Connect › Support › Advance

The Institute of Internal Auditors Australia

## Whitepaper

# Assurance over Third Party Service Providers

Updated 2022

Level 5, 580 George Street, Sydney NSW 2000 | PO Box A2311, Sydney South NSW 1235
**T** +61 2 9267 9155 **F** +61 2 9264 9240 **E** enquiry@iia.org.au **www.iia.org.au**

# Assurance over Third Party Service Providers

## Contents



## Background

### Purpose

Engaging third party service providers may provide economies of scale, cost savings, productivity gains, or other benefits to an organisation. But these relationships can also reduce an organisation's control over their product or service, which makes the third party risk management process that much more important.

When key third party service providers fall short of service expectations or fail altogether, the resulting reputational and operational damage to their clients can be significant and may even exceed any damage the service provider may suffer.

Executives and boards rely on internal auditors to assure risks are identified and assessed, appropriate internal controls are in place, and timely risk intelligence is being generated to drive informed decision-making.

### Background

Due diligence is generally undertaken when engaging a third party service provider, but there can be less attention paid to ongoing due diligence. and uncertainty over who is responsible for assuring parties further down the supply chain such as fourth, or 'nth' parties. (refer Figure 1)

*Figure 1: The outsourcing chain*


Typically, organisations leave the main responsibility with their contracted third-party service provider. If that party identifies issues with services provided by the fourth or 'nth' party, the organisation either assumes or has written into the contract that the contracted third party resolves the issues. This approach works in theory, but may not be adequate in the real world. Third party service provider incidents are increasing, often with immediate pubic visibility.

## Discussion

### Issue

The issue to be discussed is:

How can Internal Audit provide assurance that risks associated with third party service providers are being identified, assessed and responded to appropriately?

### History

Internal Audit traditionally operates 'internally' within organisations, providing assurance over their organisation's internal controls. With the advent of outsourcing and the associated risks, Internal Audit's role expanded to providing assurance in relation to third party risks, including assurance over the internal controls of third-party service providers.

'Right to audit' clauses were included in some contracts and, although not always executed, allowed Internal Audit to undertake site visits and obtain information to assess controls at third party premises.

In January 2015, the Auditing and Assurance Standards Board (AUASB) issued ASAE 3150 'Assurance Engagements on Controls' and some organisations began to rely on these reports for assurance that third party risks were being managed appropriately.

© 2022 - The Institute of Internal Auditors - Australia

# Assurance over Third Party Service Providers

## Discussion

Internal Audit can provide assurance in relation to third party risks in a number of ways. Figure 2 lists some examples.

*Figure 2: Assurance over third party risk management – may be provided by Internal Audit or other assurance providers*

**Audit the third party risk management framework**

- The third party risk management framework may be a standalone framework or an element of an organisation's overarching risk management framework.

**Audit the third party risk management process**

- For example, conduct a procurement audit that includes reviewing how third party risks were addressed.

**Include third party risk management in process audits**

- For example, in a payroll audit evaluate the third party risk management processes used in relation to the third party that processes the payroll.

**Undertake audits of third parties**

- As independent assurers, Internal Auditors can undertake audits of third parties through exercising 'right to audit' clauses in contracts.

Ideally, an organisation should have a fit-for-purpose third party risk management framework. There are no set rules as to what this should look like, but it should align with the organisation's overarching risk management framework. Figure 3 outlines common elements found in third party risk management frameworks mapped against the five components of the COSO[1] 2017 Enterprise Risk Management model.

*Figure 3: Example third party risk management framework elements*

**Governance and Culture**

- A dedicated third party risk management hub can provide insight into all third party relationships across the organisation, control over the onboarding process and ongoing oversight of third party relationships. The owner may be the head of procurement, chief operating officer, or a governance body. Alternatively, managing third party service providers may be decentralised and each business manager may own the third party relationships in their area.
- The IIA 'Three Lines Model' can be used to define third party risk management roles and help identify duplication or gaps (refer Figure 4).
- Third party risk management policies and procedures may be either standalone products or included in an organisation's overarching risk management polices and procedures.

**Strategy and Objectives**

- The organisation has a documented strategy with regard to third parties. It identifies the inherent risks of the services and how the organisation will select, assess and oversee its third party service providers.
- The organisation's risk appetite serves as the basis for determining which third party service providers are engaged and on what terms, and as a basis for ongoing monitoring.

**Performance**

- A third party relationships register is maintained. This may be as simple as a Microsoft Excel spreadsheet that includes all third party service providers:
  - segmented according to their risk profile (refer Figure 5);
  - cross-referenced to every area within the organisation that has a relationship with a third party service provider, together with details of the nature of each relationship.

1 Committee of Sponsoring Organizations of the Treadway Commission

© 2022 - The Institute of Internal Auditors - Australia

# Assurance over Third Party Service Providers

### Review and Revision

- Third party risk management performance is reviewed and the third party risk management framework revised as required, based on performance.

### Information, Communication and Reporting

- Right of access to information / audit clauses are included in contracts and these clauses are executed on a periodic basis.
- Communication about third party risk management is across, up and down the organisation. The status of third party service providers critical to the organisation is visible at the highest level.
- Third party risk reporting feeds into enterprise risk reporting processes.

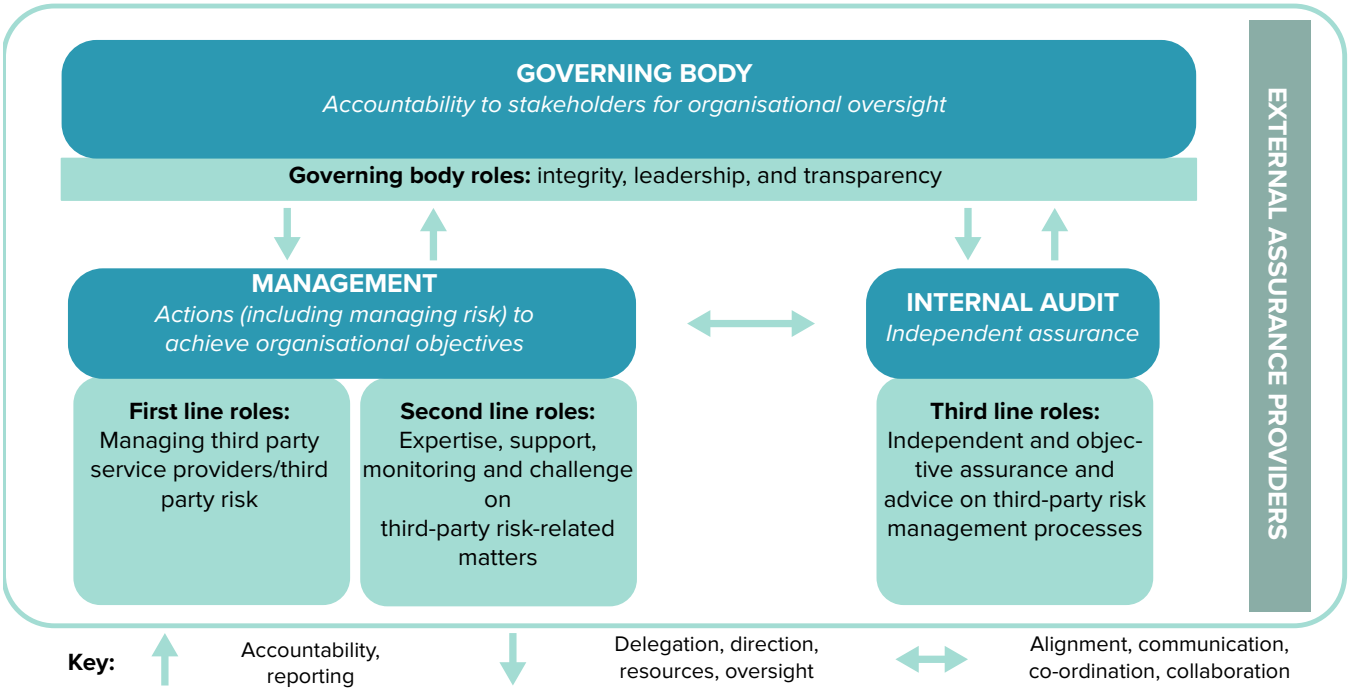
Detailed guidance on how to conduct an Internal Audit of a third party risk management framework and of a third party risk management process is available in Appendix G of the IIA Practice Guide 'Auditing Third-party Risk Management' (2018).

Third party risk management roles can be defined using the IIA's 'Three Lines Model', as illustrated in Figure 4. Defining roles with this model can help identify any potential duplication of assurance effort or assurance gaps.

It is important to recognise that, when using third party service providers, first line accountability does not go away – being at a distance just makes it more challenging. Larger organisations may have second line assurance providers that can undertake ongoing monitoring and escalation of first line activities. For these organisations, Internal Audit should assess the degree of reliance that can be placed on second line assurance activities when developing the annual Internal Audit plan.[2] Note that reliance on an external party does not reduce the obligation of the CAE to provide appropriate assurance to the board.

2 Refer IIA Practice Guide 'Reliance by Internal Audit on Other Assurance Providers' (2011)

*Figure 4: Defining third party risk management roles with the IIA's 'Three Lines Model'*




© 2022 - The Institute of Internal Auditors - Australia

# Assurance over Third Party Service Providers

If the second line, for example the procurement team, maintains a centralised repository of third party service provider information, Internal Audit can use this to understand the third party risk environment and identify high-risk areas more effectively.

Conversely, integration of Internal Audit findings into third party risk assessments can assist the risk management function identify risks it may have missed and focus on the risk areas that truly matter. Management teams and boards can then receive a holistic view of the organisation's third party risk profile.

Apart from assessing the third party risk management framework and the third party risk management process, Internal Audit can undertake audits of third party service providers directly.

Criticality and risk level of a third party service provider should determine the frequency and intensity of ongoing monitoring, as well as periodic reviews. An example of third party segmentation and the types of assurance activities that may be conducted within each tier is provided in Figure 5.

*Figure 5: Example segmentation of third party service provider relationships*

| Tier 1 (High risk) | Tier 2 (Medium risk) | Tier 3 (Low risk) |
|---|---|---|
| › Self-assessment<br>› Review of return<br>› ASAE reports<br>› Periodic audits | › Self-assessment<br>› Review of return<br>› ASAE reports<br>› Independent validation of the self-assessment every three years | › Self-assessment<br>› Review of return<br>› ASAE reports |

Low-risk third party service providers could be required to submit annual self-assessments of their performance against their contractual requirements where this is practical. These reports could be reviewed and any anomalies investigated. For medium-risk relationships, independent validation of self-assessment reports could be undertaken and, for high-risk relationships, periodic audits should be undertaken.

Where available, ASAE 3150 'Assurance Engagements on Controls' and ASAE 3402 'Assurance Reports on Controls at a Service Organisation' and related reports should be gathered and reviewed by the third party relationship owner and relevant subject matter experts for example the security team, cyber security team, etc.

It should be noted however, that ASAE 3150 engagements are structured to suit the particular circumstances of the engagement and the needs of users. The scope is set by the party engaging the assurance practitioner, and engagements can be limited to reviewing the design of controls – they may not include assessment of operating effectiveness of these controls. ASAE 3402 engagements are limited to reviewing controls relevant to financial reporting.

## Conclusion

### Summary

Third party relationships continue to expand and evolve, introducing risks that must be continuously assessed and responded to, to achieve organisational objectives. Internal auditors and risk managers, particularly those who hold the IIA Certification in Risk Management Assurance (CRMA) are uniquely qualified to identify potential third party risk exposures and make recommendations on how to respond to those risks.

### Conclusion

Internal Audit can consider third party risks in developing the annual Internal Audit plan, provide assurance and advisory services in relation to the third party risk management framework, and consider third party risks when undertaking engagements. Where 'right to audit' clauses are included in contracts with third party service providers, Internal Audit can undertake audits of these third party service providers.

© 2022 - The Institute of Internal Auditors - Australia

# Assurance over Third Party Service Providers

## Bibliography

IIA Global 'Practice Guide – Auditing Third-party Risk Management'
IIA Global 'Practice Guide – Reliance by Internal Audit on Other Assurance Providers'
IIA Global 'Tone at the Top – Managing Third-Party Risks'
IIA Global 'The IIA's Three Lines Model – an update of the three lines of defence'
Auditing and Assurance Standards Board ASAE 3150 'Assurance Engagements on Controls'
Auditing and Assurance Standards Board ASAE 3402 'Assurance Reports on Controls at a Service Organisation'
COSO '2017 Enterprise Risk Management – Integrating with Strategy and Performance'

## Purpose of White Papers

A White Paper is a report authored and peer reviewed by experienced practitioners to provide guidance on a particular subject related to governance, risk management or control. It seeks to inform readers about an issue and present ideas and options on how it might be managed. It does not necessarily represent the position or philosophy of the Institute of Internal Auditors–Global and the Institute of Internal Auditors–Australia.

## Author's Biography

This White Paper written by:
**Narelle Sheppard** BFinAdmin PFIIA CIA CGAP CRMA FCPA

Narelle is a management consultant and independent audit committee member. She has more than 25 years of experience spanning both the private and public sectors and has held various internal audit roles including at the Australian Taxation Office, Department of Defence, and the former Department of Industry, Innovation and Science where she was the Chief Audit Executive.

Narelle has been a member of the IIA since 2007 and a member of the IIA-Australia Audit and Risk Committee since 2018. Narelle was a member of the Finance Committee for the IIA 2017 International Conference and served on the IIA ACT Chapter Council for six years including a term as Chapter Chair.

This White Paper was edited by:

**Michael Parkinson** BSc(Hons), GradDipComp, PFIIA, CIA, CISA, CRMA, CRISC

**Andrew Cox** MBA, MEC, GradDipSc, GradCertPA, DipBusAdmin, DipPubAdmin, AssDipAcctg, CertSQM, PFIIA, CIA, CISA, CFE, CGAP, CSQA, MACS Snr, MRMIA

## About the Institute of Internal Auditors–Australia

The Institute of Internal Auditors (IIA) is the global professional association for Internal Auditors, with global headquarters in the USA and affiliated Institutes and Chapters throughout the world including Australia.

As the chief advocate of the Internal Audit profession, the IIA serves as the profession's international standard-setter, sole provider of globally accepted internal auditing certifications, and principal researcher and educator.

The IIA sets the bar for Internal Audit integrity and professionalism around the world with its 'International Professional Practices Framework' (IPPF), a collection of guidance that includes the 'International Standards for the Professional Practice of Internal Auditing' and the 'Code of Ethics'.

The IIA-Australia ensures its members and the profession as a whole are well-represented with decision-makers and influencers, and is extensively represented on a number of global committees and prominent working groups in Australia and internationally.

The IIA was established in 1941 and now has more than 200,000 members from 190 countries with hundreds of local area Chapters. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

© 2022 - The Institute of Internal Auditors - Australia

# Assurance over Third Party Service Providers


## Copyright

This White Paper contains a variety of copyright material. Some of this is the intellectual property of the author, some is owned by the Institute of Internal Auditors–Global or the Institute of Internal Auditors–Australia. Some material is owned by others which is shown through attribution and referencing. Some material is in the public domain. Except for material which is unambiguously and unarguably in the public domain, only material owned by the Institute of Internal Auditors–Australia–Global and the Institute of Internal Auditors–Australia, and so indicated, may be copied, provided that textual and graphical content are not altered and the source is acknowledged. The Institute of Internal Auditors–Australia reserves the right to revoke that permission at any time. Permission is not given for any commercial use or sale of the material.

## Disclaimer

Whilst the Institute of Internal Auditors–Australia has attempted to ensure the information in this White Paper is as accurate as possible, the information is for personal and educational use only, and is provided in good faith without any express or implied warranty. There is no guarantee given to the accuracy or currency of information contained in this White Paper. The Institute of Internal Auditors–Australia does not accept responsibility for any loss or damage occasioned by use of the information contained in this White Paper.