

The Future of Third-Party Assurance (TPA)  
Insights from our 2022 Global TPA Survey

February 2023



## Foreword

Organisations are more dependent than ever on third parties to fulfil critical business processes across their ecosystems. Outsourcing business functions, controls and data handling **does not outsource the risk**. As such, there is a need for transparency and monitoring over the activities and controls in place across third (and fourth) parties to ensure they are suitably robust and in line with the risk profile and appetite set.

**Third-party governance and monitoring** is emerging as a **key focus area**, all the way up to the Board level. **Regulatory scrutiny** is increasing, requiring more direct oversight and ongoing due diligence by Management and the Board on third-party risk and assurance matters. Additionally, we are seeing **third-party incidents and customer service disruptions are on the rise**, often with immediate public visibility and greater severity, including; customer, reputational, regulatory and financial consequences.



### Our Third-Party Assurance (TPA) Global Survey Report



With this context in mind, Deloitte conducted a Global TPA Survey with an objective of gaining a deeper understanding of **current and emerging third-party risks and trends across multiple geographies and industries**, in order to provide the global community with perspectives and insights into the current and future landscape of TPA reporting.

**In this report, we provide a summary of insights gained from:**

- **Surveying** the global TPA community, along with **interviewing** a selection of Deloitte clients to gain further perspectives on the preliminary survey results.
- **Our experience** having worked with a range of clients across multiple industries and geographies globally.

**This report aims to share:**

- Current and emerging **third-party risks** and trends.
- Insights into the current and **future landscape of TPA reporting**.
- **Useful perspectives** from the global TPA community.

We also **selected a sample of TPA reports**, where permissible, from across the globe and from multiple industries to **benchmark** these reports in order to identify further insights and trends in TPA reporting of key interest to the global TPA community. The results of this benchmarking will be shared anonymously in a separate report.



**Erica Pretorius**  
Partner, Canada  
Global TPA Leader



**Vincent Sita**  
Partner, Australia  
Lead Author

# Survey Approach

## Background



- This report provides an analysis of a **cross-industry and geography survey** of TPA stakeholders conducted in June 2022 that aimed to understand current and emerging third party risks and trends.
- The survey respondents included individuals from **senior levels across multiple departments**, industries and geographies, in order to gain **a broad and diverse set of perspectives**.
- The preliminary survey results were **shared with a selection of Deloitte clients** across the globe to gain their perspectives and insights on the survey results.
- Deloitte then overlaid its **experience** and insights.
- Insights gathered have been summarised into five themes and reported within this report **for the benefit of the global TPA community**.

## Data analysis and feedback



- Data analysis was conducted on the survey responses to **correlate data points, identify significant combinations and derive insights**. Analysis included consideration of the following:
  - Survey responses across each of the survey questions, both in **isolation and in combination**.
  - Demographic profile of survey respondents, including **nature of business, geography, industry and position/role**.

## Report structure



- **Five key themes** from the analysis are summarised on the next page.
- Each key theme is then presented in the following pages, including **detailed analysis and perspectives**.
- At the back of this report we provide the aggregated survey respondent **demographic profiles**.
- Finally, we have included the **contact details** of the authors, should you wish to contact us for more information.

Foreword

Survey approach

**Glossary of terms**

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

## Glossary of terms

Term	Definition
AML	Anti-money Laundering
CCM	Cloud Controls Matrix
CISO	Chief Information Security Officer
CUECs	Complementary User Entity Controls
ESG	Environmental, Social and Governance
GDPR	General Data Protection Regulation
GRC	Governance, Risk and Control
HIPAA	Health Insurance Portability and Accountability Act
ICFR	Internal Controls over Financial Reporting
ISO 27001	International Organisation for Standardisation 27001
KPI	Key Performance Indicator
NIST	National Institute of Standards and Technology
PCC DSS	Payment Card Industry Data Security Standard
SaaS	Software as a Service
SLA	Service Level Agreement
SOC Report (SOC 1, SOC 2, SOC 2+)	System and Organisation Controls Report (1, 2, 2+)
TPA	Third Party Assurance
TPRM	Third Party Risk Management
TSC	Trust Services Criteria (SOC 2 Framework)

## Summary of key themes

01

### Emerging needs for TPA reporting

The volume and intensity of risk domains is increasing, and new trends continue to emerge. Cybersecurity is the prominent trend that requires TPA to support trust and transparency in ecosystems, followed by Privacy and ESG. Consequently, organisations increasingly require new forms of TPA and there are new frameworks / approaches to deliver this. SOC2+ is a key reporting mechanism that brings a wide range of assurance requirements together under a single report.



02

### Purpose, relevance and value

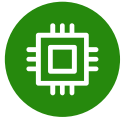
Users and service organisations have varied perspectives in terms of the purpose of TPA reporting and the value attached to it. Clarity in scope and coverage, as well as the impact of control deviations, are some reasons for these divergent views. This means that TPA reports need to be dynamic and continually assessed to ensure they meet the ever-changing needs of TPA stakeholders, particularly as the risk universe continues to proliferate.



03

### Digital Journey

Most surveyed organisations are on a digital journey and their target state is always changing. As organisations implement digital strategies to transform their business, their control environments must also transform. Many organisations indicate that control environments are not maturing at the same pace as digital change.



04

### Integrated monitoring tools

Integrated monitoring tools, like GRC tools, are increasingly being used to manage and monitor risks and controls and increase the timeliness of information flow. Modern tools work like an orchestrator and are connected to multiple business applications; however, more can be done to integrate these into business operations. A move towards automation also requires a cultural shift which can often be more difficult to embed.



05

### Monitoring activities

Organisations are primarily relying on TPA reports and publicly available information to monitor the health of their third parties, but is this level of monitoring commensurate with the risk? If businesses are outsourcing custody of critical business transactions and customer data, the answer is probably not. Monitoring of fourth parties and beyond is even less robust and there is a need for organisations to look through their entire outsourced ecosystem. A push towards automation as it relates to third party monitoring is needed to increase the speed and frequency of information between nth parties.



Foreword

Survey approach

Glossary of terms

Summary of key themes

**01. Emerging areas of TPA reporting**

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

# 01. Emerging areas of TPA reporting





Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

## Current or emerging trends where TPA is most needed to support trust and transparency in the outsourcing ecosystem

Cybersecurity is the most prevalent current/emerging trend. Privacy/GDPR and ESG are the next highest ranked areas, and are gaining prominence as regulatory, social and business expectations evolve.

01

**Cybersecurity** is the #1 emerging trend

02

**Privacy/GDPR**

03

**ESG/Climate**

53% of respondents said that Cybersecurity is included in TPA reports they distribute or receive. The **percentage further drops** for Privacy/GDPR (39%). ESG coverage is significantly lower, with just 13% of organisations believing ESG is covered in existing TPA reports distributed or received.



### Insights and perspectives



- Historically, TPA reports focused on ICFR and operational areas. With the rise of digital and cloud computing, **new risks and corresponding assurance reporting needs have emerged.**
- As the risk universe continuously expands, there is a need for organisations to **proactively scan the horizon** and assess third party risks to keep pace with this change.
- Survey results show that the **most prominent emerging risks do not have a sufficient level of coverage in TPA reports** distributed or received, particularly for ESG.
- These emerging risks, coupled with increased dependency on third parties, provides an **opportunity for TPA reports to provide assurance over broader scope areas** and deliver more value for the outsourcing ecosystem.
- This is particularly relevant as the **volume, sophistication and impact of cyber incidents** continues to rise.
- These incidents can often lead to losses of personal data, confounding the need for a **focus on addressing privacy risks.**
- With the growing awareness of climate change risk and the global call to arms related to ESG matters, its no surprise that **organisations have ambitions around assuring ESG performance.**

Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

## Current or emerging trends (continued)

*AML and supply chain also ranked highly as emerging trends where TPA is most needed.*

04

AML

05

Supply chain

31% of respondents feel that AML is included in TPA reports they distribute or receive. For supply chain, this increases to 42%.

### Insights and perspectives

- Organisational ecosystems are **growing**, becoming more **complex** and are increasingly **reliant on supply chains**. Recent supply chain disruptions across the globe are causing **significant challenges for business**.
- Organisations are increasingly identifying a need for an **agile, robust and optimised controls framework** to manage the complex supply chain risks and help prepare for potential disruptions.
- Accordingly, survey respondents recognise the importance of TPA reports in **supporting/assuring operational resilience** across their ecosystem.
- Organisations are also realising the need for enhanced due diligence with respect to AML, including obtaining assurance in this area, particularly among financial institutions. **75% of respondents** within the Financial Services industry suggested that **AML should be part of TPA reports**.
- There is a **need for future TPA reports to evolve** by focusing more on these emerging industry and subject matter specific areas of risk.



Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

## The growing market for SOC2+

SOC2+ reporting enables the consolidation of multiple frameworks and industry standards into a single TPA report. The use of SOC2+ is likely to rise over the coming years as organisations seek to demonstrate operational compliance across a broad set of risk areas.

The awareness of, and demand for SOC2+ is on the rise 

**54%** of respondents anticipate that SOC2+ would be required in their organisations in future

**66%** of respondents are either aware of, or have used or produced, a SOC2+

**34%** of respondents are either not aware of, nor have they used or produced a SOC2+

The *CISO of a mid-sized SaaS organisation* told us that it is difficult to have a one-size-fits-all approach to TPA reports as there are **so many different frameworks to comply with**. SOC2+ is one option they are considering to bring multiple information security frameworks together.



Insights and perspectives 

- Survey results show that there is an **increased awareness and use** of SOC2+ reports, with demand expected to grow.
- This is reflective of the **growing cost of compliance**, with organisations having to comply with many different frameworks and standards to meet the demands of customers, regulators and wider stakeholders.
- There is often overlap between framework/standard subject matters, meaning organisations may only need to be audited once in those areas under the SOC2+ model – a **‘test once, satisfy many’** approach.
- Demand will also be driven by **digital transformation** programs and the transition to more complex technology environments.
- That said, organisations scoping in the Privacy TSC within the standard SOC2 framework are in the minority. Given that Privacy is a key emerging risk with insufficient coverage within existing TPA reports, Service organisations are asking themselves whether they should **expand SOC2 reporting to the Privacy TSC to meet stakeholder demands** and address this risk, before making the transition to SOC2+.
- **Common inclusions to a SOC2+**, in addition to the standard SOC2 framework, are ISO 27001, NIST, PCI DSS, GDPR, CCM and HIPAA (refer to glossary for definition of these abbreviated terms).
- In Deloitte’s experience, an **increasingly common SOC2+ combination** is SOC2 and ISO 27001.
- This is supported by the survey, with 43% of respondents indicating that **ISO certification is a “Very Important” area** to be incorporated into existing TPA reports.



Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

**02. Purpose, relevance and value**

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

## 02. Purpose, relevance and value



Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

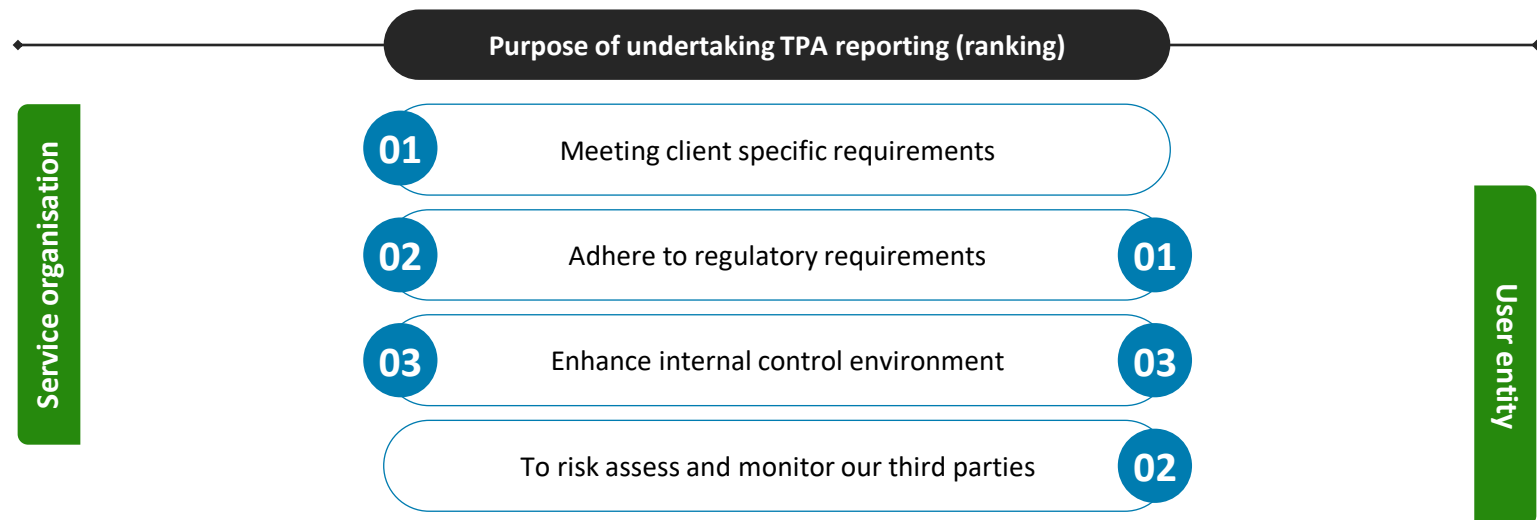
05. Monitoring activities

Respondents profile

Contacts

## Perspectives on TPA reporting | service organisation vs user entity

Service organisations and user entities have slightly different perspectives on the purpose of undertaking TPA reporting.



### Insights and perspectives

- The survey results indicate that from a service provider's perspective, '*Meeting client specific requirements*' is the key purpose for undertaking TPA reporting whereas user organisations believe that '*Adhering to regulatory requirements*' is the key objective.
- Traditionally**, TPA reports have been used as an **auditor-to-auditor tool** to communicate the effectiveness of Internal Controls over Financial Reporting (ICFR) between service organisations and their users (and user auditors). One of the most recognised global frameworks for this is SOC 1.
- However, the TPA stakeholder universe is growing and **additional stakeholders** (e.g., regulators, investors, and other nth parties) are now using TPA reports, and for **varying purposes**.
- One consequence of this misalignment in purpose and use is that the **efficiency benefits of undertaking TPA reporting is not always being realised**. For example, service organisations continue to have to respond to client specific contractual requirements (e.g. questionnaires) which can be burdensome and disruptive.
- Consequently, there exists an **opportunity** for TPA reports to be enhanced to make them **more fit for purpose** and allow TPA stakeholders to realise a greater number of benefits from TPA reports.

Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

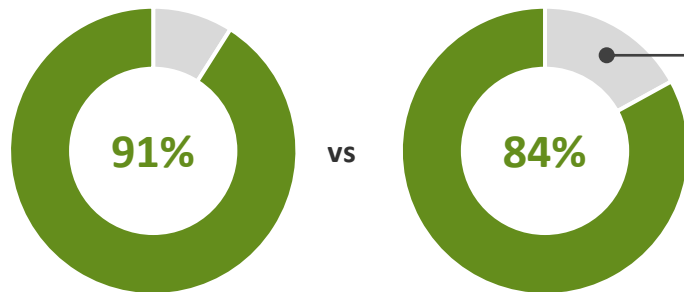
Contacts

## Perspectives on TPA reporting | service organisation vs user organisations

Users find TPA reports less relevant and valuable compared to service organisations, with understandability of scope, coverage, and the impact of control deviations being the most cited reasons for this.

### Relevancy and value of TPA reports

Based on both **current and emerging risks**, service organisations find TPA reports to be more **relevant and valuable** than users.



#### Service Organisation

**91%** find TPA reports 'mostly or very' relevant and valuable

**48%** find TPA reports to be 'very relevant'

#### Users of TPA

**84%** find TPA reports 'mostly or very' relevant and valuable

**35%** find TPA reports to be 'very relevant'

*Of the surveyed respondents, those from **Operations** roles (at both service organisations and user entities) found TPA reports to be least relevant and valuable.*

### Possible reasons for lower user relevancy and value

Of the 16% of users who said TPA reports were less relevant and valuable:

- 50% are **unsure or can not clearly understand the impact control deviations** or qualifications in TPA reports have on their organisations.
- 60% said TPA reports are **not easy to understand in terms of scope and coverage**.
- 80% said they were only able to **map CUECs** within service organisation reports to their own control environment **to a moderate - low degree**.

### Insights and perspectives

- There is an **opportunity** for service organisations and service auditors to **better describe the scope and coverage** of TPA reports and the **nature of control deviations** so that users can better understand the impact TPA reports have on their business, and what monitoring/follow up activities may be required.
- The **disparity** between the relevancy and value of TPA reports between users and service organisations may also stem from **other correlated results** to survey questions, including:
  - No user respondents from 2nd/3rd lines and finance/tax roles thought TPA reports meet all their requirements
  - 68% of respondents said there were 'some or no' controls related to KPIs over contract and/or service level compliance, suggesting they may not find TPA reports relevant and valuable in linking service provider performance with specific controls being assured.



Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

**03. Digital journey**

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

## 03. Digital journey



Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

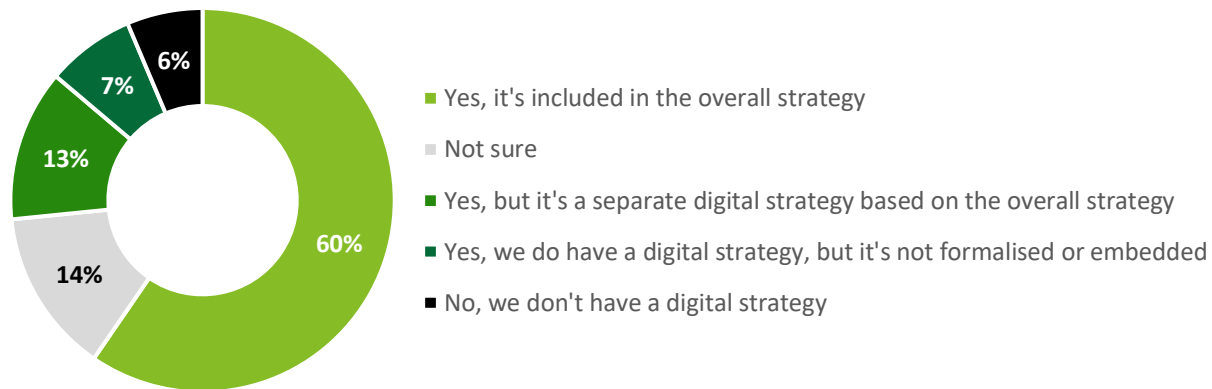
Respondents profile

Contacts

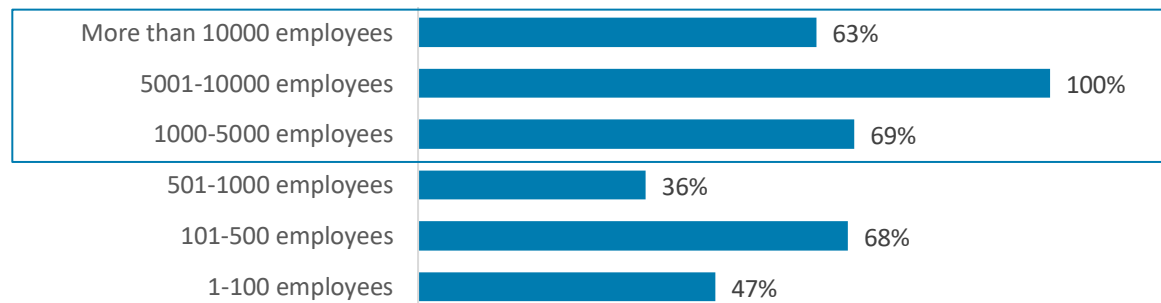
## Digital strategy

Digitisation presents great opportunity, but also brings significant new and unforeseen risks. As organisations digitally transform, so too must their control environments in order to keep pace with digital change. The scope of TPA reporting may need to change as new technologies and risks emerge.

20% of respondents do not currently have a digital strategy or are unsure whether they have a digital strategy



Larger organisations are more likely to have a digital strategy



### Insights and perspectives



- The survey results found that 80% of responding organisations have a digital strategy in place to some degree.
- Whilst most surveyed organisations have started the journey to develop a digital strategy and transform their business, **smaller organisations are less advanced.**
- Access to subscription-based or on demand technical capabilities (e.g. SaaS)** has resulted in huge growth in the use of digital technologies and data proliferation across the landscape. This has brought with it significant new risks and challenges to manage/monitor third parties.
- This also creates **data management and governance challenges** as organisations endeavor to manage data exposures across their third parties.
- A digital strategy that carefully considers these opportunities and risks is required to ensure appropriate governance and controls are designed, operated and evolved to **keep pace with digital transformation.**
- One way that organisations are seeking to achieve this is through the use of integrated monitoring/GRC tools (see page 16) and, more specifically, **continuous controls monitoring.**



Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

## Reporting in a connected ecosystem

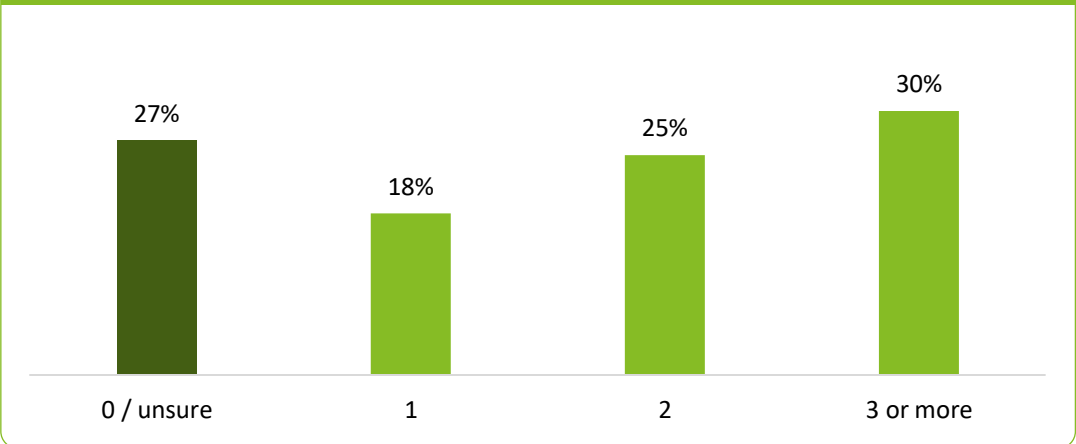
The use of hyperscalers is increasing post the COVID-19 pandemic as businesses increasingly move to outsourced technology services. While this can create many advantages, it also increases third-party risk

### Insights and perspectives



- Organisations are increasingly reliant on hyperscalers for reasons such as **convenience, scalability and security**.
- 73% of organisations are reliant on one or more hyperscaler. This provides the opportunity to leverage best-in-class services from a range of different providers. Using more than one hyperscaler also **reduces the single point of failure risk/increases redundancy**.
- While this is hugely beneficial for organisations, it also increases the potential for third party risks. Assessing cloud security risk in TPA reports will be key going forward as organisations look at **innovative ways to incorporate this into assurance reporting**.
- The 27% of the respondents who were either **unsure or said they used no hyperscalers** are largely from non-IT and/or smaller businesses. This may be indicative of one or more of the following:
  - Budget **constraints**.
  - **Definition** of the term ‘hyperscaler’ is evolving and not all organizations have built out their internal understanding of what constitutes hyperscalers and the support they provide, e.g. infrastructure vs cloud-based business applications.
  - **Under appreciation** of the potential benefit of hyperscalers.
  - Simply **no requirement** for hyperscalers at this time.

### 73% of organisations are reliant on hyperscalers\*



\* Hyperscaler refers to a mix of hardware and cloud platforms that can achieve significant scale in computing in a distributed computing environment.

Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

**04. Integrated monitoring tools**

05. Monitoring activities

Respondents profile

Contacts

## 04. Integrated monitoring tools



Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

## Deployment of integrated monitoring tools

Integrated monitoring tools, like GRC tools, are increasingly being used to manage and monitor risks and controls. However, more can be done to further integrate these into business operations.



### Insights and perspectives

- The survey results suggest that, while GRC tools are increasingly being adopted, it will take **more time for them to become fully embedded**, effectively linking risks, controls and technology landscapes.
- Automation through the use integrated monitoring tools also requires **significant education and upskilling**, as well as a **cultural shift**, and this can often lag behind the implementation of such technologies.
- From a Deloitte perspective, whilst some of our clients are using integrated monitoring tools to facilitate an efficient attestation/audit process, there still exists **significant opportunity** to:
  - Increase the use of integrated monitoring tools to **fast track** the attestation/audit process
  - Leverage these tools for a much **broader set of purposes** and for use by many stakeholders.
- Linked to this, Deloitte are seeing audit firms increasingly collaborating with tool providers to **integrate audit requirements** with business operations to **more efficiently access and test** information stored in systems.

### Top 3 ranked coverage areas for use of monitoring tools



ee

“Many organisations are using GRC tools, but most will not be maximising the benefits. In terms of my own organisation, rather than deploying a single holistic tool, we are leveraging a combination of smaller tools for specific purposes. Implementing one tool would be a major project as impacted team members would need to be on boarded and taught how to use the system and interpret the results.” – C-Suite Executive of a mid-sized organisation

99



Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

**05. Monitoring activities**

Respondents profile

Contacts

## 05. Monitoring activities



Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

## Monitoring activities

In a world where third party service providers are part of an extended enterprise, it is critical for organisations to ensure greater oversight and governance across the ecosystem. The majority of survey respondents are currently uncomfortable with the level of monitoring of nth parties. This exposes organisations to additional risk and compliance concerns.

### Insights and perspectives



- 51% of respondents are **uncomfortable** with the current level of monitoring of nth parties (i.e., third parties, fourth parties, and beyond). A **lack of insights** within available nth-party compliance / assurance reports is cited as one of the main reasons for this. Based on discussion with a selection of clients, Deloitte noted a **lack of availability** of assurance reports is also a possible reason.
- Despite this, survey respondents are mainly leveraging published reports and publicly available information to gain assurance **instead of performing direct procedures** (e.g., on site visits, interviews, etc.)
- Whilst this may be appropriate for some suppliers, it is unlikely this approach will be adequate for critical nth parties (e.g., those holding assets or customer data) – **the level of monitoring must be commensurate with the level of risk.**
- Relying primarily on the review of TPA reports for monitoring purposes also raises the issue of the **timeliness of monitoring.** Most service providers issue their TPA reports at a six- or 12-month cadence, with reports being released a number of months after period end. Is this timely enough to deal with potential outsourcing risk?
- For many third-party relationships, the answer is probably no, which further strengthens the **need for automation / real-time monitoring** of nth parties, with more timely flow of information between outsourcers and the outsourced.
- From a Deloitte perspective, we also find that monitoring of third parties is a focus for our clients but that this **does not always extend to fourth parties and beyond** – organisations often rely on their third parties to carry out this due diligence.
- Given the interdependencies within the outsourcing ecosystem and the operational, financial and reputational risks associated with this, there is a need for organisations to **look through the entire supply chain.**

### Monitoring activities performed to gain assurance over 'nth parties' ranked:

- 01 ➤ Review TPA reporting
- 02 ➤ Review relevant periodic reporting directly from nth party
- 03 ➤ Review market available news/information
- 04 ➤ Site visits/direct presentations/interviews with management | of the nth party

One client interviewed told us that: **“Third party monitoring is a focus area but it’s harder for smaller organisations who do not have the ability to influence change.”**

This is particularly relevant for large global service providers – **“we review their SOC reports but do not have the status to challenge the scope or demand more information on control exceptions.”**

99



Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

**Respondents profile**

Contacts

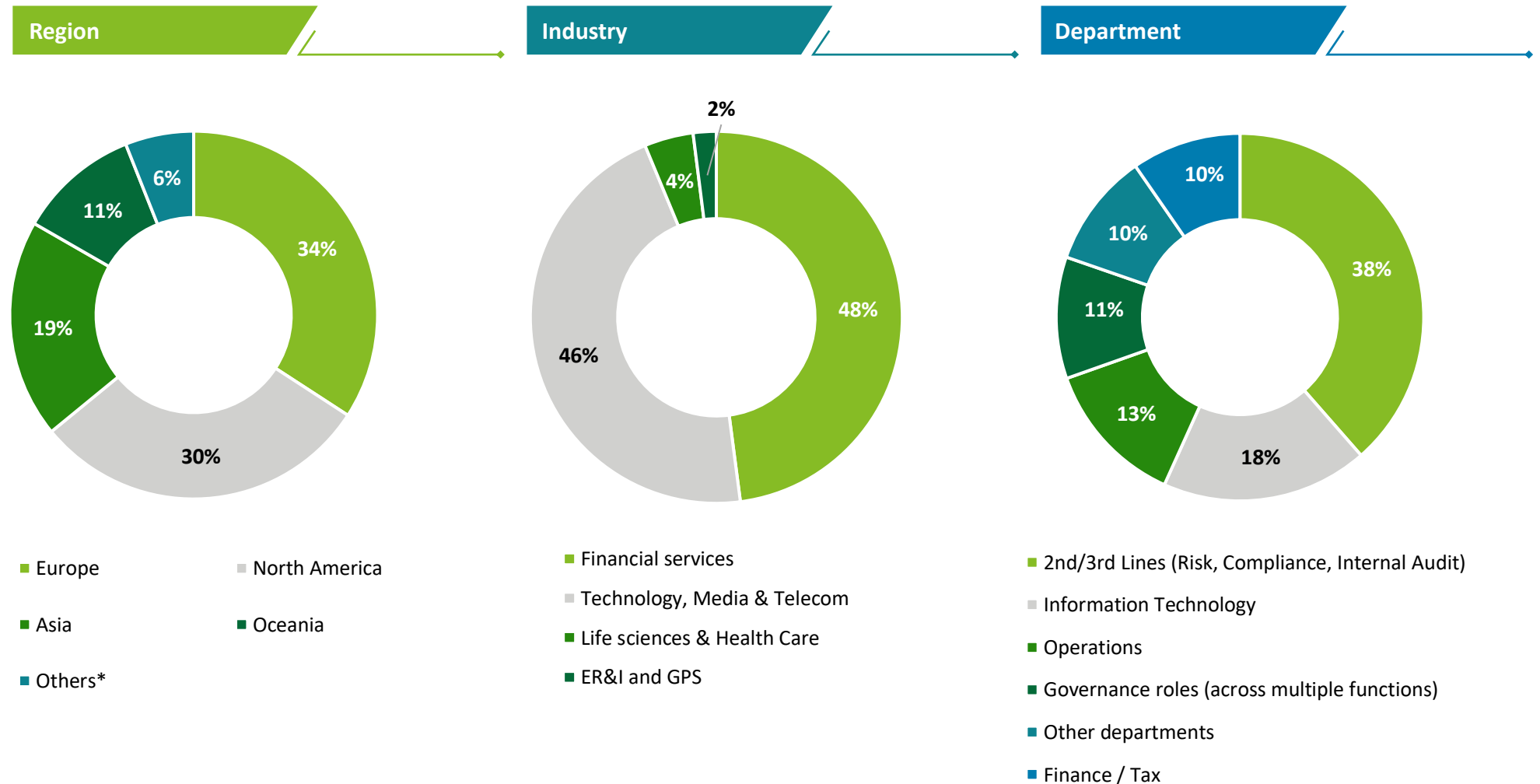
# Respondents profile





## Respondents profile (1/2)

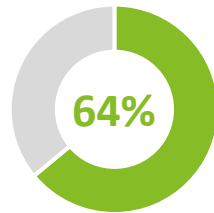
Deloitte received a wide range of responses from individuals across 14 countries. 64% of respondents were from either Europe or North America. 94% of respondents operated within either the financial services or TMT industries.



## Respondents profile (2/2)

The majority of respondents are from leadership roles in large organisations. Respondents were primarily users of TPA reports, or were both a service provider and user.

### Top 2 respondents by roles

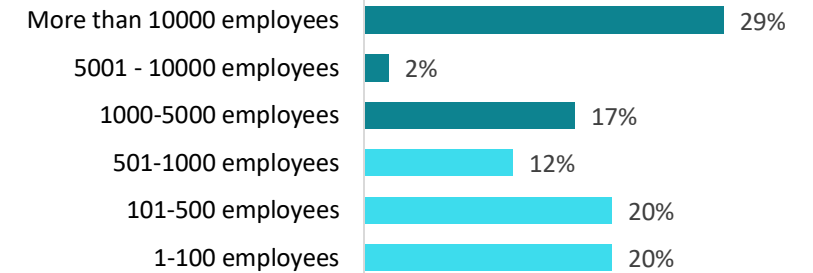


01. Head of Dept/Senior Manager/Manager

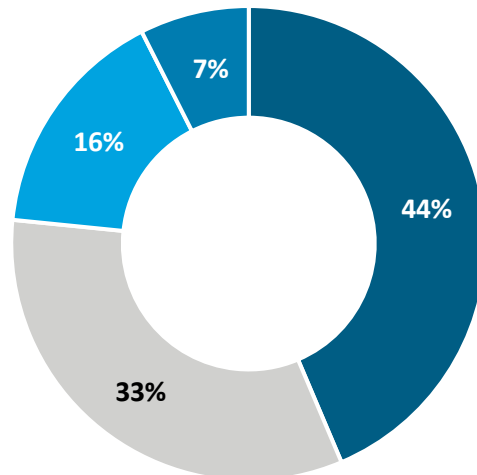


02. Non-executive Director

### Responses by size of organisations



### TPA profile



- Both a service provider and user of TPA reports
- A service provider who distributes TPA report(s)
- A user entity who receives TPA report(s)
- Neither

Foreword

Survey approach

Glossary of terms

Summary of key themes

01. Emerging areas of TPA reporting

02. Purpose, relevance and value

03. Digital journey

04. Integrated monitoring tools

05. Monitoring activities

Respondents profile

Contacts

## Contacts

Should you have any questions or would like to discuss this report further, please contact one of our team listed below.



**Michele Townsend**  
**Director**  
**Risk Advisory Africa**  
Mobile: +27 (0)82 441 7164  
Email: [mntownsend@deloitte.co.za](mailto:mntownsend@deloitte.co.za)

### East Africa



**Urvi Patel**  
**Emerging Technology Leader**  
**Risk Advisory East Africa**  
Mobile: +254 71 405 6887  
Email: [ubpatel@deloitte.co.ke](mailto:ubpatel@deloitte.co.ke)

### Central Africa



**Tricha Simon**  
**Risk Advisory**  
**Central Africa Leader**  
Mobile: +263 867 700 0261  
Email: [tsimon@deloitte.co.zm](mailto:tsimon@deloitte.co.zm)



**Jan Herbst**  
**Senior Associate Director**  
**Risk Advisory Africa**  
Mobile: +27 (0)83 609 1161  
Email: [jherbst@deloitte.co.za](mailto:jherbst@deloitte.co.za)

### West Africa



**Temitope Aladenusi**  
**Risk Advisory**  
**West Africa Leader**  
Mobile: +234 805 901 6630  
Email: [taladenusi@deloitte.com.ng](mailto:taladenusi@deloitte.com.ng)



**Trevor Wright**  
**Associate Director**  
**Risk Advisory Africa**  
Mobile: +27 (0)83 675 7997  
Email: [trewright@deloitte.co.za](mailto:trewright@deloitte.co.za)



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organisation”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organisation”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 312,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

This communication contains general information only, and none of DTTL, or the Deloitte organisation is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities

Liability limited by a scheme approved under Professional Standards Legislation.

© 2023 Deloitte Touche Tohmatsu Limited.