Why Attestation Services Are Becoming More Important for Tech

Third-party attestation (TPA) reports prove to a company's customers and stakeholders that it has the proper internal controls to meet compliance requirements, and more importantly, its customers' expectations, as well as mitigate risk.

Depending on the organization's needs, attestation services can take the form of system and organization controls (SOC) reports, International Organization for Standardization (ISO) certifications, HITRUST certifications, and other types of assessments or reports.

Attestation reports are essential for tech companies, especially software as a service (SaaS) and other "x-as-a-service" providers. This is because across industries, most companies work with "x-as-a-service" providers routinely to meet their needs by partnering with SaaS, platform-as-a-service (PaaS), AI-as-a-service (AIaaS), or infrastructure-as-a-service (IaaS) and other XaaS providers. Examples include customer relationship management systems, cybersecurity management systems, payroll providers, and other third-party systems that many companies rely on to run their businesses. This creates increased connectivity between two or more organizations, throughout a given data's life cycle, which often means greater vulnerability to or increased access points for threat actors. Every organization, as well as every SaaS, PaaS, IaaS, AIaaS, or other XaaS provider that is part of the data's life cycle shares in the responsibility of data protection throughout the given data's life cycle, whether it be to comply with applicable laws and regulations, or for contractual, professional, or other business requirements.

To uphold their shared responsibility, each provider involved must have an effective internal control system to ensure they do their part to maintain the integrity of increasingly connected networks. Because of this, many tech companies face mounting pressure from their stakeholders to obtain appropriate assurances aligned with their interests and pursue TPA reports and certifications to vet their systems and related controls.

Today, there are even more "x-as-a-service" providers in the market than there were just a few years ago, meaning the need for attestation services has grown substantially. Any company that does the following likely needs TPA reports and certifications:

Controls systems of data

Has access to personally identifiable information or electronic protected health information (ePHI)

Processes financial information

Logically or physically stores another organization's data and/or systems

Given those identifiers, this means many — if not most — tech/XaaS companies qualify for and would stand to benefit from attestation services

Why Tech Companies Face Mounting Pressure for Attestation Reports

Pressure for attestation is coming from all angles.

In the current landscape, many tech companies find that their customers require them to obtain attestation reports or certifications. In particular, enterprise-level, sophisticated customers are increasingly demanding assurance to verify the tech company's control environment. These stakeholders view SOC reports and other third-party assessments as table stakes.

Venture capital (VC) firms are another stakeholder increasingly mandating assessments by a third party. VC firms are pushing their startups to get SOC certified with either or both SOC 1 and 2 reports. VCs know that not being SOC certified may cause roadblocks at exit. Tech companies seeking VC or private equity (PE) investment, or those generally planning for an exit, would be wise to proactively pursue attestations, as it may help demonstrate value ahead of fundraising or dealmaking.

Regulators and new compliance mandates also increase the need for attestation services. Industries dealing with sensitive customer information, such as healthcare and financial services, will find regulators will scrutinize data privacy and protection controls. Take the Health Insurance Portability and Accountability Act (HIPAA) as an example. Tech companies operating in the healthcare space may find a HITRUST certification is an effective way to demonstrate rigorous data protection and privacy controls are in place while also meeting HIPAA compliance demands.

Now, the regulatory microscope is particularly focused on artificial intelligence (AI), given the appetite across industries for generative AI adoption. The European Union (EU) Council recently approved **the AI Act** — a landmark law that establishes comprehensive rules for and strict guardrails around AI use. As the first of its kind, the EU AI Act will regulate AI via a "risk-based approach" that considers the different applications of AI and the associated risks or threats posed to society. Multinational tech companies with EU exposure will need to comply with the Act, which highlights the importance of putting robust internal controls and processes in place around AI operability.

Global regulations often influence U.S. regulations. The EU AI Act may be a sign of what's to come in the U.S., leading to more robust AI regulation in the states. Already, there has been proactive movement within the U.S. government, prompted by President Joe Biden's **executive order** on AI from October 2023. Many government agencies have taken strides to meet various provisions of the sweeping executive order, such as submitting **AI-system risk assessments** to the Department of Homeland Security.

At the same time, the U.S. has seen state-level laws come into play, such as New York City's Automated Employee Decision Tool law. This NYC law mandates an annual audit of technology for local employers using AI as part of their hiring process.

For tech companies planning to expand internationally, it is essential to build room for compliance assessments and attestation into project timelines. But even organizations without a global presence should pay attention as AI regulations are likely to become more prevalent and far-reaching within the U.S. New tech innovations, such as generative AI, come with inherent risks. Third-party attestation can help mitigate those risks by ensuring a tech company using AI or offering AI-as-a-service is doing so in a compliant, ethical manner and that appropriate processes are in place to maintain data integrity.

What Tech Companies Can Gain by Pursuing Third-Party Attestations

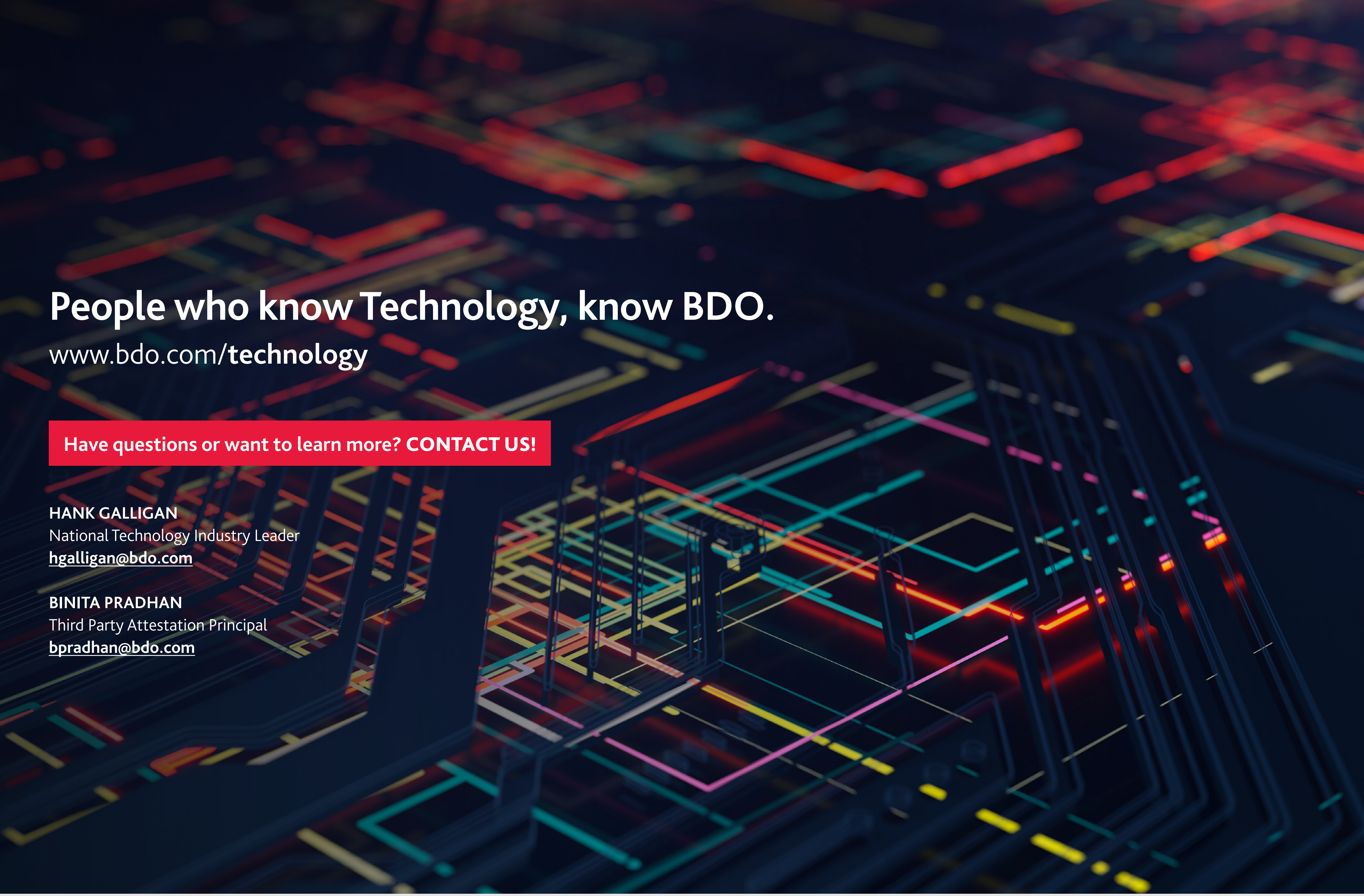
Tech companies that forgo attestation services risk losing customers, jeopardizing trust, or limiting their ability to grow. As customer demand for SOC reports and other forms of attestation increases, companies must meet these expectations to retain their current customers and win new ones. Beyond this, tech companies that do not pursue attestation risk violating contractual mandates or regulations, which could result in fines and reputational damage to the brand.

There are many benefits to pursuing TPA, including:

- Enhancing organizational risk management processes
- Providing a competitive advantage
- Demonstrating value for dealmaking
- Promoting compliance with data privacy regulations, which is critical for tech companies managing troves of sensitive personal data
- Establishing trust between the organization and stakeholders via independent, third-party verification

At BDO, our Third-Party Attestation team focuses on providing fair and balanced compliance assessments that help build trust with your stakeholders. Our industry specialists can work with your team to deliver assurance to your customers by verifying your internal controls and systems, as well as identifying areas for improvement to better protect sensitive data. From there, we work with your teams to remediate issues and finetune processes that can, ultimately, help you grow your business.

Selecting a data privacy and reporting framework can be complex. Check out our insight to discover which framework is right for your organization. ▶



People who know Technology, know BDO.

www.bdo.com/**technology**

Have questions or want to learn more? CONTACT US!

HANK GALLIGAN
National Technology Industry Leader
hgalligan@bdo.com

BINITA PRADHAN
Third Party Attestation Principal
bpradhan@bdo.com

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.