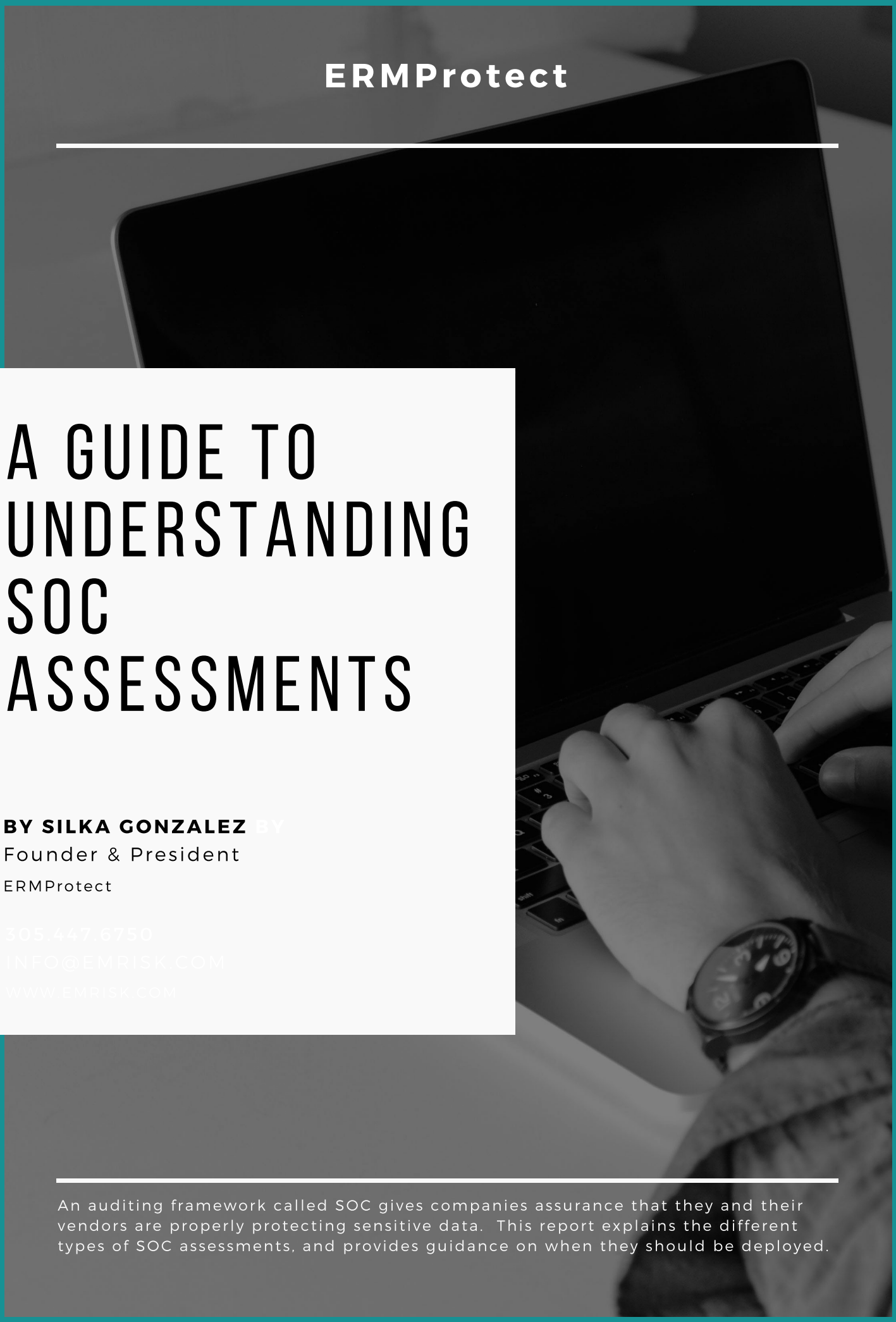
ERMProtect



A GUIDE TO UNDERSTANDING SOC ASSESSMENTS

BY SILKA GONZALEZ BY
Founder & President
ERMProtect

305.447.6750
INFO@EMRISK.COM
WWW.EMRISK.COM

An auditing framework called SOC gives companies assurance that they and their vendors are properly protecting sensitive data. This report explains the different types of SOC assessments, and provides guidance on when they should be deployed.

ARE YOUR SERVICE PROVIDERS LEAKING OUT YOUR CONFIDENTIAL DATA?

HERE'S HOW TO FIND OUT

Third party service providers (TSPs) continue to be an integral part of an organization's strategy since they facilitate a focus on an organization's core areas of strength while reducing expenses and increasing efficiency and growth. With all of this to offer, outsourcing to TSPs sounds like a no-brainer. But there are still risks. TPSs, after all, are an extension of an organization. While you can delegate tasks and even authority to TSPs, you can't really delegate responsibility and accountability for security and controls. That's where a SOC comes into play.

What is SOC?

Organizations face pressures from regulators and other stakeholders to demonstrate the operational effectiveness of controls that protect the processing of transactions and safeguard sensitive data. As a result, the American Institute of Certified Public Accountants (AICPA) created a framework better known as the "System and Organization Controls" (SOC) framework to enable CPAs to review and comment on the adequacy of a TSP's controls pertaining to sensitive data. A SOC examination is performed by a CPA who reviews the design and operating effectiveness of controls employed at an organization over a period of time.

Types of SOC

A SOC report has different reporting options – SOC 1, SOC 2, SOC 3, and SOC for Cybersecurity.

• **SOC 1** examinations focus solely on systems and controls that may be relevant to your TSP's internal control over financial reporting. In simpler terms, if your TSP's main focus is the processing or handling of financial information, then a SOC 1 may be appropriate.

• **SOC 2** examinations focus on controls at a TSP that are aligned with one or more trust service principles that include data security,

data availability, data processing integrity, data confidentiality, and data privacy. Put simply, if your TSP's main focus is on the protection of sensitive data, then a SOC 2 might be appropriate.

• **SOC 3** reports are based on the same concept and trust service principles as a SOC 2, but do not include an opinion, detailed description, or results of testing controls as in a SOC 2 examination. As a result, a SOC 3 report is not restricted and can be posted on an organization's website and shared with any party. It's important to note that the same is not true with SOC 2 reports, which are restricted use because they may expose critical cybersecurity measures.

• **SOC for Cybersecurity** reports are designed to examine an organization's entity-wide Cybersecurity Risk Management Program. A SOC for Cybersecurity can serve as a very efficient way for an organization to demonstrate the effectiveness of its cybersecurity controls over all aspects of its operations.

Who needs a SOC?

So, does your organization need a SOC examination and do you know which one applies to you?

If you are collecting, processing, transmitting, or storing sensitive data, then the answer will likely be that you need a SOC 2. No matter what your business type or size, a SOC report can be a very powerful tool in establishing trust with current and prospective customers. Organizations want to know that their TSPs take cybersecurity as seriously as they do.

Up Next

This is the first article in our six-part SOC series to guide organizations and help them understand the SOC framework better. In our next article, we'll dig deeper into each SOC examination type.

SOC: UNDERSTANDING A TOOL THAT ASSURES BEST PRACTICES IN CYBERSECURITY

SOC examinations have become a necessity. They assure organizations that they can trust third party service providers (TSPs) with sensitive data, so that the contracting organization can fulfill its monitoring and oversight responsibilities. The main purpose of a SOC examination is to provide independent assurance on the design and operating effectiveness of controls at a TSP. But there are several types of SOCs, and they differ in scope. Organizations need to understand what these are so that they can appropriately choose which one best fits their customer and regulatory requirements.

Here's an in-depth look:

SOC 1

A SOC 1 examination evaluates the design and operating effectiveness of controls at a TSP relevant to financial reporting. A SOC 1 examination is generally required when a TSP is processing financial information such as employee payroll, claims, or other data that rolls up into financial statements.

The scope of a SOC 1 examination is determined by the people, processes, and systems used to provide an organization's products/services. Because SOC 1 reports can include sensitive information, distribution is restricted to current customers, their auditors, and other regulatory agencies.

There are two types of SOC 1 reports – Type 1 and Type 2.

• A **Type I** examination and report provides an opinion on the fairness and suitability of the description of the system as of a particular date. A Type 1 examination only focuses on whether internal controls are suitably designed and does not determine whether they are operating effectively.

• A **Type II** examination and report provides an opinion on both the fairness and suitability of the description and operating effectiveness of controls for a period of time, which is usually between six to twelve months. A successful SOC 1, Type II, examination demonstrates that there are adequate internal controls at the

TSP surrounding the financial reporting process and that they are operating as intended.

SOC 2

A SOC 2 examination is probably the more important examination in today's environment due to the increased number of security breaches and concern over the security, availability, processing integrity, confidentiality, and privacy of data. A SOC 2 examination provides deeper assurance of a TSP's controls over the infrastructure, software, people, procedures, and data used in providing products and services. In simple terms, a SOC 2 examination and report focuses on at least one or more of following five trust service principles:

• **Security:** The system is protected against both physical and logical unauthorized access.

• **Availability:** The system is available for operation and use, as committed or agreed.

• **Processing Integrity:** System processing is complete, accurate, timely, and authorized.

• **Confidentiality:** Information designated as confidential is protected as committed or agreed.

• **Privacy:** Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and criteria set forth in Generally Accepted Privacy Principles issued jointly by the AICPA and the Canadian Institute of Chartered Accountants (CICA).

There are two types of SOC 2 reports – Type 1 and Type 2.

• A **Type 1** examination and report provides an opinion on the fairness and suitability of the description of the system as of a particular date. A Type 1 examination only focuses on whether trust service principles criteria and controls are suitably designed and does not determine whether they are operating effectively.

• A **Type 2** examination and report provides an opinion on both the fairness and suitability of the description of the system and the operating effectiveness of controls for a period of time, which is usually between six to twelve months. Like a SOC 1, SOC 2 reports are restricted-use reports since they contain sensitive information. The unauthorized access or distribution of a SOC 2 report poses a security risk to the TSP since information in the report's description can be used to discover

potential security vulnerabilities.

SOC 3

SOC 3 reports are similar to SOC 2, Type 1, reports in that they provide an abbreviated version of the description of the system. No opinion or information on the testing of controls is provided. But unlike SOC 2 reports, a SOC 3 is classified as a general use report and can be posted on an organization's web page and shared with the public. A SOC 3 report expands an organization's marketing initiatives and demonstrates its commitment toward providing outstanding services through adherence to one of more of the five trust services principles.

Moving Forward

It is critical for TSPs to choose wisely from the various SOC options available. To gain customer trust, a TSP must demonstrate its commitment to a secure and robust system of internal controls.

Next Time

The next article in our SOC series, will explain what TSPs need to consider before beginning a SOC 2 examination.

SOC 2: AN INDEPENDENT CYBERSECURITY EXAM THAT HELPS KEEP THE HACKERS AWAY

The continued growth of technology-oriented third-party service providers (TSPs) has caused the SOC 2 to become a widely sought-after attestation. A SOC 2 evaluates the cybersecurity posture of any TSP that collects, processes, transmits, or stores sensitive data whether it be in a local data center, the cloud, or with another vendor (subservice organization).

In a SOC 2 examination, an independent CPA firm (service auditor) performs an on-site assessment and test procedures on a system that is defined as the infrastructure, software, people, procedures and data used to provide services or products. The CPA formally attests to whether the system adheres to trust service principles pertaining to sensitive data including security of data, availability of data, processing integrity of data, confidentially of data and privacy of data.

A SOC 2 examination demands granular visibility into the governance of the system and the roles and responsibilities of the customer organization, TSP, and any subservice organizations used. In simple terms, the SOC 2 service auditor examines how the TSP meets trust service principles and requirements and commitments made to customers in providing their products and services.

SOC 2: What TSPs Need to Know

A SOC 2 brings with it some responsibilities and potential associated liabilities that TSPs need to keep in mind. Let's take a look at these:

• **Scope Definition:** Defining the scope for a SOC 2 examination is crucial. A narrow scope might not give the assurance customers want. Too broad of a scope might cause unnecessary work affecting budget and other priority initiatives. The key lies in defining the system and selecting the trust service principles that are necessary to meet service requirements and commitments. For example, if a TSP provides data storage services, but performs no information processing, security and availability trust service principles may apply. Further, if the data stored is protected health

information (PHI) or personally identifiable information (PII), then the privacy trust service principle may also apply.

• **Documentation:** A TSP should have comprehensive policies and procedures in place that incorporate what the service auditor is essentially going to be looking for – how system trust services principles and criteria are met. It is important to remember that not all of the five trust principles may be in scope and that policies and procedures will need to only focus on the in-scope areas.

• **Written Assertion:** A SOC 2 examination requires that the TSP provide both a written management assertion on the description of the system and management representation of certain responsibilities. Hence, it is imperative that a TSP have a complete understanding of the description of the system. Their assertions and representations are to be taken seriously as they define responsibility and potential subsequent liability.

• **Service Auditor Selection:** A SOC 2 examination needs to be performed by a CPA firm whose professionals have auditing experience and deep knowledge of information-security. A CPA without information security expertise would not be able to provide the service properly. SOC 2 examinations are conducted in accordance with American Institute of Certified Public Accountants (AICPA) Attestation Standards.

• **Do Not Share:** The distribution of a SOC 2 report is intended solely for the information and use of TSP management, user entities of the system during some or all of the service period, and practitioners and regulators providing services to user entities. Because of the sensitive information discussed in the description, SOC 2 reports should not be shared openly. Ensuring that a SOC 2 report doesn't fall into the wrong hands is a TSP responsibility.

Continuous Commitment

Getting a SOC 2 examination is not a one-time event. Subsequent examinations after the first year are typically performed on an annual basis. SOC 2 compliance demands a control-focused culture practicing continuous improvement.

Next Time

Our next article will look at the responsibilities of the SOC 2 service auditor.

HOW TO HIRE THE RIGHT SOC CYBERSECURITY AUDITOR

The last article in our SOC series touched on the responsibilities of third party service providers (TSPs) undergoing a SOC 2 examination. Once a TSP is done with its due diligence, a service auditor with the appropriate mix of practical experience and subject matter expertise is selected. In fulfilling its responsibilities, a TSP must also understand the responsibilities and potential liabilities of the SOC 2 service auditor.

SOC 2: Responsibilities of the Service Auditor

SOC 2 examinations are unique to each TSP. The success or failure of a TSP's controls can have both a direct or indirect impact on the TSP's reputation. Hence, selecting the right service auditor and getting him or her involved early in the SOC 2 planning process is critical to achieving a favorable SOC 2 report. TSPs also need to be mindful of the responsibilities and potential liabilities of service auditors and ensure auditors acknowledge their share of responsibilities. Here are a few things that the service auditor performing a SOC 2 examination should follow and assist the TSP with:

• **Scoping:** The service auditor can guide the TSP in defining the system and description that is used to provide products/services as well as the trust service principles that should be in scope. However, when providing assistance to the TSP, the service auditor cannot make decisions on the TSP's behalf; otherwise the service auditor's independence and objectivity will be compromised.

• **Service Auditor Standards:** The service auditor performing the SOC 2 examination is required to maintain a high level of professional ethics, follow quality control standards, and comply with applicable legal and regulatory requirements. The service auditor must be a Certified Public Accountant and perform the examination in accordance with American Institute of Certified Public Accountants (AICPA) Attestation Standards. The service auditor must also display the highest levels of ethics, objectivity, and independence at all times.

The SOC 2 examination is simply a service auditor's opinion on how the TSP meets it service requirements and commitments made in its assertion.

• **Examination Process:** The service auditor should provide the TSP with a list of requirements at least one month in advance that includes the evidence necessary to evaluate the fairness and suitability of the design of controls and their operating effectiveness. The service auditor should also provide the TSP with examples of written assertions prior to the actual examination. During the examination, the service auditor will visit the TSP to perform on-site interviews and evaluations, and document results. The service auditor should also perform a thorough analysis of the policies and procedures in place.

• **Do Not Share:** Because a SOC 2 report contains sensitive information, the TSP should be very cautious to restrict distribution. TSPs should require a service auditor to sign a non-disclosure agreement (NDA) before a SOC 2 report is released.

Moving Forward

A SOC 2 examination involves responsibilities and potential liabilities for both the TSP and the service auditor. It's imperative that both entities consider and respect these responsibilities. A TSP should leverage the practical experience of the service auditor in an advisory capacity only, so the service auditor's independence and objectivity will not be impaired.

Next Time

In the next article in our SOC series, we'll talk about how you can achieve a SOC 2 examination with favorable results.

THE PATH TO ASSURING A SUCCESSFUL SOC 2 EXAM

A favorable SOC 2 report is significant to third party service organizations (TSPs). In simple terms, it gives the TSP the ability to instill confidence in customers that purchase their products and services. A SOC 2 report can demonstrate the use of best practices in collecting, processing, transmitting, or storing sensitive information.

The path to a successful SOC 2 examination is not always easy. Depending on the maturity of the TSP, preparing for the examination can be more time consuming and expensive than the actual examination itself.

A SOC 2 examination provides deeper assurance of a TSP's controls over the infrastructure, software, people, procedures, and data used in providing products and services in accordance with one or more trust service principles: security, availability, processing integrity, confidentiality and privacy of data. Prior to the commencement of the actual SOC 2 examination, it's imperative that TSPs take steps to ensure that they are well-prepared. Sufficient preparation can be complicated, time consuming, and draining. However, if an organization has a control-focused culture that emphasizes continuous improvement, then the actual SOC 2 examination can be painless, and even simple.

SOC 2 Readiness

Here is what you need to know and incorporate when readying yourself for a SOC 2 examination:

• **Readiness Assessment:** A readiness assessment gives a TSP a chance to warm up before an actual examination takes place and allows for the remediation of shortcomings that are identified during the assessment. A readiness assessment can be performed internally or by a service auditor. An assessment performed by a service auditor would obviously be more objective, independent, and honest about the design and operating effectiveness of controls.

• **Risk Assessment:** A risk assessment identifies critical gaps in the information security architecture that prevent the achievement of

information security goals and objectives. Conducting a thorough risk assessment on a periodic basis identifies and evaluates ever-changing risks and provides an opportunity to remediate identified gaps. The main focus of a risk assessment is to examine the greatest threats to the infrastructure, software, people, procedures, and data used by the system to provide products and services. The performance of a periodic risk assessment allows a TSP to effectively manage and mitigate risk.

• **Documentation:** Comprehensive policies and procedures are critical for a successful SOC 2 examination. To pass a SOC examination, they must also be monitored, enforced, and periodically updated. Remember that the service auditor will not just stop at a cursory review of the documentation in place. The service auditor's larger goal is to observe how much of what is documented is actually practiced. Once policies and procedures are developed and implemented, they must be periodically reviewed to ensure that they are current.

• **The 3 P's:** Unpredictable and unforeseen events, ranging from data breaches to natural disasters affect all TSPs. These events can halt day-to-day operations and a quick recovery is needed to ensure uninterrupted delivery of products and services. An Incident Response Plan (IRP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) all play a major role in providing transparency. To be effective, these plans must be in place and tested and updated on a periodic basis.

• **Security Awareness Training:** Even with the most robust technology and highly skilled professionals in place, the weakest link when it comes to controls and security are employees. Ongoing and engaging cybersecurity awareness training will make employees aware of ever-evolving cyber threats that target human vulnerabilities. The key word here is "engaging." To be effective, security awareness training cannot be boring and should be provided to everyone on a regular basis. By adopting a comprehensive security awareness training program, TSPs can greatly improve their overall controls and security posture by creating human firewalls that help guard the TSP's information.

• **Vendor Management:** The continued growth in outsourcing is the main catalyst for mandatory governance and oversight of TSPs through the formalization of vendor management risk practices.

Many data breaches in recent years have materialized due to vulnerabilities that were poorly managed by TSPs. The use of vendors (subservice organizations) to augment the products and services provided by a TSP requires oversight and monitoring. In this scenario, the TSP evaluates the security and controls of subservice organizations using methods similar to how customers evaluate TSPs. Periodic risk assessments of subservice organizations should be performed and integrated into the TSP's enterprise-wide risk management process. Adopting a proactive approach to managing risks associated with subservice organizations is required for a SOC 2 examination and will be assessed by the service auditor.

Moving Forward

Once a successful SOC 2 examination has been performed and a report issued, don't stop there. SOC examinations are performed on a periodic basis. TSPs should proactively address the quality of their SOC 2 report by soliciting feedback from their customers and their auditors.

Next Time

SOC for Cybersecurity has been generating a considerable amount of interest and expectation. In the next article in our SOC series, we'll take a look at a SOC for Cybersecurity.

SOC FOR CYBERSECURITY PUTS YOUR ENTIRE ENTERPRISE TO THE TEST

Cyberattacks today have risen to record levels and trends point toward a continued upward trajectory. These incidents cause significant damage to business growth, mission objectives, and bottom lines. And hackers continue to innovate, unleashing attacks that organizations aren't prepared to defend. This means organizations need to reinforce themselves with robust and efficient Cybersecurity Risk Management Programs.

An effective Cybersecurity Risk Management Program enables organizations to detect security events in a timely manner and respond to and recover from them with minimal operational disruption. For a business to be successful today, organizations must demonstrate to customers and other stakeholders that they are able to manage cybersecurity threats. And this is where SOC for Cybersecurity enters the picture.

What is SOC for Cybersecurity?

SOC for Cybersecurity is designed to evaluate an entity-wide Cybersecurity Risk Management Program for organizations. A SOC for Cybersecurity examination can be performed for any organization, not just third- party service providers (TSPs). CPAs who are experts in cybersecurity evaluate the businesses' description of its cybersecurity risk program and the effectiveness of controls used to achieve its security objectives. The evaluation must be performed by a firm staffed by CPAs with extensive knowledge in all areas of cybersecurity.

A SOC for Cybersecurity has three key components:

• **Management's Description:** In the first component, organization management provides a description of its Cybersecurity Risk Management Program. The description should address the identification of information assets, how cybersecurity risks that threaten these assets are managed, and the key security policies and procedures in place to protect information assets against risks.

• **Management's Assertion:** In the second component, organization management provides an assertion of whether the described Cybersecurity

Risk Management Program is in accordance with SOC for Cybersecurity criteria and whether the controls of the Program operate effectively in meeting cybersecurity objectives.

• **Practitioner's Report:** In the third component, an independent auditor's report includes an opinion of whether the description of the Cybersecurity Risk Management Program was designed in accordable with SOC for Cybersecurity criteria and whether controls in the Program are operating effectively. The SOC for Cybersecurity report can be distributed to regulators, stakeholders, and current and prospective customers to demonstrate a commitment to cybersecurity.

Types of SOC for Cybersecurity Reports

There are two kinds of SOC for Cybersecurity reports:

• **Type I report:** The CPA firm independently examines the description of the organization's controls on a particular date to ensure they are designed in accordance with SOC for Cybersecurity criteria.

• **Type II report:** The CPA firm includes the components of a Type I report and comments on the operating effectiveness of controls over a period of time, usually six to twelve months.

How is a SOC for Cybersecurity different from a SOC 2?

A SOC 2 examination is designed to evaluate the security control measures of a TSP's systems and services as it relates to the data services provided to their customers and clients. A SOC for cybersecurity is designed to address an entity-wide Cybersecurity Risk Management Program.

Here are some of the differences:

• A SOC 2 examination uses the trust service principles and criteria as a baseline to measure compliance. A SOC for Cybersecurity uses the American Institute for Public Accounting (AICPA) Cybersecurity Management Program criteria as a baseline to measure compliance. However, other reputable information security frameworks by the National Institute of Standards and Technology (NIST) or the International Standards Organization (ISO) can be used as baselines to measure compliance. These include NIST's 800-53 or ISO's 27001 / 28002 frameworks.

• In a SOC 2 examination, TSPs can choose to exclude from their examination the supporting services provided by other vendors, if the subservice organization is not providing a core service. In a SOC for Cybersecurity examination, all organizations providing services for any aspect of the Cybersecurity Risk Management Program must be included in scope.

• A SOC 2 report is a restricted use report intended for internal use by management. In contrast, a SOC for Cybersecurity report can be shared with all stakeholders including current and prospective customers. This is because detailed testing is eliminated from the report that could be used to discover vulnerabilities in planning a cyberattack.

Practitioner Expertise

SOC for Cybersecurity is a unique examination that requires a combination of expertise in controls and cybersecurity. CPA firms with deep knowledge in cybersecurity must be utilized for this type of service. CPA firms that do not have experienced cybersecurity practitioners will not be able to provide this service properly.

Bottom Line

Cybersecurity issues – both technical and compliance related – will only increase in the future. Organizations can establish credibility in the market and with regulators if they can prove their ability to manage evolving cyber threats. A SOC for Cybersecurity examination could be an investment worth considering.

Wrapping Up

This was the last article in our SOC series. We hope you found the articles useful and informative.

If you have any questions, feel free to write to us at info@ermprotect.com or call us at 305-447-6750.