Volume 5 | Issue 2

HOLBORN™
Our Independence. Your Advantage.

ViewPoint

Analyzing Industry Issues from an Independent Perspective

Data Privacy Standardization

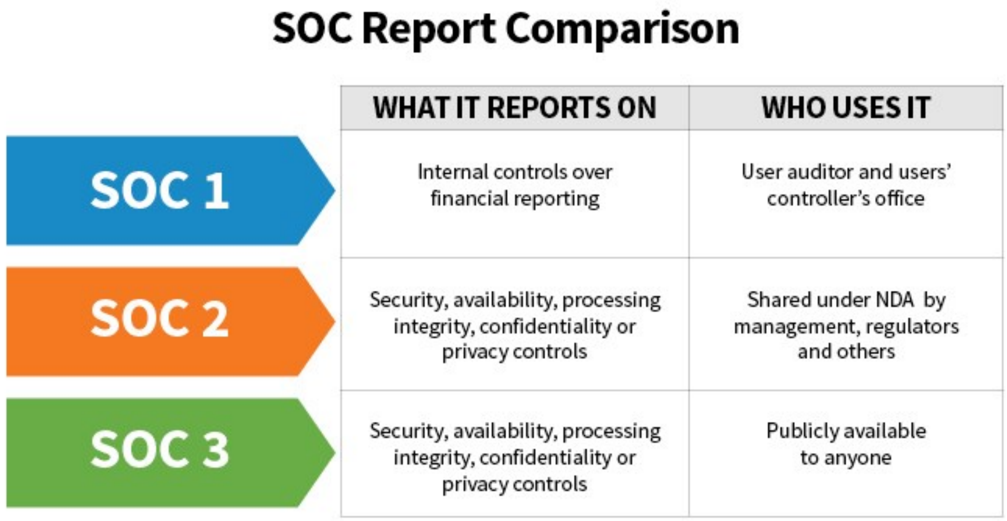
Implications in a Changing World

In today's interconnected world, the need for risk management of third party vendors is increasingly important. In response, the American Institute of Certified Public Accountants (AICPA) instituted System and Organization Controls (SOC). SOC refers to a report outlining standards with which technology companies must follow; it evolved from the original version called SAS 70 (Statement on Auditing Standards No. 70). It is important to note that SOC is not a statute or regulation, rather a reporting standard.

SOC applies to a category of organizations known as SaaS ("Software as a Service") companies. An SaaS company is categorized as one that maintains servers, databases and software accessed over the internet (i.e., web browsers, or cloud software). Examples of which are payroll processors, medical claims processors, loan servicing companies, and data center companies.

> *"...SOC is not a statute or regulation, rather...[a] reporting standard..."*

There are three levels of SOC reports—SOC 1, SOC 2, and SOC 3. While each vary in detail, all affirm to



SOC Report Comparison

	WHAT IT REPORTS ON	WHO USES IT
SOC 1	Internal controls over financial reporting	User auditor and users' controller's office
SOC 2	Security, availability, processing integrity, confidentiality or privacy controls	Shared under NDA by management, regulators and others
SOC 3	Security, availability, processing integrity, confidentiality or privacy controls	Publicly available to anyone

SaaS clients that the software in use maintains the proper security and privacy controls.

SOC 1

SOC 1 targets organizations that store financial data. It requires written evidence of the company's internal controls of financial reporting and the monitoring of security activities, for auditors. Examples of companies that need to comply with SOC 1 are SaaS organizations, medical or payroll processing, cloud computing, and lending services.

There are two types of reports for SOC 1:

Type 1—Focuses on whether the control design and implementation is adequate, as of specified dates.

Type 2—Addresses the control effectiveness over a specified period of time. It includes a description of the tests performed and the company's response to the results.

The reports are intended for internal Board and management reports, Compliance Officers, and external auditors. A complete report will include an independent auditor's opinion of the effectiveness of controls in place and adequate description of such controls.

SOC 2

SOC 2 broadens the scope of the report by including protections unrelated to financial reporting. It is more technical and security-focused than a SOC 1 report. SOC 2 reports include a description of the infrastructure, software, people, procedures (i.e. a "system"). There is also a privacy and confidentiality component.

The following five areas should be addressed, as they relate to controls:

1. **Security**—Confirmation that the system in place is protected against unauthorized access. This includes monitoring system activity and alerting procedures.
2. **Availability**—The system is available for use as agreed.
3. **Processing Integrity**—System is complete, accurate, valid, timely, and authorized.
4. **Confidentiality**—Information designated confidential is protected.
5. **Privacy**—Personal information is stored, used, and disposed in accordance to best practices.

Due to more reliance on outsourcing data processing and other corporate functions, there is an increased request for SOC 2 reports. Those companies that handle both financial and non-financial data will complete both SOC 1 and SOC 2 reports.

SOC 2 reports are typically of interest to vendors, prospective clients, and regulators, among others. Like SOC 1, there are two types of reports:

Type 1—Specific evaluation of controls at a point in time; and to include a description of the system, auditor's opinion of the description and design of programs in place.

Type 2—Again covers a range of time and follows that of Type 1, with the added requirement of the detailed tests, their results, and the company's response.

SOC 3

SOC 3 is a certification primarily for general public use. It is mainly comprised of a system description and an auditor's opinion in a less detailed and technical manner. In order to have a SOC 3 examination, first a SOC 2, Type 2 report must be complete.

SOC and Europe's GDPR

Other statutes reflect the principles of SOC, including the European Union's (EU) GDPR (General Data Protection Regulation), which was enforced on May 25, 2018 following a two-year transition period. Like SOC, it is intended to protect customers' privacy in the following ways:

- Standardize data privacy laws across Europe,
- Protect EU citizens data privacy
- Ensure organizations' strict adherence to data privacy.

The regulation applies to all companies' processing personally identifiable data of residents of the EU, whether the processing of data occurs in the EU, or not. Moreover, it applies to organizations outside the EU that provide goods or services to EU residents.

European residents have the following rights under GDPR:

- Knowledge of who is processing the data, and why
- Access to the data a company has on you, in a readable format
- Objection of use, if for marketing or other unsolicited use
- Correction of data, if you believe it might be inaccurate
- Timely deletion of data, if there are no legal grounds for maintaining the information
- Automated (algorithm-based) marketing rules reviewed by a person
- Transfer of data among vendors

Unlike SOC, GDPR is law in the EU and therefore operates on a pass / fail system. Companies failing to adhere to the Guidelines can be penalized up to the greater amount of €20Mn or 4% of annual global turnover. All consent forms must be clear and concise, with the ability to consent or opt out. Should a client wish to be removed from a company's database, it must be immediately done.

> *"...GDPR is thought to become the global standard in the future. ..."*

Companies must also appoint a Data Protection Office (DPO) if processing data is a core business activity, or on a large scale. Following a breach, the organization has 72 hours to advise regulators without penalty.

Transferring personal data outside the European Economic Area, to include the EU, Iceland, Liechtenstein, and Norway is permitted if the following criteria are met:

- Receiving country's protections are considered adequate by the EU,
- The company takes steps to ensure privacy of data, or
- Agreement to the sharing of personal data.

California and New York: Setting Standards

SOC is a reporting standard and not yet law. GDPR is setting the global standard for data privacy.

California

For its part, California is ironing out the details of the California Consumer Privacy Act (CCPA) of 2018. The CCPA follows much of the same principles in the GDPR and is expected to take effect on January 1, 2020.

The CCPA applies to for-profit businesses that collect and process personal information of California residents and do business in California. The Act applies to businesses that meet one or more of the following:

- Gross revenue in excess of $25Mn
- Receive or share personal data of more than 50,000 individuals
- Derive 50%+ annual revenue from selling personal information of California residents

Noncompliance may result in fines, including $2,500 for each violation and $7,500 for each intentional violation.

New York

On March 1, 2017, New York's Department of Financial Services issued 23 NYCRR 500, or NY Cyber Regulation, with a two-year implementation period. The regulation requires financial services companies meeting certain criteria to adhere to security guidelines, including:

- Written cybersecurity policy that has been approved by the Board of Directors or Senior Officer;
- Access privileges;
- Cybersecurity risk assessments;
- Training and monitoring for authorized users;
- Governance process for senior leadership; and
- Appointment of a Chief Information Security Officer.

The purpose is to continually improve the maintenance and protection of personal data, while also mitigating cybersecurity attacks. Specifically, Superintendent Vullo highlights in her letter the importance of the following procedures to avoid cyber attacks:

1. Multi-factor Authentication
2. Encryption
3. Training, with regard to vigilance and protection

All eligible companies must yearly perform an assessment in order to receive a certification of compliance from the DFS. All annual filings are due on February 15th of the following year.

Conclusion

With the importance of data security increasing daily, understanding and addressing the use of private data is of utmost importance. It is likely these regulations will become the nationwide standard for U.S. companies. Understanding the regulations and preparing for future implementation may ultimately save time and expense .

As a New York based organization, Holborn remains in strict compliance with NY Cyber Regulation. We will continuously monitor the developments in this rapidly evolving area. As always, the Holborn team is available as a resource and to provide guidance to our clients.

Holborn Corporation is an independent reinsurance brokerage firm, which was founded in 1920 and is headquartered in New York. Through the adoption of an Employee Stock Ownership Plan (ESOP) in 1998, it became exclusively owned by its employees. For additional information, please visit our website at **www.holborn.com**.

HOLBORN™
Our Independence. Your Advantage.