THIRD-PARTY PROVIDERS

Charlotte Valeur

Most organisations rely on third parties to save costs, improve services, give an independent view, and help on flexibility and competitiveness. Using third parties therefore has become a natural part of an organisation's everyday operations.

A third party is an organisation, supplier, agent, individual, or vendor that interacts on behalf of or with the organisation. Third-party providers provide all kinds of services from legal and accounts to IT, lobbying, or joint ventures. One of the big challenges facing boards and organisations is gaining an understanding of the full extent of their third-party relationships and how to manage the inherent risks associated with them.

Third parties can create risks as well as opportunities which can impact on areas such as reputation and brand value, or potentially give rise to financial and legal risks. This means that organisations need to conduct careful due diligence up front as well as throughout the relationship in order to appropriately monitor third-party risks. This monitoring can be carried out through a combination of on-site visits and the completing of questionnaires. The frequency of the monitoring depends on the risk rating of each third party and should be part of the contractual arrangement.

Having an efficient and effective third-party management system in place is key to ensuring that all risks are being properly monitored and addressed on an ongoing basis.

Why is third-party management and risk oversight a board matter?

Increasingly boards need to ensure they have proper oversight of third-party providers. Some organisations can have thousands of different providers, all with different risk profiles. In a world of cyber risks, data protection, corruption, and new levels of transparency through technology, boards cannot sit idle with regards to which third-party providers their organisations use and the risk management of same. In many countries there are anti-corruption laws, bribery acts, and similar legislation, where organisations are increasingly being found liable for illegal activities or unethical behaviour of their third-party providers. In addition, customers generally don't make the differential between an organisation and its third-party providers and will hold the organisation accountable to any problems that occur, even if that problem lies solely with a third-party provider. This means that organisations today should ensure their oversight of third-party providers is broad enough to capture health and safety, environmental practices, compliance with laws and regulations, use of intellectual property, corruption, bribery, and many more.

Organisations should also ensure that their ethical standards and codes of conduct applies to all their third-party providers as well. All processes concerning ethics, including training and workshops, should include the organisation's third-party providers, particularly those related to employee standards, health and safety, working conditions, legal and regulative behaviours, and environmental, social, governance measures.

Some organisations have interconnected systems with their third-party providers, which makes it necessary to assure that they have appropriate data security and cyber risk systems in place.

The board should have a clear role in providing oversight and ensuring that executive management has a process in place to manage third-party risks. It should also ensure that contract compliance is being monitored on a regular basis and that adequate resources are available to do this. The objective of the board's ensuring that the organisation has full

knowledge and understanding of its third-party exposure, should be to mitigate risks whilst improving quality and reliability of the third-party relationship.

Questions about third parties

- What are the roles and responsibilities for board members and senior management in overseeing third-party risks and opportunities?
- What are the roles and responsibilities for line functions?
- Are there adequate resources to properly manage third parties?
- How often does management update the board on its assessment of third-party risks?
- Are the updates of appropriate timeliness and level of detail?
- Do we have a complete list of all third-party relationships the organisation has?
- Do we have policies and procedures in place for appointing and managing third parties?
- Do our own ethical standards and codes of conduct apply to third-party providers?
- Which third parties can significantly impact the organisation's ability to achieve its strategic goals?
- Should we consider diversifying or consolidating some third-party relationships to reduce risks?
- What approach does the organisation take to perform due diligence on its third parties?
- What are the parameters of oversight of third parties?
- Is internal audit involved with the process?
- How do we ensure all new third parties go through the approval process?
- Does the organisation have robust third-party risk management?
- How often is the risk management matrix updated?
- What controls are in place to mitigate the risks posed by third parties?
- How are problems with third parties identified and addressed?
- Are any significant third-party contracts up for renewal within the next 12 months?
- Do we have a specific third-party risk matrix that is updated on a regular basis?

- Do we have a tech-enabled infrastructure to support the risk management of third parties?
- Do we perform regular third-party due diligence/review?
- Do we have a heightened reputational risk with any of our third parties?
- Do we ensure that our third parties operate according to best practice and our values/ethical values?
- What questions do we ask in third-party reviews?

Third-party review questionnaires should cover a number of relevant questions that can give the board assurances that key third parties to the organisation are fit and proper. The board should ensure they have enough information to gain an understanding of the full extent of the organisation's third-party relationships and associated risks. The third-party monitoring and due diligence should be readily available for boards to inspect.

Questions for third parties

- What is the date of appointment and terms of the contract?
- Have there been any significant or material changes in the ownership structure during the period?
- Have there been any material changes to the team connected to the organisation in the period?
- Has the organisation experienced any operational difficulties during the period?
- What is their internal control framework?
- Have there been any third-party reviews conducted during the period?
- Has the organisation experienced any operational incidents and/or complaints during the period?
- Does the organisation have a disaster recovery and business continuity process plan in place?
- If so, is it available for inspection upon request?
- For information security, does the organisation hold a certification, ISO27001 or similar?
- If not, can you provide confirmation that suitable technology investment and related processes are in place to maintain information security and client confidentiality?

- Have the organisation's information/cybersecurity controls operated effectively during the period?
- Has the organisation experienced any data breaches in the period?
- If yes, please outline any incidents detailing nature, cause, impact, and future mitigation.
- Does the organisation have a testing regime covering PEN tests, social engineering reviews, and business continuity tests?
- Can you provide details of the cybersecurity insurance in place?
- Can you provide details on the level of PI insurance in place?
- Are there anti-bribery, corruption (ABC) and anti-money laundering (AML) policies and procedures in place within the organisation?
- Is the organisation a regulated business?
- If so, can you confirm that it has operated in accordance with its regulatory permits?
- Has the organisation been subject to any regulatory investigation or enforcement in the period?
- Does the organisation outsource any part of its services? If yes, please provide details of such outsourcing.
- Can you confirm that the organisation complies with labour laws and other regulatory requirements?
- Does the organisation use intellectual property appropriately?
- Does the organisation have a diversity policy?
- Does the organisation have policies and appropriate oversight of health and safety?
- Does the organisation monitor environmental impact/emissions?