and processes is useful but CAEs also need to be providing boards with adequate strategic level assurances to enable them to make informed decisions about the organisations capabilities in relation to third party risks.

> *"High achievement always takes place in the framework of high expectation."*
>
> - Charles Kettering

Further reading

Chartered IIA technical guidance

Risk-based internal auditing

Data security in third party agreements

Auditing supply chains

Outsourcing and the role of internal audit

External

HM Treasury: Building a cooperative assurance relationship between internal audit, departmental gateway, coordinators and centres of excellence

Crown Commercial Service: Public procurement policy guidance

Parliament: Sourcing public services: lessons learned from the collapse of Carillion inquiry

Deloitte: Overcoming the threats and uncertainty: Extended enterprise risk management global survey report 2017

Institute of Risk Management: Extended enterprise risk; managing complexity in 21st Century organisations

Isaca: COBIT 5 guidance

National Outsourcing Association: Outsourcing Life Cycle 2012

BSI: BS 11000 - Collaborate successfully with your chosen partners

Centre for the protection of national infrastructure: Security for industrial control systems - manage third party risks