Need a privacy control and reporting framework?

HERE'S HOW TO CHOOSE ONE THAT'S RIGHT FOR YOUR ORGANIZATION.

As data privacy laws become increasingly stringent, it's more important than ever for technology companies to prove the efficacy of their privacy and data protection programs through data privacy control and reporting frameworks.

Most tech leaders are already familiar with key privacy laws such as the EU's General Data Protection Regulation (GDPR) and the California Privacy Rights Act (CPRA). Companies also have to consider relevant regional, national, and state privacy laws and regulations which continue to evolve and make data privacy compliance and reporting more complex and multifaceted.

Customers, prospects, and other stakeholders are increasingly scrutinizing companies' data privacy compliance programs. As a result, we are seeing an uptick in requirements to address data privacy compliance in a meaningful way, making it clear that pushing off data privacy compliance is no longer a feasible option. Proving you have a strong privacy and data protection program is critical to remaining competitive if you are an organization that has significant personal data processing responsibilities.

The Business Case for Data Privacy Frameworks

First and foremost, establishing a data privacy control and reporting framework is paramount for compliance. A strong framework can help technology companies methodically meet multiple complex legal and ergulatory requirements, build strong partnerships, and mitigate risks associated with non-compliance, including fines and fees and loss of customer trust.

Implementing a robust framework has many additional benefits beyond compliance, such as:

- Maturing the data privacy program controls to enhance business resilience (i.e., going beyond a 'contractual or policy perspective' as it relates to privacy)
- Building stakeholder confidence in the company's privacy capabilities and fostering trust with customers
- Reducing the burden of proof when asked about policies for vendor management for due diligence purposes
- Articulating the effectiveness of the company's data privacy program to customers, prospects and regulators
- Driving efficiency and rigor with external reporting

For many tech companies, the ultimate goal of implementing a data privacy control and reporting framework is performing a successful audit or achieving an industry certification, which can serve as proof points to show customers and vendors an effective program is in place. These audits can demonstrate a clear commitment to protecting customers' privacy and build trust with stakeholders.

See our related series of articles on how to evolve your privacy and data protection program using our three-part checklist.

READ NOW

SELECTING THE FOUNDATIONAL FRAMEWORK

Tech companies generally build their privacy control and reporting frameworks around one of two standards: ISO 27701 and/or SOC 2.

ISO 27701 Certification: ISO 27701 is an international certification, which many companies select because it lends credibility to a company's privacy framework. ISO 27701 is also well-suited to companies that are actively pursuing international growth, particularly in Europe and Asia, or that already have the ISO 27001 security certification.

Key elements of ISO 27701:

- Builds on top of the leading ISO security standard 27001 — be mindful that you need the ISO security certification before or in conjunction with getting the ISO privacy certification
- Maps to requirements from GDPR, which is the dominant legal framework globally and extremely applicable for companies serving EU-based customers
- Differentiates between data processer and data controller responsibilities
- Covers important areas like privacy by design, data risk management, consent, and data subject requests

SOC 2: SOC 2 attestation is a widely adopted reporting approach used by many global and U.S.-based tech companies. It is well-suited to companies that have already adopted SOC 2 reporting for security, those that have not already implemented ISO 27001, and those with a need to provide more privacy program detail in their audit reporting.

Key elements of SOC 2:

- Builds on a company's existing SOC 2 security reporting framework
- Based on a defined set of common privacy requirements
- Offers some more flexibility than ISO in defining the relevant privacy controls
- Results in a report that describes overall privacy processes, detailed controls, and the auditor's testing
- Allows the company to describe and highlight its privacy processes and controls
- Includes both descriptive and control components that help tech companies articulate their program controls to demonstrate their program's effectiveness

ADDITIONAL CONSIDERATIONS FOR CHOOSING AND TAILORING YOUR FRAMEWORK

Both ISO 27701 and SOC 2 act as a foundation to serve most technology companies' privacy reporting needs. Tech companies should be mindful that the current best practice is to adopt a framework and then add further controls designed to meet the unique needs of your organization.

If you are unsure which framework may work best for your company and/or how to tailor your controls and reporting, consider the following questions:

1. Where do you operate? What are the dominant data privacy standards in those regions?
2. What privacy laws apply to your company and the services you provide?
3. Where are your customers based and what are the dominant data privacy standards in those geographies?
4. What types of personal information/data are you collecting from customers?
5. What privacy and data related risks does your company face? How are you addressing these risks?
6. What are customers or stakeholders requesting — a specific type of report or certification?
7. Where are you trying to expand your customer base? Do those customers' industry or regional privacy requirements align with the privacy requirements and expectations of your current customer base?
8. What data privacy regulations do your customers have to adhere to? How does that impact the regulatory requirements and risks your company faces?

What's Next?

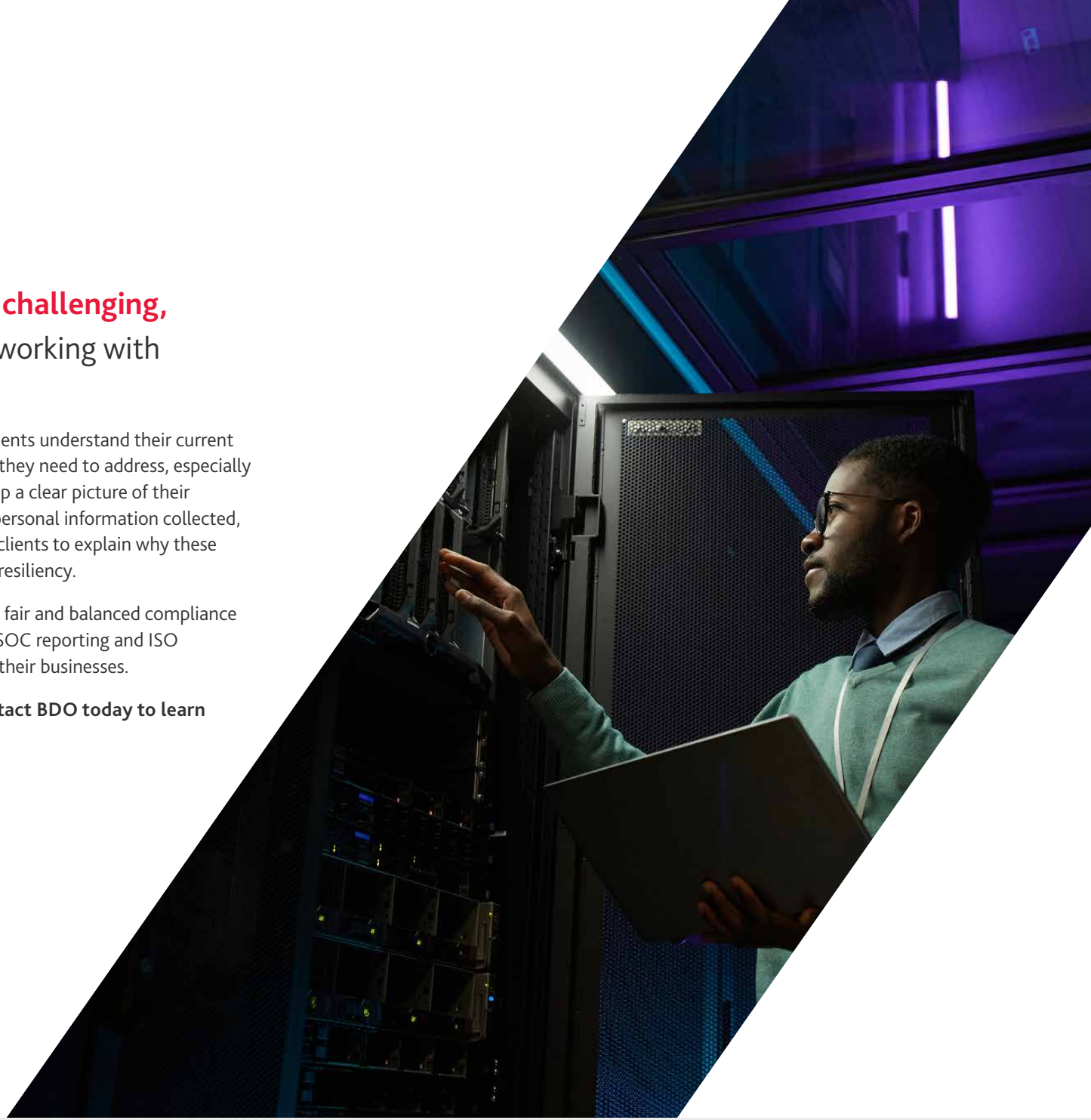
Adopting these standards can be challenging, and tech companies may find that working with a third-party advisor can help.

At BDO, we start with a readiness assessment to help clients understand their current level of privacy program maturity and identify any gaps they need to address, especially ahead of an audit. We work with organizations to develop a clear picture of their contractual and regulatory commitments, the types of personal information collected, and where it is processed and stored. We work with our clients to explain why these details matter to overall organizational compliance and resiliency.

Our **third-party attestation team** focuses on providing fair and balanced compliance assessments, as well as comprehensive services around SOC reporting and ISO certifications, all while helping clients protect and grow their businesses.

Ready to enhance your data privacy reporting? Contact BDO today to learn which reporting approach is right for you.

CONTACT US



CONTACT US

HANK GALLIGAN
National Technology Industry Leader
hgalligan@bdo.com

JASON LIPSCHULTZ
Assurance Principal
Third Party Attestation
jilipschultz@bdo.com

MARK LUNDIN
Assurance Principal
Third Party Attestation
mlundin@bdo.com

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

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: www.bdo.com

Material discussed in this publication is meant to provide general information and should not be acted on without professional advice tailored to your needs.