THIRD PARTY ATTESTATION

A STRATEGIC & SYSTEMATIC APPROACH TO MANAGING RISKS

BDO

FOREWORD

As management teams and boards of directors grapple with a rapidly evolving set of risks facing their companies, third party attestation has become an increasingly important tool for creating trust and efficiency across supply chains and vendor relationships.

Identifying and mitigating risk is one of the most critical issues facing organisations today. As the types and complexities of threats continue to multiply, it is increasingly difficult for management teams and directors to think strategically about risks and address them in a way that complies with the requirements of regulators and the needs of customers and other stakeholders. These challenges are particularly acute for businesses that outsource aspects of their operations, infrastructure and controls.

Third party attestation (TPA) involves certifying the business processes of outsourced service providers to ensure that proper procedures are being followed and that vendors can be trusted to complete their designated tasks.

TPA can play a critical role in helping business leaders think holistically about the risks their organisations face while also bringing rigour and discipline to the company's risk management and compliance efforts both for their outsourced providers as well as for their own internal processes.

In this paper, we provide an overview of TPA and discuss the benefits of System and Organisation Controls (SOC) reports as a key risk management tool. We describe how TPA can help you strengthen your business practices, maintain compliance where applicable, and build trust with your constituents. We then explore trends and emerging risks in several critical areas, ranging from protecting against cyberattacks to offering more transparent environmental, social, and governance (ESG) reporting. Finally, we outline how BDO's TPA services are uniquely positioned to help your company navigate risks in an increasingly complex global framework.

Key terms

Third party attestation:
Certifying the business processes of outsourced service providers to ensure that proper procedures are being followed and that the vendor can be trusted to complete their designated tasks.

System and organisation Controls (SOC) reports:
Written affirmation certifying the vailidity of internal process or attesting that an external party has proper procedures and controls in place to perform an outsourced function.

Type I attestation:
The design and implementation of relevant control procedures are confirmed and TPA Type I ('point in time') report is issued.

Type II attestation:
The operating effectiveness of control procedures are reviewed and TPA Type II ('period of time') report is issued.

THE BENEFITS OF TPA AND SOC REPORTS IN AN EVOLVING WORLD

TPA can help businesses focus on their core areas of strength while providing peace of mind when they outsource certain processes or tasks to external specialists. For example, an online retailer may have expertise in sales and marketing, but may lack internal employees with the skillset to prevent data breaches or protect customer data. As a result, the online retailer may outsource those activities to a dedicated managed security services provider with cybersecurity expertise.

Outsourcing this function, however, brings along its own risks. These include reputational, control, compliance, privacy, financial and operational risks. For instance, if the retailer were compromised by a cyberattack, its systems could be offline and inaccessible until the situation is resolved. In addition, proprietary customer data, including personally identifiable information (PII), could be accessed and exposed by the hackers. A data breach could lead to reputational damage, as well as direct and indirect financial costs due to potential loss of business, lawsuits, fines, or other regulatory penalties.

When entrusting outsourced functions like cybersecurity to a third party, a company needs assurance that the provider can adequately protect those valuable assets.

To conclude: **while you can outsource certain activities, you cannot outsource their accompanying risks.**

How TPA can help you

TPA offers an objective lens to certify that processes whether internal or done by third parties consist of best practices and follow adequate controls. In our example, the managed security services provider could use TPA to certify that it has the required operations, controls, and technology in place to proactively combat cyberattacks and safeguard against data breaches. In this scenario, the online retailer can rest assured that an objective party has reviewed and approved its vendor's capabilities. While there is no guarantee that the retailer will be protected from a breach or other security incident, the company has assurance that it indeed hired a certified expert to protect itself.
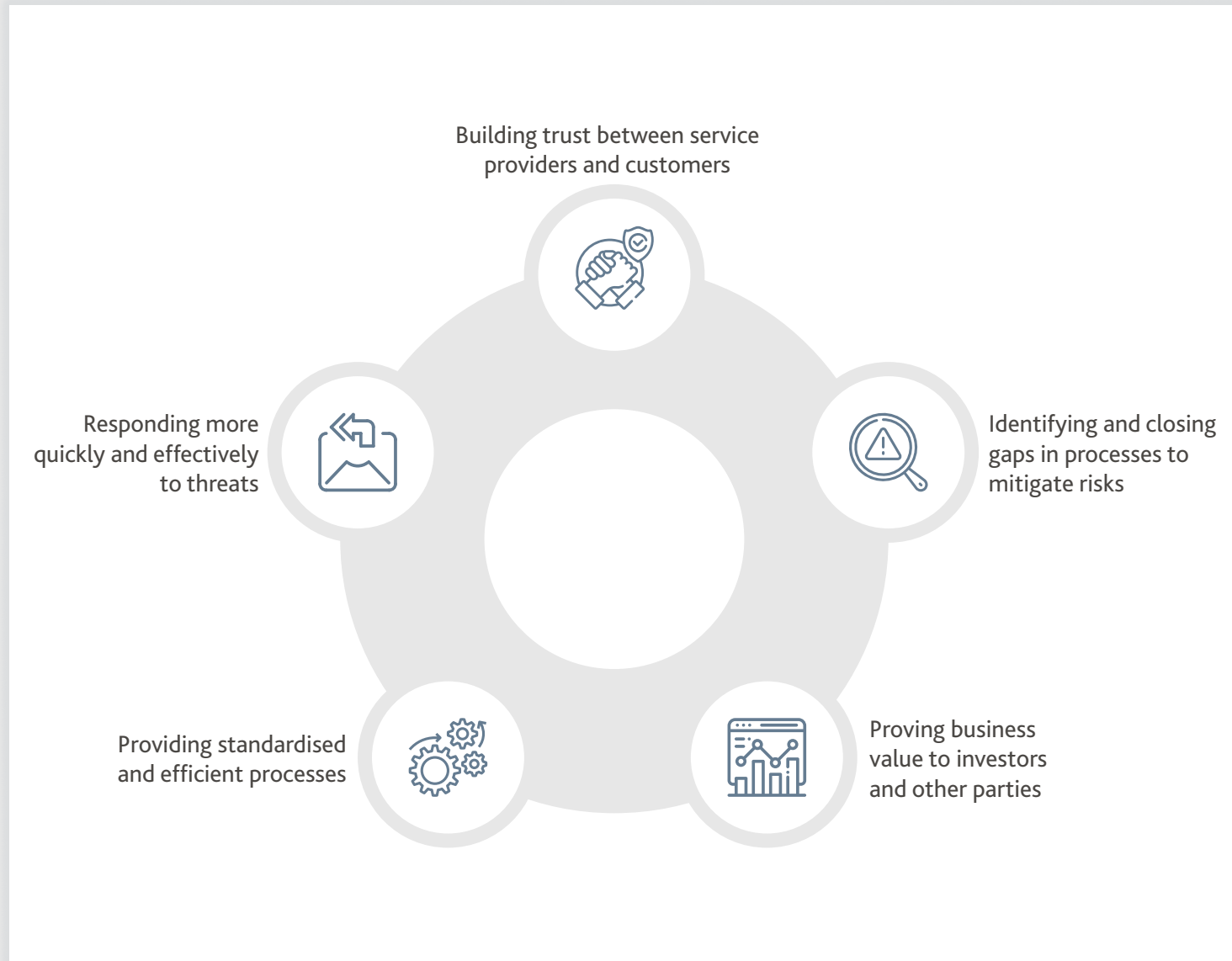
Benefits of third party attestation

For a service provider, TPA can provide an objective 'stamp of approval' that its controls and business processes are adequate. All service providers in theory can benefit from investing in TPA. Especially those operating within regulated industries such as financial services or fintech and technology providers (including cloud and SaaS operators), active in the TMT industry, have this on their radar. Achieving TPA can provide these organisations a competitive advantage, as many companies seek to hire service providers that are TPA-certified.

In this type of situation, service providers like the managed security service provider in our example above often look to companies like BDO to create SOC reports. SOC reports provide written affirmation certifying the validity of internal process or attesting that an external party has proper procedures and controls in place to perform an outsourced function. There are many types of SOC reports available, but at their heart, all SOC reports aim to build trust and allow companies to conduct business with more confidence. On the next page, we discuss several key benefits of SOC reports.

# KEY BENEFITS OF SOC REPORTS ACROSS THE VALUE CHAIN

Building trust between service providers and customers

Responding more quickly and effectively to threats

Identifying and closing gaps in processes to mitigate risks

Providing standardised and efficient processes

Proving business value to investors and other parties

Building trust

In today's global economy, companies absolutely need to trust their counterparties to conduct business. This is even more critical when operating across a broad range of jurisdictions and in varied domestic and international regulatory environments, as well as in an increasingly virtual environment.

In these circumstances, SOC reports can provide objective verification that service providers comply with a wide variety of regulations. SOC reports have become a must-have in many vendor management and RFP processes, opening the door to more business opportunities without the need to start from scratch for each inquiry or request. When it comes to building trust, SOC reports play a critical role ultimately reducing compliance efforts each year and leading to fewer onsite vendor or partner audits. By fostering trust, SOC reports enable more efficient and potentially profitable ways for companies to conduct business with each other.

Identifying and closing gaps

Having a third party examine organisational controls can determine whether systems are designed, implemented, and operating as expected, as well as how they can be improved. A SOC report can indicate where and when there are breakdowns in controls that could possibly lead to a business disruption, allowing service providers to proactively mitigate these risks. In addition to highlighting shortcomings, SOC reports can also focus on strengths in a service provider's processes and controls and offer guidance on how to improve areas that require more attention.
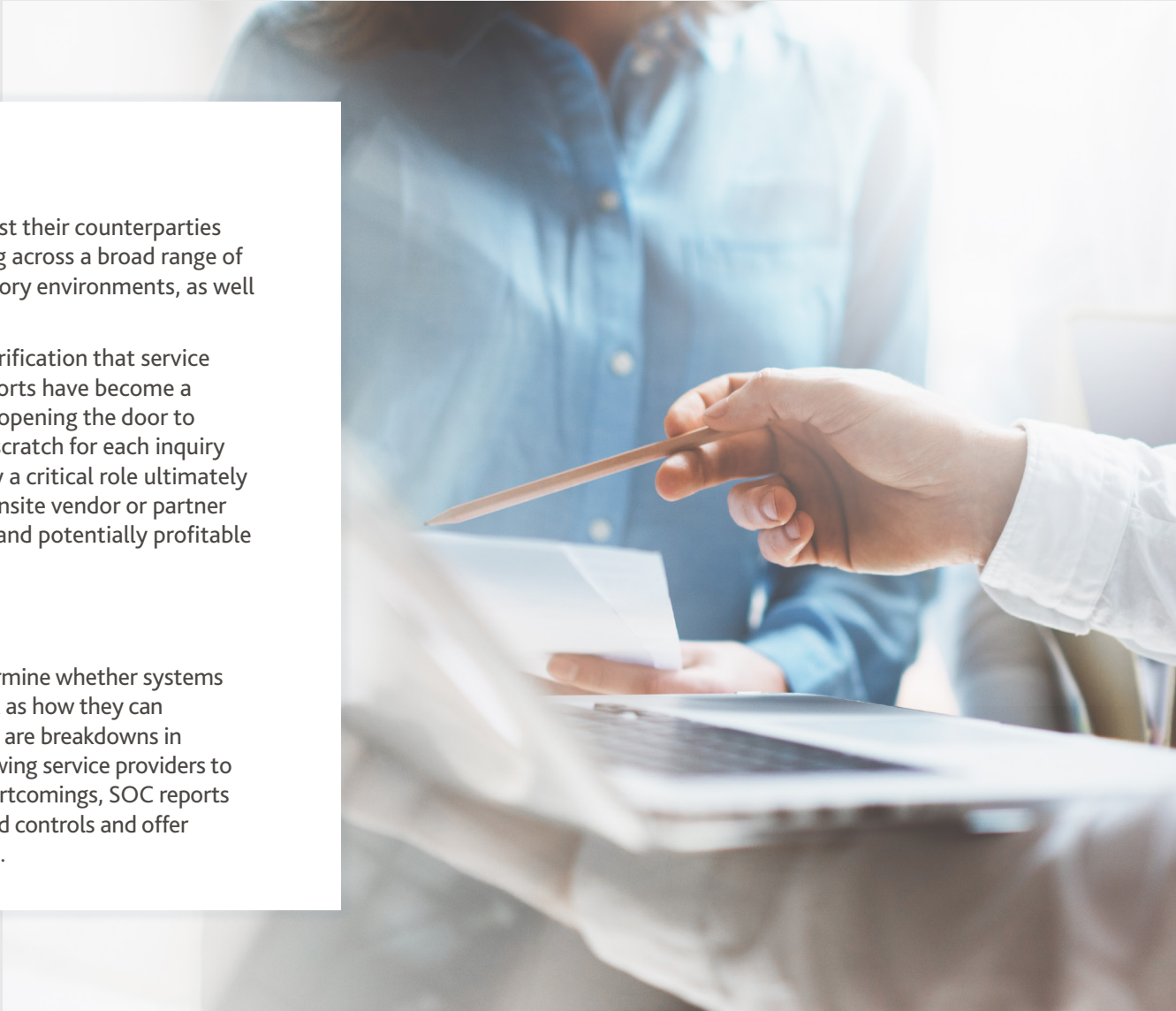
Proving business value

SOC reports can provide a good signal of corporate health for both service providers and the companies that hire them. As mentioned above, many companies seek out service providers that are objectively certified as experts in certain areas. SOC reports for service providers can be valuable when service providers are planning a strategic event, such as an initial public offering (IPO) or a sale, as SOC reports are commonly used by investors in the due diligence and valuation process. Investors often look at the effectiveness of risk management programs as an indicator of shareholder value.

Responding efficiently and effectively to threats

Improved efficiencies can also help organisations more quickly and effectively respond to threats. No matter how well you are prepared, incidents are likely going to occur, so the speed at which you can respond and mitigate the damage is essential. SOC reports that identify risks and put response measures/plans in place before an incident occurs allow organisations to be more proactive rather than just reactive. This preparation can be crucial in facilitating a nimble response, particularly when time is of the utmost essence.
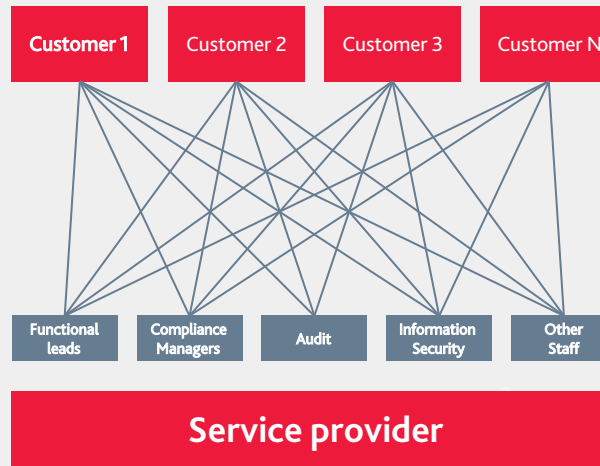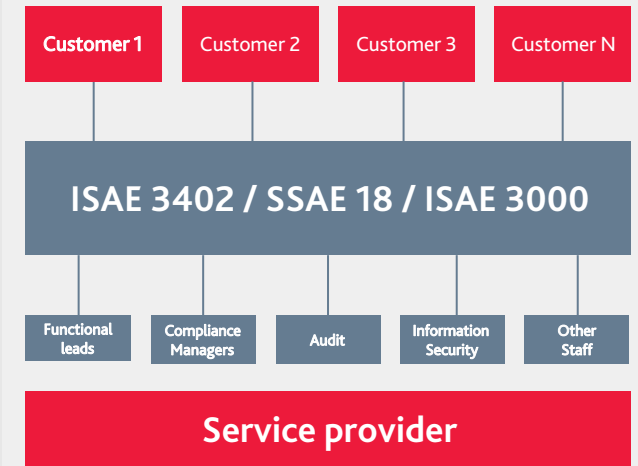
SOC REPORTS STREAMLINE PROCESSES

Providing standardised and efficient processes

SOC reports also allow for more standardised and efficient processes, potentially leading to time and cost savings. These figures, the 'SOC reports streamline processes,' shows how SOC reports can create more streamlined processes, allowing for faster everyday business operations. The diagram on the left illustrates a tangled web of one-off requests, questions, and audits that require responses by several different internal parties. Without a systematised approach, these requests can overwhelm resources and potentially lead to interruptions and delayed response times to customers or prospects. The diagram on the right shows how SOC reports can significantly simplify and standardise request streams. By creating a SOC report that clearly lays out required procedures in advance, you can limit the ad hoc nature of requests or questions and allow for faster and nimbler responses. This can also save time for your internal parties and allow you to better serve customers and prospects.

Situation without SOC report: separate requests, leading to inefficiencies

Customer 1	Customer 2	Customer 3	Customer N

Functional leads	Compliance Managers	Audit	Information Security	Other Staff

Service provider

Situation with SOC report: An efficient and standardised approach

Customer 1	Customer 2	Customer 3	Customer N

ISAE 3402 / SSAE 18 / ISAE 3000

Functional leads	Compliance Managers	Audit	Information Security	Other Staff

Service provider

WHICH SOC IS RIGHT FOR YOU?

With SOC 1, SOC 2, SOC 2+, SOC 3, SOC for Cybersecurity, and SOC for Supply chain, it can be challenging to determine which report best addresses a business needs. Consider the risks your organisation seeks to dispel – and who needs assurance that your company has the right controls in place.

	SOC 1	SOC 2	SOC 2+	SOC 3	SOC for Cybersecurity	SOC for Supply Chain
WHO IS THIS SOC FOR?						
A Service Organisation (One that provides services to user entities)	●	●	●	●		
Any Type of Organisation					●	
An entity that produces, manufactures, or distributes products						●
REPORTS ON AN ORGANISATION'S...						
Financial Reporting	●					
Security		●	●	●	●	●
Availability		●	●	●	●	●
Process integrity		●	●	●		●
Confidentiality		●	●	●	●	●
Privacy		●	●	●		●
DISTRIBUTION						
Restricted (users)	⊕	⊕	⊕			⊕
Unrestricted (general use)				●	●	

TPA IN ACTION: TRENDS AND DEVELOPMENTS ACROSS FUNCTIONAL AREAS

TPA and SOC reports can be implemented in many ways. Here, we highlight recent developments across several areas and discuss how TPA can help you gain a more holistic and integrated view of all the risks facing your organization and its stakeholders.

Cybersecurity and artificial intelligence

Technological innovations require organisations to navigate new and unfamiliar areas, many of which have the potential to both create opportunities and expose vulnerabilities. In an increasingly digital world, protecting against cyberattacks and leveraging the power of artificial intelligence are two evolving areas that require special attention. Advances in technology allow attackers to use new tools and techniques to steal valuable data and even hold entire organisations hostage via ransomware.

While there is no way to fully prevent cyberattacks, TPA helps service providers validate that they have processes and controls in place to stay a step ahead of threats, or at least have built-in procedures to respond quickly and efficiently once they occur. The TPA report should clearly establish steps for monitoring, addressing, and eradicating incidents to provide a blueprint for protecting against and responding to cyberattacks. For example, when an organisation outsources security-related activities to a managed security services provider, a TPA report brings assurance that security controls are implemented and security tasks are performed with due care.

The continued growth of artificial intelligence (AI) and machine learning (ML) can unlock opportunities for businesses seeking to automate tasks and gain more insight into their customers, among many other applications. But even as leveraging big data can help companies expand into new areas, it can also lead to unexpected risks. For example, there has been controversy and increased political interest in the use of AI-driven algorithms in employment screening[1]. Other companies have faced lawsuits and been forced to pay massive settlements for using AI in facial recognition software[2].

With new technologies accelerating at an increasing rate — and an uncertain and evolving regulatory landscape — you need experts to help you identify and adapt to these new types of risks. Hiring a TPA provider with expertise in artificial intelligence can help you avoid known risks while preparing you for emerging risks that may not even be on your radar.

[1] https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/ai-based-hiring-concerns-academics-regulators.aspx
[2] https://www.cnet.com/news/facebook-privacy-lawsuit-over-facial-recognition-leads-to-650m-settlement/

Data privacy

Data privacy poses several challenges and has already drawn significant political and regulatory attention. Unlike a tangible item, data is not contained within a certain territory or nation. As a result, the same piece of data may be regulated differently in Europe, the United States, and Asia. Multinational organisations operating across jurisdictions need to make sure they comply with all the relevant data privacy frameworks.

- In the European Union, violating General Data Protection Regulation (GDPR) requirements can lead to fines and other penalties.

- In the United States, there is no central data privacy regime; a patchwork of regulations across numerous states and cities makes the complex task of staying compliant even more difficult. Especially when personal data is exchanged between an organisation (the controller) and a service provider (the processor), special attention on data privacy is required. The organisation should verify that the service provider is compliant and that its processes are in accordance with the relevant data privacy legislation. This verification can be achieved through SOC reports.

Data privacy laws also continue to evolve, so it is imperative to stay on top of new developments and regulatory trends. Ensuring that your organisation or third-party vendor is compliant with the various relevant jurisdictions requires a comprehensive data governance framework and experts with a breadth of knowledge of global regulations as well as in-depth industry acumen.

Supply chain management

Global supply chains are often extremely sophisticated and complex. Companies need to be able to rely on multiple third parties to fulfill the promises to their own customers. Organisations that manufacture and distribute products across geographies need to be able to trust their suppliers and other counterparties, regardless of where they are located. While gaining new business partners can allow for time savings, expansion opportunities, and the potential for greater profits, these relationships can also lead to unforeseen risks. For example, your company may not be able to meet its commitments due to an unexpected delay by a partner or a delivery of materials that do not meet your specific requirements.

One way to mitigate these types of risks is through a reporting framework that introduces more transparency into the global supply chain. Supply chain-specific SOC reports help manufacturers and related parties identify gaps and develop a plan to close them. The reports can be customised for specific purposes while following standardised and approved methodologies. The result is a higher level of trust and the potential to ease some of the complications of the global supply chain.

Regulatory compliance

Across industries, service providers can benefit from SOC reports that certify their compliance with various regulatory regimes. This is especially true in heavily regulated areas such as healthcare, financial services, utilities and telecommunications, among others. For example, a U.S.-based healthcare service provider may seek a SOC report that certifies its compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations. Likewise, a service provider that works with financial institutions would likely want to confirm that its processes comply with U.S. Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA) stipulations.

SOC reports can be especially valuable for companies operating in multiple regulatory environments. As the world becomes increasingly interconnected, a company with a global customer base needs to ensure that its data privacy policies comply with laws in specific geographies. For instance, companies with customers in the European Union need to be GDPR-compliant, even if they are domiciled outside of Europe. A SOC report certifying this compliance can both protect the company as well as potentially offer a competitive advantage for new business opportunities. In some cases, regulatory bodies require that service providers prove that they comply with the appropriate regulations in their jurisdictions. Again, SOC reports can serve to fulfill these requirements.

Evolving ESG transparency demands

Environmental, social, and governance (ESG) reporting has been in place for several decades and will take on even more prominence in the years ahead. Many private and listed companies are undertaking ESG initiatives to highlight how they are contributing to the community and protecting the environment.

But even as investors, consumers and regulators demand more transparency into corporate ESG practices, there is still no standard ESG reporting template. Many regulatory bodies — from the European Commission to the International Financial Reporting Standards Foundation — and nonprofit advocacy organisations — such as the Sustainable Accounting Standards Board, the Global Reporting Initiative, and the Climate Disclosure Standards Board — have issued separate standards and priorities for ESG reporting. The lack of consistency highlights the challenges facing companies trying to keep up with the rapidly evolving ESG reporting landscape.

Increasingly, companies are using TPA to communicate their commitment to sustainability and social practices to investors and other parties. An objective certification of strong ESG principles can help companies stand out and potentially enhance their reputation with the public and with regulators.
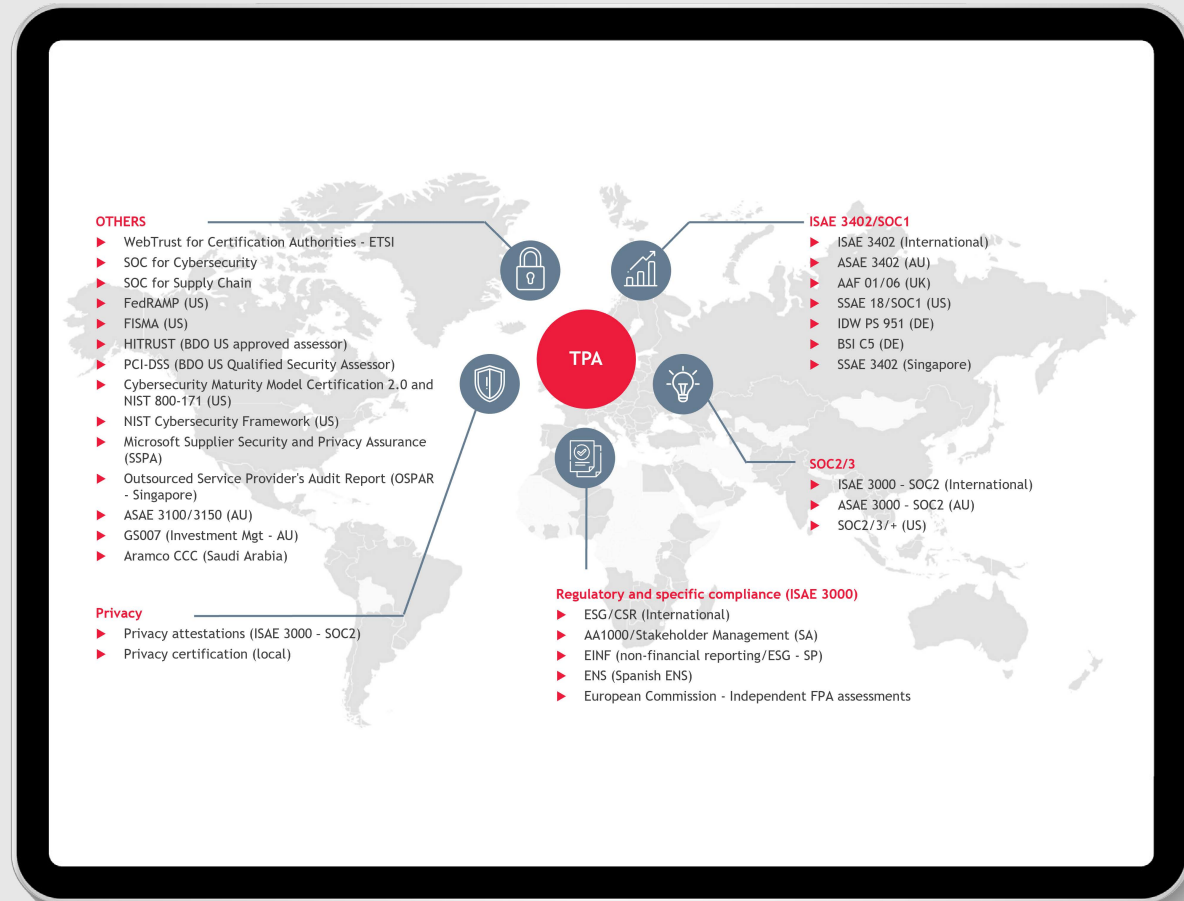
THE NEED FOR EXPERTISE TRANSCENDING GEOGRAPHIES AND INDUSTRIES

The need for expertise transcending geographies and industries

TPA can allow you to better identify and manage risks both in your organisation and for your external vendors. As challenging as staying at the leading edge of risk management and compliance is for any organisation, this burden grows exponentially for organisations operating across multiple countries and/or across multiple industries. That is why it is important to partner with an assurance provider whose capabilities are truly global—both in terms of their geographic reach and industry expertise.

At BDO, we have dedicated TPA professionals in every major region of the world with deep experience working in the industry verticals that we serve. BDO understands varying international standards and works with clients to determine the most appropriate standards to adopt. These professionals are backed by a global assurance practice that includes deep expertise in all the primary areas of TPA. Whether you are looking for TPA for your own internal processes or for external vendors, we have the expertise and breadth of experience to help you navigate a complex world full of both opportunities and threats.

BDO's global TPA capabilities and resources

OTHERS
- WebTrust for Certification Authorities - ETSI
- SOC for Cybersecurity
- SOC for Supply Chain
- FedRAMP (US)
- FISMA (US)
- HITRUST (BDO US approved assessor)
- PCI-DSS (BDO US Qualified Security Assessor)
- Cybersecurity Maturity Model Certification 2.0 and NIST 800-171 (US)
- NIST Cybersecurity Framework (US)
- Microsoft Supplier Security and Privacy Assurance (SSPA)
- Outsourced Service Provider's Audit Report (OSPAR - Singapore)
- ASAE 3100/3150 (AU)
- GS007 (Investment Mgt - AU)
- Aramco CCC (Saudi Arabia)

ISAE 3402/SOC1
- ISAE 3402 (International)
- ASAE 3402 (AU)
- AAF 01/06 (UK)
- SSAE 18/SOC1 (US)
- IDW PS 951 (DE)
- BSI C5 (DE)
- SSAE 3402 (Singapore)

TPA

SOC2/3
- ISAE 3000 - SOC2 (International)
- ASAE 3000 - SOC2 (AU)
- SOC2/3/+ (US)

Privacy
- Privacy attestations (ISAE 3000 - SOC2)
- Privacy certification (local)

Regulatory and specific compliance (ISAE 3000)
- ESG/CSR (International)
- AA1000/Stakeholder Management (SA)
- EINF (non-financial reporting/ESG - SP)
- ENS (Spanish ENS)
- European Commission - Independent FPA assessments

Local presence in every region

North America: 150+ staff **Europe**: 320+ staff **Asia Pacific**: 80+ staff **South America**: 30+ staff **Africa**: 35+ staff

CONTACTS

Country	Key contact	
Australia	Sean Pascoe, Partner	sean.pascoe@bdo.com.au
Belgium	Christophe Daems, Global TPA workgroup leader	christophe.daems@bdo.be
Canada	Sam Khoury, Partner	SKhoury@bdo.ca
Cayman Islands	Muzaffar Soomro, Partner	msoomro@bdo.ky
Czech Republic	Martin Horicky, Partner, Digital services	martin.horicky@bdo.cz
Denmark	Mikkel Jon Larsen	MLA@bdo.dk
Germany	Luc Ernes, Partner	luc.ernes@bdo.de
Hong Kong	Ricky Cheng, Director and Head of Risk Advisory	rickycheng@bdo.com.hk
India	Vishal Shah, Partner	VishalShah@bdo.in
Ireland	Brían Gartlan, Partner	bgartlan@bdo.ie
Israel	Tal Dolev, Partner	TalDo@bdo.co.il
Japan	Yusuke Chifuku, Manager	chifuku@bdo.or.jp
Jersey	Tanya Grove, Manager	tgrove@bdo.je
Luxembourg	Benoit Wtterwulghe	Benoit.Wtterwulghe@bdo.lu

Country	Key contact	
Malaysia	Sanjay Sidhu	sanjay@bdo.my
Malta	Ivan Spiteri	ivan.spiteri@bdo.com.mt
Morocco	Zayed Fahim, Manager	zayedfahim@bdo.ma
Netherlands	Jeroen van Schajik, Partner IT audit	jeroen.van.schajik@bdo.nl
Norway	Siv Irene Aasen, Partner	siv.irene.aasen@bdo.no
Pakistan	Shoukat Shah	sshah@bdo.com.pk
Singapore	Willy Leow, Partner	willyleow@bdo.com.sg
Slovenia	Manuela Sribar	manuela.sribar@bdo.si
South Africa	Suman Moonilal, Manager	Smoonilal@bdo.co.za
Spain	Enrique Turrillo, RAS IT Director	enrique.turrillo@bdo.es
Suriname	Anamika Mangroo, Director	anamika.mangroo@bdo.sr
Switzerland	Reto Buergi	Reto.Buergi@bdo.ch
UK	Fiona Davis, Partner	fiona.davis@bdo.co.uk
USA	Jeff Ward, Partner Josh Ayers, Partner	jward@bdo.com jayers@bdo.com

BDO

www.bdo.global

BDO