

White Paper



Why is Compliance Important for SaaS Providers?

Introduction

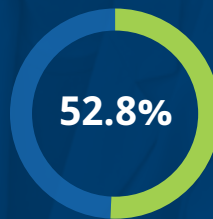
Communications Service Providers (CSPs) have faced compliance demands for as long as they have existed. Compliance touches every corner of the enterprise, including data security and privacy, industry-specific requirements and internal control mechanisms, among other factors. Assurance reporting plays an important role in compliance, providing company leaders with in-depth operational and control information, and assessment results that either verify compliance or highlight issues that need to be addressed.

Companies have relied on assurance reports as mechanisms for demonstrating internal control design and operational effectiveness to their board of directors, external and internal auditors, regulatory committees, customers and other relevant parties. Rather than perform audits of their vendors and partners themselves, CSPs have historically relied on assurance reports to provide insight into the control environments of third-parties, and fulfill broader risk management requirements.

Assurance demands have steadily increased over time as a result of CSPs' maturing risk management functions as well as the emergence and evolution of new compliance requirements. Software-as-a-Service (SaaS) providers need to account for numerous compliance frameworks,

depending on various factors such as their customers' specific industry and geographic locations they serve.

Companies continue to spend more on regulatory compliance solutions with each passing year.



According to Grand View Research, the global regulatory technology (RegTech) market will increase at a **52.8%** compound annual growth rate through 2025, when it will be worth **\$55.28 billion.**

Given these demands, the need for comprehensive assurance reporting is as pressing as ever, especially for SaaS providers catering to the CSPs. Since these companies host their customers' core business processes and data, they are a vital part of the broader compliance framework.

External assurance reporting not only confirms compliance to internal stakeholders, but demonstrates to customers that their service provider adheres to leading practices regarding security, compliance and controls. SaaS providers should view compliance strategies as both a way to mitigate risk and deliver more value to their customers.

Assurance reporting supports stronger SaaS partnerships

CSPs need to demonstrate to all of their stakeholders, including the board of directors and auditors, how their business processes adhere to internal control requirements. Due to the critical role that SaaS providers play in the CSP ecosystem as hosts of business processes and data, they must also be able to show their compliance with a variety of regulatory and control guidelines. Assurance reporting provides that essential documentation, proving that SaaS companies adhere to leading practices regarding security and compliance as well as have proper controls in place to manage, process and protect various types of

data. Without those assurance reports, CSPs will find it extremely difficult to partner with SaaS providers. In some cases, it will be impossible to get approval to work with a SaaS company if it cannot produce the necessary assurance reports.

Both CSPs and SaaS companies stand to benefit from assurance reporting. CSPs are not required to execute their own audits to determine SaaS provider compliance, avoiding loss of productivity. SaaS providers, meanwhile, can generate more revenue by working with CSPs that have strict assurance reporting requirements.

To meet those needs, SaaS companies should establish meticulous compliance programs and risk management functions. In addition, SaaS providers need to create governance structures that monitor and respond to the shifting regulatory landscape as well their customers' risk assurance needs and expectations. Because these requirements can change from year to year, SaaS companies must also continually refine their assurance reports to account for the latest best practices and

tailor their compliance strategies to their target customers' demands.

Above all else, SaaS companies should view assurance reports as an important way to earn trust with their CSP customers. CSPs need to have complete faith in their SaaS providers to securely host data and manage business processes, and independent assurance reporting delivers that verification.

The evolution of assurance reporting requirements

Assurance reporting within the United States has its roots in financial reporting requirements, such as the Statement on Auditing Standards No. 70 (SAS 70) that governed internal controls. These reports applied to companies outsourcing certain business functions to external organizations and required assurances that those third parties also had the required controls in place to issue audited financial statements.

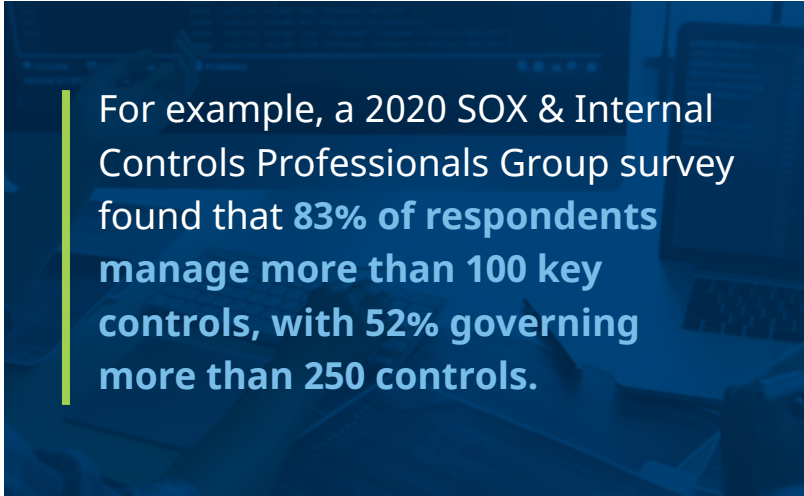
Reporting requirements are not confined exclusively to financial processes — they have since expanded to cover numerous internal controls that impact many other aspects of operations. The American Institute of Certified Public Accountants' (AICPA) Trust Framework is an especially relevant example for SaaS providers. Using the Trust Framework, the AICPA implemented System and Organization Control (SOC) 2 reporting. SOC 2 reports cover internal controls and policies related to data security, confidentiality, privacy and availability, as well as an organization's data processing practices.

Until recently, SOC reports have historically been viewed as a competitive advantage, but they have become an essential requirement for SaaS providers. Today, many third-party service providers will not be allowed to participate in a request for proposal (RFP) if they are unable to provide the necessary assurance reports.

Reporting needs have continued to expand, encompassing industry-specific frameworks, government regulations and regional requirements, among other concerns. For instance, companies that

are members of or sell to the healthcare industry must comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

In a rapidly shifting regulatory landscape, third parties need to continuously refine and improve their control environments. With the advent of new technology like cloud computing and the Internet of Things, SaaS companies face more difficult challenges and complex reporting requirements regarding the confidentiality, integrity and availability of business data.



For example, a 2020 SOX & Internal Controls Professionals Group survey found that **83% of respondents manage more than 100 key controls, with 52% governing more than 250 controls.**

In response to these developments, assurance reporting needs to augment and support necessary controls to meet CSP needs and establish trust.



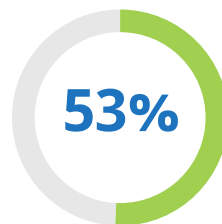
Rising threats drive security oversight

The steady rise of cyber threats and data breaches has added another wrinkle to compliance demands, making data security among the most important reporting requirements for SaaS providers to address.

IBM's latest analysis noted that the average cost per record is \$175 when the affected records contain customer information.

Businesses need to assess their risk levels across both internal and external channels. In particular, companies have become increasingly aware of the risk presented by third-party vendors that do not invest in security or measure themselves against recognized security standards.

According to the Identity Theft Resource Center, the number of reported data breaches **increased 17% in 2019, totaling nearly 1,500 separate incidents.**



According to a 2019 Ponemon Institute survey, 53% of respondents reported a data breach stemming from a third-party relationship.

Such events can be incredibly expensive once the dust settles and organizations tally up total costs relating to remediation, compliance and reputational damage.

On average, those security incidents cost \$7.5 million to fully remediate.

IDI Billing Solutions' diligent approach to assurance reporting

As assurance reporting requirements grow more complex, service providers need to adapt with their customers' changing needs. IDI Billing Solutions' reporting practices have evolved through the years to align with new market developments, regulatory frameworks and business environments. IDI teams continue to prioritize assurance reporting to build trust with customers.

In 2018, **IDI partnered with Freed Maxick, a Top 100 Accounting Firm with a dedicated risk advisory and assurance practice that focuses on third-party service providers**, to align controls with recognized standards and frameworks and build a strong security and compliance program.

"Over time, IDI has foreseen a lot of these assurance requirements, and evolved along with those changes," said David Hansen, Freed Maxick's Director of Risk Advisory Services. "They've worked with us to elevate their risk management and compliance program, as well as their reports, to a stage of continuous improvement. IDI works to forecast what customer needs might be to ensure that the trust they've earned continues over the course of their relationship."

IDI reporting practices cover many regulatory requirements, industry-specific guidelines and other compliance factors. As part of IDI's SaaS offering, IDI currently provides assurance on its internal controls through the issuance of its SOC 1 focusing on financial reporting risks and SOC 2 covering security, availability and confidentiality. Additional assurance is provided through its Report on Compliance with the Payment Card Industry (PCI) Data Security Standards (DSS), and a report on its compliance with HIPAA.

In addition, IDI continues to review and assess its controls against other recognized frameworks, such as HITRUST. In this way, IDI can proactively address the changing needs of the business environment where the company operates.

Throughout the years, IDI has made regulatory compliance and assurance reporting a major priority. **Company leaders have significantly invested in people, processes and technology to ensure a robust assurance reporting roadmap that is aligned with the specific needs of their customers.**

“Our commitment to security and compliance comes from our company culture. Everyone is working together. We have trust and security all the way from product development to our operations.”

-Patrick Talty, IDI Billing Solutions President and Chief Security Officer



IDI delivers peace of mind

CSPs need third-party service providers and business partners they can trust, especially regarding data governance and hosting. IDI has steadily established a sterling reputation in the telecom industry and become a market leader by building that trust and forging lasting relationships with their customers.

IDI's approach to service delivery focuses on people, process and technology, and that mindset continually instills confidence in their capabilities and unwavering commitment to customers. Due to the high stakes involved, CSPs should only work with SaaS providers that prioritize security and risk mitigation as part of their overall operations strategy.

Sources:

https://www.grandviewresearch.com/press-release/global-regulatory-technology-market?utm_source=Medium&utm_medium=referral&utm_campaign=Abhijit_July4_ict_Pr&utm_content=Content

<https://www.workiva.com/sites/workiva/files/pdfs/thought-leadership/sox-state-of-market-report-2020.pdf>

<https://www.marketwatch.com/story/data-breaches-soared-by-17-in-2019-but-theres-some-good-news-too-2020-01-29>

<https://www.ibm.com/easytools/runtime/hspx/prod/public/X0029/PortalX/filedocid/c0bc9b5abedf4f6b8a1e3409081e89b9/Infographiccostofadatabreachreport2020.pdf>

<https://cdn2.hubspot.net/hubfs/2378677/Content-Assets/CyberGRX%20Ponemon%20Report.pdf>

If you are interested in learning more about IDI's security and compliance function, please contact **IDI Billing Solutions** or visit www.idibilling.com.



7615 Omnitech Place, Victor, NY 14564
Tel: 888 924 4110

