Deloitte Third Party Assurance Benchmarking
Quarterly Deep Dive – December 2015

Monitoring of Outsourced Service Providers
Background
As part of Deloitte’s annual third party assurance benchmarking exercise where we survey approximately 60 reports across various service organisations in different industries, we are extending our insights by performing a deeper analysis over selected individual control objectives. This represents the first in a series of quarterly newsletters, and provides insight into the control objective relating to monitoring subservice organisations.

Why is monitoring outsourced service providers important?
The use and reliance on third parties is becoming more pervasive and complex across the Australian Financial Services Industry. In this complex environment, organisations are seeking new ways to reap substantial upside benefits and drive performance through the third party ecosystem. Extracting greater value from your extended enterprise means more than negotiating favourable terms and pricing. More effective and efficient third party management will improve quality, increase productivity, and strengthen relationships with your service providers and ultimately your customers.

Results of analysis
Across the industry, there is inconsistency in the classification of subservice or outsourced providers and a lack of clarity as to which services and service entities are being classified as a key subservice organisation. Historically, organisations considered the following example questions to determine if a service provider should be considered a key subservice organisation:

- Do they process client transactions?
- How key is it to their ongoing daily business operations?
- What is the size and cost of the contract?
- How difficult is it to quickly replace the service provider?

However, increasingly with the emergence of cloud based storage and cyber threats, organisations are realising that providers that do not fit the above criteria could still be considered key sub service organisations as they do maintain client data that can be accessed and manipulated by others. Regardless, organisations should be clear, consistent and transparent as to the classification of subservice organisations in their organisation.

The types and depth of controls over subservice organisations in the industry also varies – many are not described in enough detail in third party assurance reports to determine the extent, consistency and quality of controls implemented to monitor subservice organisations. We have analysed a selection of third party assurance reports across the Investment Management industry and benchmarked the maturity of controls in place to address the following objective:

Appointments of subservice organisations are approved, subservice organisations are properly managed and their activities are adequately monitored on a timely basis. The below chart contains examples of control activities we are seeing across the industry in order of complexity:
<table>
<thead>
<tr>
<th>Category</th>
<th>Basic</th>
<th>Sound practice</th>
<th>Better practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Due Diligence</td>
<td>Initial Due Diligence performed over key factors such as price, service, company, management.</td>
<td>Comprehensive initial Due Diligence performed. Due diligence re-performed annually.</td>
<td>Comprehensive initial and ongoing Due Diligence performed; Embeds oneself in subservice organisations strategic planning and decision making. Executive champions on both sides, aligning service delivery to strategic objectives.</td>
</tr>
<tr>
<td>Approval of arrangement</td>
<td>Executive approval required.</td>
<td>Board/Committee approval required.</td>
<td>Board/Committee approval required. Annual re-evaluation of outsourced service provider at Board/Committee level.</td>
</tr>
<tr>
<td>Review and Report Performance</td>
<td>The Board/Sub-Committee receive sufficient information to be comfortable that its polices and controls have been operating effectively to monitor key subservice organisations, including at least an annual review of performance levels in accordance with service level agreements.</td>
<td>In addition to basic practice, users will maintain periodic contact with its subservice organisation to be comfortable service standards and contracted terms are being adhered to and issues are discussed on a timely basis.</td>
<td>In addition to sound practice, there is more frequent (monthly/quarterly) monitoring and contact with subservice organisations. Incidents or breaches are reported immediately. Reporting from the subservice organisation is more comprehensive and includes changes in systems, people, or processes. Attestations from the subservice organisation are received in respect to key contract or regulatory requirements. The Board/Committee receives reporting that enables periodic re-assessment of its third party arrangements and operating model.</td>
</tr>
<tr>
<td>Audited service organisation report</td>
<td>Review of audited controls report for deviations.</td>
<td>Review of audited controls report for deviations as well as for design and implementation of controls over outsourced services provided.</td>
<td>Review of audited controls report for deviations as well as for design and implementation of controls over outsourced services provided. Mapping of audited controls report to risks / objectives of the user organisation.</td>
</tr>
</tbody>
</table>

**Key insights**

As demonstrated above, regular, ongoing monitoring and review of the performance of subservice organisations is necessary in managing third party risks. Due diligence of subservice organisations should not just be performed at the onset of an outsourcing arrangement – it is important to reperform this regularly. A few key insights from our analysis include:

- Simply receiving a subservice organisation’s audited controls report is not sufficient – key stakeholders should review the results and understand the complimentary controls in place at your organisation in order to ensure adequate, effective and efficient integration with your extended enterprise
- Most service organisations did not classify software vendors as subservice organisations – we believe they should reconsider whether some of these should be classified as subservice organisations
- Many subservice organisations are not themselves providing assurance reporting on their controls (e.g. gateway providers, loan administrators and IT infrastructure providers). Users of these organisations should consider pressing them to provide a third party assurance report.

**Beyond third party assurance: Better practices**

Organisations should reassess their third party arrangement and controls, including:

- Taking an inventory of your organisations extended enterprise
- Determining a risk rating of each entity based on a series of key factors that may impact your business value chain
- Develop or enhance third party provider profiles to capture key information including relationships, company news, services provided, risk ratings, operational performance, and fee terms
- Creating a reporting structure on higher risk entities for presentation to the Board and Committee level
- Embedding policies, procedures and technology to enable better management and monitoring for higher risk entities
- Creating accountability and ownership within the business to manage these risks.
A selection of our thought leadership in respect to Third Party Assurance is outlined below. Please give us a call if you’d like further information.