

# Third Party Risk Management:

# Outsourcing



# Third Party Risk Management: Outsourcing

# What should you consider?

Over recent years, organisations have chosen to outsource their business activities in order to reduce costs and improve their flexibility and efficiency. Outsourcing is one of the specific aspects of institutions governance arrangements and is now a key focus of both the European Banking Authority ('EBA') and the Central Bank of Ireland ('CBI').

On 25 February 2019, the EBA published its final revised 'Guidelines on outsourcing arrangements'. The Guidelines will repeal the 2006 guidelines on outsourcing and the EBA's recommendation on outsourcing to cloud service providers.

Furthermore, the CBI's discussion paper 'Outsourcing Findings and Issues for Discussion' issued on 19 November 2018, follows on from an extensive review of outsourcing arrangements across the Irish financial sector in which 185 regulated firms were surveyed. The review identified significant weaknesses in how outsourcing arrangements are being managed, with the results of the survey being described as "disappointing."

See here for a summary of the paper: https://home.kpmg.com/ie/en/home/insights/2018/11/ central-banking-outsourcing-findings.html

We have outlined below a number of key questions to consider in relation to your outsourcing arrangements in order to ensure adequate management of your third party risks.



# 1 Does the Board have a sufficient level of awareness and control of outsourcing arrangements?

• Institutions should ensure that the Board is aware of the scale of outsourcing arrangements and the consequent level of third party dependencies.

## What should you consider?

- Do the Board consider the potential impact of outsourcing on end to end processes when making a decision to outsource?
- Do firms need to apply operational risk management and governance practices to outsourcing arrangements?
- Are Board considerations of outsourcing arrangements evidenced by records of discussions and decisions?



# 2 Has sufficient risk assessment been completed on outsourcing partners?

• Firms should ensure that they conduct adequate risk assessments before entering into an outsourcing arrangement. Risk assessments of outsourcing arrangements should be revisited on an ongoing basis.

- Have you conducted a detailed risk assessment of all relevant risks, which includes risks associated with sub-contracting? Do you know where the risks exist in these relationships?
- Is the planned outsourcing arrangement critical or an important function of your business? Do you understand the role and need for the service provider?
- Have you identified and assessed any conflicts of interest that may exist with the service provider?
- Have you considered the visibility of the internal control environment in the service provider?



# 3 Have you carried out appropriate due diligence?

 Institutions should ensure through their selection process and assessment that the service provider has appropriate and sufficient ability, capacity, resources, organisational structure and, if applicable, required regulatory authorisation(s) to perform the critical or important function in a reliable, controlled and professional manner over the duration of the proposed contract.

## What should you consider?

- When conducting due diligence, have you considered the service provider's business model, nature, scale, complexity, financial situation, and, if applicable, group structure?
- Can Outsourcing Service Providers meet their requirements and contractual obligations in relation to service quality and reliability, security and business continuity?
- Could the failure of an Outsourcing Service Provider's activity breach a firm's risk appetite?
- Is the same level of Due Diligence carried out on intragroup outsourcing arrangements as compared to third party outsourcing arrangements?

# 4 Is there adequate responsibility and oversight over outsourcing arrangements?

• Is the ownership of outsourcing risk clearly designated and is there an appropriate oversight and governance structure in place?

- What oversight and governance is there in place over outsourcing activities?
- Are there clearly established lines of responsibility in place from Business Areas up to Board Level?
- When a 'cross functional arrangement' exists, what additional measures are needed to ensure effective oversight and risk management?
- Does the outsourcing inhibit the firm from having appropriate access to information, processes and personnel?



# 5 Outsourcing to a service provider abroad

- Institutions should ensure that banking activities or payment services that require authorisation by a competent authority can only be outsourced to a service provider abroad, if:
  - The service provider is authorised or registered by a competent authority to perform such banking activities or payment services; or
  - The service provider is otherwise allowed to carry out those services or activities in accordance with the relevant national legal framework.

# What should you consider?

- For outsourcing of banking activities based overseas, have you considered whether they are regulated?
- What framework does this country have in place to regulate banking activities, is it performed to a similar level as the EBA?

# 6 Documentation of outsourcing arrangements

- Firms should maintain a register of all outsourcing arrangements at institution and group level.
- It is key that regulated firms have a firmwide outsourcing policy outlining clear lines of responsibility for initial due diligence and ongoing management and review of outsourced arrangements in place.

- Does an outsourcing policy exist and if so, is the policy adequate to satisfy EBA and CBI requirements?
- Are all outsourcing contracts documented centrally on a register? Have you sufficient detail on each outsourcing arrangement to produce a register as prescribed above?



# 7 Monitoring

 Institutions should monitor on an ongoing basis the performance by service providers and sub-contractors. Institutions must place particular focus on the outsourcing of critical or important functions, including that the availability, integrity and security of data and information is ensured.

# What should you consider?

- Is there a contract and SLA in place? Are you monitoring the key performance indicators as set out in the contract and SLA?
- Are you comfortable that the risks are being continuously monitored and managed?
- Have you planned to monitor the key risks such as availability, integrity and security of data through conducting regular internal audit or assurance
- Have you received and reviewed all third party assurance reports from your outsourcing partner such as SOC1 and SOC2?

# 8 Do you have an exit strategy and business continuity plan?

- Institutions should have a clearly defined exit strategy and business continuity plan for all outsourcing of critical or important functions in line with their outsourcing policy, including for the following possibilities:
  - Termination of an outsourcing arrangement;
  - Failure of a service provider; or
  - Material deterioration of the service provided.

- Would the termination of a service provider impact adversely on your compliance with regulatory requirements and/or your day-to-day operations?
- Have you identified alternative solutions and transition plans to include the removal and transfer of data from the service provider to an alternative provider?



# How KPMG can help

The Central Bank of Ireland expects that all regulated firms take appropriate action to address the issues outlined in the Outsourcing Findings and Issues for Discussion paper and be in a position to evidence same to the Central Bank if required. KPMG can help you review your outsourcing arrangements already in place as well as assist you consider new ones. KPMG can also help you assess the design and implementation of the appropriate policies, procedures and controls or update your existing outsourcing frameworks to ensure that they are appropriately considered and adequately managed. We can help you assess your outsourcing arrangements against our third party risk management framework (TPRFM). Our framework is aligned to regulatory and best practice requirements. Each of the framework elements present different but often interrelated challenges including implementation challenges we have helped our clients address.

Strategy		Governance
<ul> <li>Mission and objectives</li> <li>Align third party use to risk appetite</li> <li>Management of operating expenditures</li> </ul>		<ul> <li>Oversight structure/ committees (i.e., Board, Enterprise risk management, Operations risk)</li> <li>Tone &amp; culture</li> <li>Structure and organisatio</li> </ul>
Information reporting & technology	Credible challenge	Policies and procedures
<ul> <li>Dashboards/reports</li> <li>Key risk indicators (KRIs)</li> <li>Key performance indicators (KPIs)</li> <li>Process automation</li> </ul>	Third party oversight framework	<ul><li>Standard setting</li><li>Policy management</li></ul>
People	diole chance	Process
<ul> <li>Roles &amp; responsibilities</li> <li>Skills &amp; training</li> <li>Performance management &amp; compensation</li> </ul>		<ul> <li>Planning</li> <li>Risk assessment, due diligence and selection</li> <li>Contracting</li> <li>Monitoring &amp; testing</li> <li>Off-boarding</li> </ul>



### **Contact Us:**

Please call us if you would like to discuss the design, implementation or assurance of processes relating to outsourcing and third party risk management.

Michael Daughton Partner T. +353 87 744 2965 E. michael.daughton@kpmg.ie Jackie Hennessy Director T. +353 87 050 4171 E. jackie.hennessy@kpmg.ie Shane Bolger Manager T. +353 87 050 4382 E. shane.bolger@kpmg.ie Tara Lenihan

Senior Associate T. +353 1 410 1697 E. tara.lenihan@kpmg.ie

# y 🐻 in kpmg.ie

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2019 KPMG, an Irish partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International. (4714)