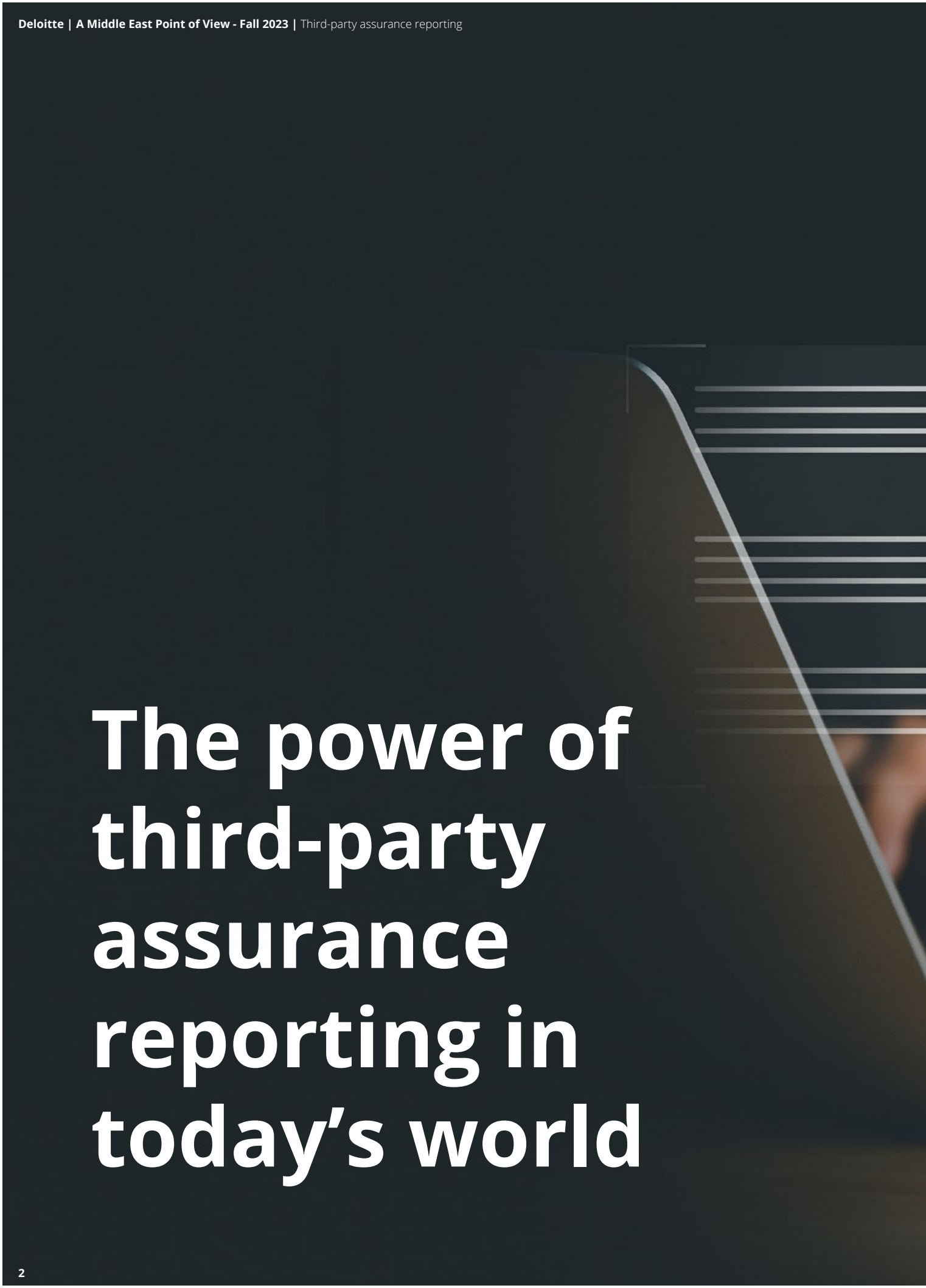

The power of third-party assurance reporting in today's world

Amid global megatrends and a connected financial landscape, organizations increasingly rely on third-party vendors for critical services. The Deloitte Global Outsourcing Survey 2022 indicated that 76% of global executives outsourced their IT services via third-party models, while 52% of global executives outsourced various business functions.[1]

Considering the growth of the outsourcing ecosystem, compliance pressures grow and regulations evolve. Customers now demand security and confidentiality assurances through third-party assurance reports, typically Service Organization Control (SOC) reports. These reports assess internal control effectiveness in meeting shared business objectives; they are also commonly used and requested, especially by service organizations serving customers across diverse regions.

SOC reports encompass three primary types: SOC 1, SOC 2, and SOC 3, each tailored to specific objectives and areas of emphasis. The below table provides insight into the differences between each type.[2]

SOC 1	SOC 2	SOC 3
Designed to assess the effectiveness of internal controls pertaining to financial reporting, making them particularly pertinent to financial processes such as payroll, accounting, and financial transaction processing.	Examination of controls related to specific trust categories; availability, processing integrity, confidentiality, and privacy of a service organization's systems and services.	Closely resemble SOC 2 reports but are intended for a broader audience. They provide a condensed overview of a service organization's controls without delving into intricate details.
Applicable to organizations providing services that could impact the financial statements of their clients, including third-party administrators, payment processors, and cloud service providers.	Well-suited for any organization that delivers services involving sensitive data or critical processes, such as data centers, managed IT services, or Software as a Service (SaaS) providers.	Similar to SOC 2 reports, SOC 3 reports apply to organizations offering services with an emphasis on security, availability, processing integrity, confidentiality, and privacy.
They delineate critical controls essential for ensuring financial accuracy and compliance while evaluating their design and operational efficiency.	Aligns with the Trust Services Criteria and evaluates controls related to security, availability, processing integrity, confidentiality, and privacy, depending on the specific criteria.	Evaluate controls based on the Trust Services Criteria, albeit in a less detailed and technical manner compared to SOC 2 reports.
Primarily serve the interests of the service organization's management, the service auditor, and the customers of the service organization.	Customers, business partners, and regulatory authorities commonly request and rely on SOC 2 reports to assess the security and privacy protocols of service providers.	Designed for public consumption and are frequently utilized for marketing purposes. They are openly accessible to anyone and offer a generalized assurance of a service organization's controls and practices.[3]

Disclaimer: SOC 1 and SOC 2 are terms used to distinguish between reports that focus on internal controls over financial reporting (SOC 1) and reports that focus on internal controls over data management (SOC 2). Not all reports across all regions use the SOC framework (e.g. under ISAE 3402, there are frameworks such as AAF 01/20 from the UK, GS 007 from Australia etc.), however for simplicity, we categorized the type of report framework as either SOC 1 or SOC 2.

Why third-party assurance reporting?
Third-party assurance reporting provides benefits to both service organizations and their customers. Some of the key benefits for service organizations who request third-party assurance reporting, explicitly SOC reporting[4], are:

- Positive SOC reports offer a competitive edge, showing dedication to security and reliability, attracting new clients, and increasing conversion rates.
- SOC reporting enhances credibility by providing high assurance on internal controls.
- Simplifies due diligence, reducing customer audit efforts, reassuring existing clients, and increasing customer retention rates.
- Helps meet compliance requirements, avoids legal issues, reduces audit costs, and enhances operational efficiency and risk management.

For businesses engaging with service organizations, some of key benefits of requesting SOC reports are:[5]

- SOC reports instill customer confidence in a service provider's commitment to security, reliability, and transparency.
- SOC reports provide insight into a service organization's controls, helping customers understand data handling and operations.
- Strong SOC reports build trust in data safeguarding, particularly for sensitive information.
- Relying on SOC reports instead of extensive audits leads to cost savings for customers, reducing expenses and administrative overhead.
- In regulated sectors, SOC reports serve as evidence of compliance with specific prerequisites, valuable for sensitive data or specialized industry regulations.

Third-party assurance attestation journey
For service organizations that are preparing to conduct SOC 1 , SOC 2, or SOC 3 attestations, and in order to move from the steady to the ready stage, there are key steps to be taken to accomplish an efficient assessment:

A. Define SOC report scope
B. Understand current state of controls
C. Assess design and implementation of controls
D. Identify gaps in achieving control objectives
E. Report to management with insight and recommendations for remediation

Upon completing the readiness assessment, service organizations will have the opportunity to showcase the level of effectiveness of their internal controls within the environment where customer data and information are hosted. If positive outcomes are confirmed in the report, this can position them as industry leaders, instilling confidence and trust among their customers.

Even if companies today are not yet prepared for third-party attestations, forward-thinking organizations are planning for the future.

Prior to jumping ahead in conducting an attestation assessment, companies can opt towards having a readiness assessment. Service organizations will be able to answer the following questions:

- Is my organization properly prepared for an SOC attestation?
- Are my relevant internal controls effective and policies in place?
- What are the key weaknesses present?
- How can those weaknesses be remediated before the attestation?

With this context in mind, Deloitte surveyed a sample of TPA reports (where permissible) from across the globe and from multiple industries to benchmark them and identify further insights and trends of key interest to the global TPA community. The key highlights from the benchmarking analysis of 98 sampled TPA reports include:

- TPA reports address internal control over financial reporting (ICFR) and operational areas but recently started to adapt more on emerging digital and cloud-related risks, requiring organizations to monitor and assess third-party risks amid the evolving risk landscape.
- Emerging risks and growing third-party reliance create an opportunity for TPA reports to offer assurance in broader areas, enhancing their value in the outsourcing ecosystem.
- Increasing awareness and use of SOC 2+ reports is driven by the growing compliance costs as organizations strive to meet customer, regulatory, and stakeholder demands. This trend is expected to result in continued demand growth.

In brief, as businesses expand within their respective markets, their dependence on service organizations for supporting their expanding operations intensifies. This heightened reliance raises critical concerns regarding the security and integrity of the data managed. Consequently, third-party assurance reporting addresses key inquiries, such as the security of data and the effectiveness of controls within the service organization responsible for businesses' information. As business navigates this landscape, fostering a proactive commitment from service providers to the robustness of internal controls environment fortify the foundation upon which successful business expansion rests.

By **Bhavna Lakhani**, Partner, Technology Assurance & Analytics, **Fadi Ghawi**, Director, Technology Assurance, and **Mais Barouqa**, Senior Manager, Technology Assurance, Deloitte Middle East

Endnotes

1. "Beyond outsourcing: Entering a new sourcing ecosystem,", Deloitte & Touche, 2022.
2. "Third- Party Assurance Engagement – SOC2," Deloitte & Touche.
3. "Third Party Assurance Engagement – SOC2," Deloitte & Touche.
4. "Providing Assurance through SOC Reports," Deloitte & Touche.