ACCEDERE

SOC Reporting for Cyber Risk

06.01.2017

SOC Reporting for Cyber Risk

Let's begin with introduction of the terms used in SSAE 18 & SOC attest engagements.

Some specific terms used in the document

- **User Organization** The entity that has engaged a service organization and whose financial statements are being audited.
- **User Auditor** The auditor who reports on the financial statements of the user organization
- **Service Organization** The entity (or segment of an entity) that provides services to a user organization that are part of the user organization's information system.
- **Service Auditor** The auditor who reports on controls of a service organization that may be relevant to a user organization's internal control as it relates to an audit of financial statements.

About SSAE 18 and SOC Attestation

Effective May 2017, the new service organization reporting standard is Statement on Standards for Attestation Engagements (SSAE) No. 18. supersedes the SSAE 16, and other SSAE, AT Standards. The earlier standard was Statement on Auditing Standards **SAS 70** concerning the professional guidance on performing the service auditor's examination for Service Organizations. This was In line with the global standard called the International Standard on Assurance Engagements (ISAE) 3402 issued by the International Auditing and Assurance Standards Board (IAASB).

The new SSAE 18 standard is pronounced by the American institute of certified public accountant (AICPA) for use of all attest engagements including for a service organization. The SSAE 18 –SOC criteria are used to evaluate the internal control environment of a service organization as part of a financial statement audit of the user organization under AT-C 320. SOC now stands for "System and Organization Controls". Formerly it was "Service Organization Controls". The Service Auditor is to report on Controls implemented and/or operating effectively at the Service Organization.

The standard requires organizations to demonstrate controls in operations and its design to achieve objectives set forth. SOC report is attested by an Independent Auditor. The auditors are subjected to training, continuous professional education by the AICPA. Further, the engagements are subject to peer reviews periodically. The standard provides for two types of reporting Type 1 and Type II as covered in this document.

SOC REPORTS FOR CYBERSECURITY RISK MANAGEMENT

In 2017 AICPA has developed a cybersecurity reporting framework that organizations can use to demonstrate to key stakeholders the extent and effectiveness of an entity's cybersecurity risk management program. A critical element of any cybersecurity risk management program is the formulation of objectives by management. Management establishes cybersecurity objectives that address cybersecurity risks that could affect the achievement of the entity's overall business objectives (including compliance, reporting, and operational objectives). They may vary depending on the environment in which the entity operates, the entity's mission and vision, the overall business objectives established by management, risk appetite and other factors.

NEED (DEMAND) FOR SOC REPORTS FOR CYBER RISK

Cyber risk has become a front-and-center issue in today's global economy. The media is rife with reports of cyberattacks ranging from major customer records thefts and health care records breaches, to political incidents.

Unfortunately, we are living in a world where the risk of a cyber intrusion is no longer a question of if, but a question of when. In fact, according to the **World Economic Forum 2017 Global Risk Report, data fraud or theft, and cyberattacks rank fifth and sixth, respectively, on their list of Top Ten Risks in Terms of Likelihood.**

In a WEF article, "What cyber-security insiders discussed at Davos 2017," industry insiders made three points about the theme of the summit — "responsive and responsible leadership":

1. Be proactive, prevent threats and prepare yourself.
2. Educate your people.
3. Promote cyber resilience.

Systems security is no longer an issue that resides solely with the IT department and chief information officer. In this age, it is imperative that executives and boards take a top-down, bottoms-up and organization-wide approach to cybersecurity. It provides an understanding of security risks, approaches and responses to addressing this threat. In addition, it incorporates essential elements from a framework developed by the American Institute of CPAs that you can use to develop an effective cybersecurity risk management program and ensure the continued success of your organization.

Cybersecurity brings extraordinary challenges. Organizations face varying threats with varying impacts—all in an environment marked by rapid technological change. What's more, various stakeholders must gather information and converse about cybersecurity between and among each other.

The nature of cybersecurity challenges requires that every sector of the economy play a role. While government policy and activity will be important in promoting cybersecurity resilience, the energy, agility, and innovation of the private sector must be harnessed as well. The auditing profession will do its part by playing a key role in helping organizations—public and private—adapt to this challenging landscape.

Given the high-profile nature of cyber-attacks on corporations, both the demand for information related to cybersecurity—and the need to facilitate robust conversations on these topics—have grown exponentially across major stakeholder groups.

Board members: Boards of directors need information about the entity's cybersecurity program and the cyber threats facing the entity to help the boards fulfill their oversight responsibilities. They also want information that will help them evaluate the entity's effectiveness in managing cybersecurity risks.

Cost of doing business in the digital age		
$4 million is the average cost of a Data Breach	$158 is the average cost per lost or stolen Record	The biggest financial consequence is lost Business and Customers

Source Ponemon Institute

CYBER THREATS

Many organizations that transact business today are susceptible to a cybersecurity breach. Why? One key reason is that cybersecurity threats emerge from a diverse and growing number of sources.

Cybercriminals seek to steal data from organizations to use it for quick, unlawful financial gain.

Nation-states may launch cyber-attacks to conduct economic espionage or to fulfill geopolitical objectives (or both).

Employees, unfortunately, are all too often a source of compromised security access. Even when organizations and employees have the best of intentions, unintentional security lapses can occur when employees use basic passwords or succumb to phishing emails and other seemingly genuine correspondence. These types of internal threats heighten the need for better internal controls, training, and monitoring of compliance within an organization's

Investors: When making investment decisions, analysts and investors need information about an entity's cybersecurity measures. This information can help them understand the cybersecurity risk that could threaten the achievement of the entity's operational, reporting, legal, and regulatory objectives—which each can have implications for an entity's market value. own system.

Regulators: Regulators may benefit from information about an entity's cybersecurity risk management program to support their oversight role.

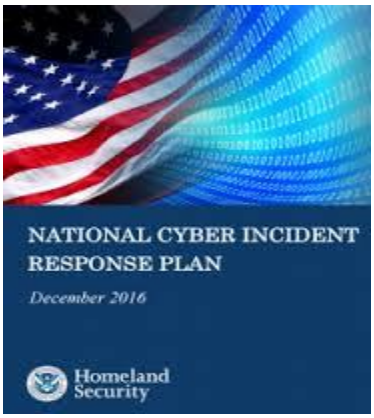
Business partners: Business partners may need information about the entity's cybersecurity risk management program as part of its overall risk assessment. This information can help them determine matters such as the entity's ability to provide goods/services in the event of a disruption to its IT systems.

Complicating all these threats is the fact that technology continues to evolve rapidly. As organizations have hardened their security defenses, adversaries have shifted to new tactics and targets, requiring organizations to continuously evolve their cybersecurity risk management programs.

As threats multiply and technology evolves, the consequences for stakeholders vary in turn. For investors, consequences of a cybersecurity breach can include loss of business or public trust that

can reduce the value of their investment. Customers and business partners may face denial of access to products and services due to an attack or have to grapple with disclosure of their confidential information.

CYBER RESPONSES



Previously, most companies relegated all things "cyber" to the IT department. Today, the trend has shifted, and C-suites and boards of directors are increasing their oversight and accountability for cyber risk. As recognition grows that cyber risks also come from personnel practices, supply chain management, and operational decisions, a more enterprise-wide approach to managing these risks is evolving. Senior management, with board oversight, is taking on more of the challenging work of developing a comprehensive cybersecurity risk management program, including an effective internal control structure that responds to the identified threats and the evolving cybersecurity risk environment.

As management and boards endeavor to determine their responsibilities related to cybersecurity, many organizations are still working towards the most comprehensive and effective cybersecurity risk management structure. Just a few years ago, management and boards had limited resources in designing a framework for risk identification, response, control design and implementation, assessment, and recovery. Now, there are several leading frameworks as well as numerous standards, methodologies, and processes that have been put forth by federal and state governments, industry specific groups, independent agencies, and other stakeholders.

These frameworks exist to aid companies in designing cybersecurity controls specific to cybersecurity risks. AICPA's cybersecurity reporting framework facilitates the ability of a company to describe, in a common language, their enterprise-wide cybersecurity risk management program.

WHY CPA FOR CYBER RISKS

In approaching cybersecurity, audit firms offer key strengths:

Core CPA values and attributes: Adhering to core values of independence, objectivity, and skepticism, Certified Public Accountants (CPAs) are viewed by management and boards as trusted advisors who have a broad understanding of businesses, who receive appropriate annual training, who comply with a code of ethics, and who are subject to rigorous external quality reviews.

Experience in independent evaluations: Audit firms have deep experience in independent evaluations, with the most common example being the financial statement auditor's opinions, required by US federal law for most public companies, on the audits of financial statements and internal control over financial reporting (ICFR). Additionally, many CPA firms have built substantial information technology (IT) practices that provide attestation and advisory services to entities on IT security-related matters and the effectiveness of IT security controls.

Multidisciplinary strengths: Today's public accounting firms employ individuals with CPAs
as well as other credentials specifically related to information technology and security. These include Certified Information Systems Security Professionals (CISSP), Certified Information Systems Auditors (CISA), and Certified Information Technology Professionals (CITP).

AICPA CYBERSECURITY REPORTING FRAMEWORK

The AICPA's cybersecurity reporting framework has been developed to provide the market with a common approach to reporting on and evaluating a company's cybersecurity risk management program. A common and consistent approach for companies to report information about their cybersecurity risk management program, once established and accepted in the market, could potentially reduce industry and other regulatory compliance requirements that can

- distract company resources away from cybersecurity risk management and
- burden companies with checklist compliance exercises that are typically ineffective responses to advancing data security threats.

Widespread market consensus around a given approach can aid in establishing a uniform, cross-industry methodology to evaluating a company's cybersecurity risk management program.

Key components of the reporting framework

This reporting framework represents a major step forward in addressing cybersecurity challenges. The reporting framework provides the user with three key pieces of information that, taken together, can greatly enhance the confidence that a user can place on the cybersecurity information provided by management.

Management's Description of the Entity's Cybersecurity Risk Management Program. Management will provide potential users with a description of an entity's cybersecurity risk management program. Management will utilize suitable description criteria in developing Management's

Description of the subject matter, and for CPAs in evaluating the description. **The AICPA's Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program (Description Criteria) has been designed to be suitable criteria.**

The Description Criteria are categorized into **nine areas** so that Management's Description provides users with information about an entity that will enable them to better understand the entity and its cybersecurity risk management program. Management's Description will include information about the entity's operations, how the entity identifies its sensitive information and systems, the ways in which the entity manages the cybersecurity risks that threaten it, and a summary of cybersecurity controls processes. **Management's Description is intended to provide the context needed for users to understand the conclusions expressed by management in its assertion, and by the auditor in its opinion**

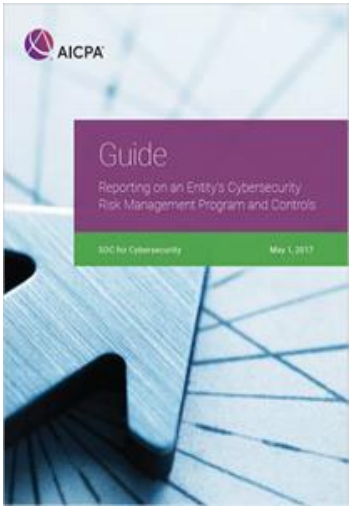
Nine areas are:

- Nature of Business and Operations
- Nature of Information at Risk
- Cybersecurity Risk Management Program Objectives (Cybersecurity Objectives)
- Factors that Have a Significant Effect on Inherent Cybersecurity Risks.
- Cybersecurity Risk Governance Structure
- Cybersecurity Risk Assessment Process
- Cybersecurity Communications and the Quality of Cybersecurity Information
- Monitoring of the Cybersecurity Risk Management Program
- Cybersecurity Control Processes

Management's Assertion: Management will assert to the presentation of the Management's Description of the entity's cybersecurity risk management program in accordance with the description criteria, and whether the controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on a suitable set of control criteria. One example of suitable control criteria is the 2017 Trust Services Criteria (criteria for security, availability, and confidentiality).

The CPA's Opinion. The CPA's Report contains an opinion on

- the description of the entity's cybersecurity risk management program **(Type I Report)** and
- the effectiveness of the controls within the program to achieve the entity's cybersecurity objectives **(Type II Report)**



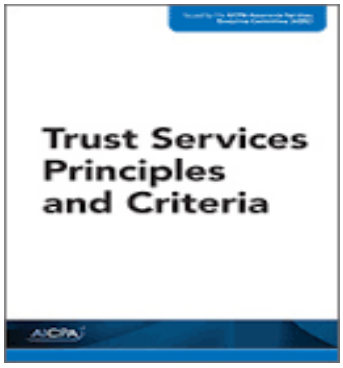
The cybersecurity reporting framework is objectives based and voluntary. Of course, the Examination cannot prevent a cybersecurity threat or breach, nor is it designed to. It can, however, add substantial credibility to assertions made by management about their cybersecurity risk management program to protect information and data, thereby increasing stakeholder confidence.

The reporting framework and its accompanying Examination would be separate and apart from the existing financial statement audit process.

OPTIONAL FRAMEWORKS

The following are the various optional frameworks that can be used for SOC reporting for Cyber Risk Management.

New Trust Services Criteria (TSC) with COSO



This guidance is used in reporting on SOC engagements. The 2017 edition revises the TSC to align with the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) 2013 Internal Control—Integrated Framework, to better address cybersecurity risks and increase flexibility in application across an entire entity, including at a subsidiary, division, or operating unit level within a function relevant to an entity's operational, reporting, or compliance objectives.

NIST Framework for Improving Critical Infrastructure Cyber Security

A 2013 Presidential Executive Order called for the creation of a voluntary, risk-based cybersecurity framework that would provide a set of industry standards and best practices for all organizations. The resulting NIST framework came together with collaboration between industry and government. Organizations can turn to the C³ Voluntary Program, which was created to help organizations use the NIST Cybersecurity Framework to improve their cyber resilience. According to the United States Computer Emergency Readiness Team, the program connects organizations with public and private sector resources that align to the NIST Framework's five functional areas: Identify, Protect, Detect, Respond, and Recover.

NIST National Institute of Standards and Technology U.S. Department of Commerce

ISO/IEC 27001/27002

Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), this group of standards is intended to be used as guidance for securing financial information, intellectual property, employee data, and other information entrusted to the organization by third parties.

ISO 27001

OBJECTIVES OF THE AICPA'S REPORTING FRAMEWORK

Provide useful information to a broad range of users, while minimizing the risk of creating vulnerabilities — Information provided in the report would meet the shared needs of a broad spectrum of users.

Provide comparability — The report provides users with information that could be used to compare both with other organizations and for the same organization across time.

Permit management flexibility — The framework would not constrain management to a particular cybersecurity description or control framework.

Connect the dots on best practices — The framework enables management to consider best practices encouraged by most commonly used control and cyber frameworks regardless of which framework(s) management has chosen to follow internally.

Be voluntary — The framework is valuable to organizations and their stakeholders to drive adoption in the marketplace.

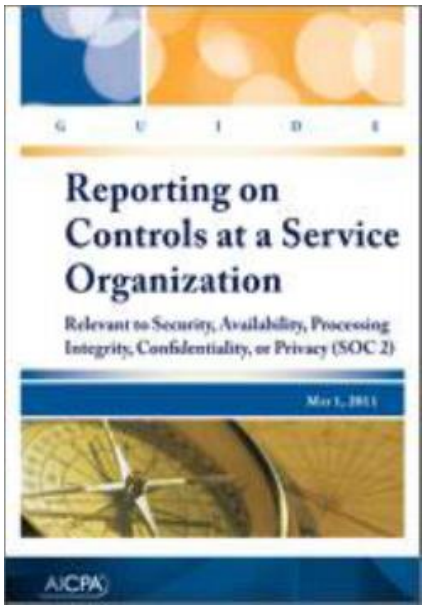
Be scalable and flexible — The framework is useful to organizations of varying sizes and across all industries.

Evolve to meet changes — The framework will be updated and modified over time based on marketplace adoption, a changing environment, and organizational and stakeholder needs.

WHY SOC Type II FOR CYBER RISK MANAGEMENT

- SOC Type II report can cover the entire year and the effectiveness of the controls in place can be reported
- It is a Third Party Period- of-Time assessment and so has Accountability
- Since it is a period of time assessment, it is more like a continuous compliance with low risk and high reliability
- Most other assurance programs or audits are only, at a point in time
- Comprehensive Framework for managing cyber risks
- Provides a high reliability SOC Seal by AICPA

SOC ENGAGEMENTS or AUDITS

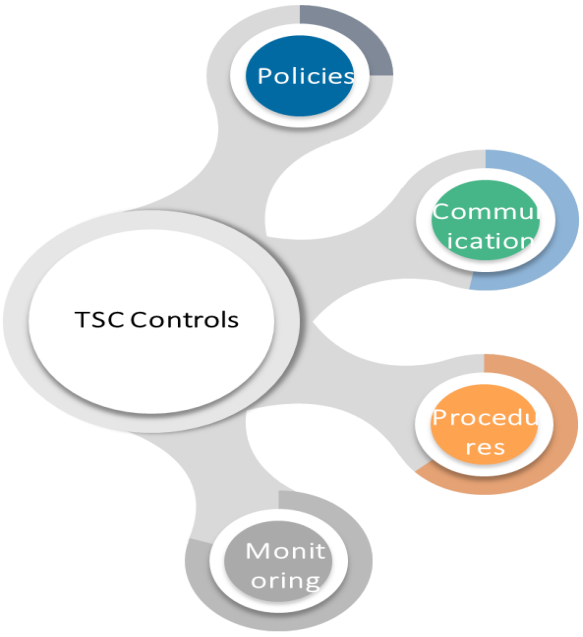


- Technically SOC is an Attest Report not an Audit Report.
- SOC - "System Organization Controls"
- Controls implemented and/or operating effectively at the Organization
- Provide information and a Service Auditors (Practitioner in case of SOC for Cyber Risk) independent opinion about controls at the organization to Management, Stakeholders and other concerned parties
- Provides user entities (customers) with detailed information on the design and/or operating effectiveness of the service organization's implemented controls
- Organizations are required to provide a Management Assertion letter and a System Description which provides the basis of reporting for the service auditor/ practitioner.

TRUST SERVICES CRITERIA AS A CONTROL TOOL

The 2017 Trust services Criteria can be used as a control and reporting tool. It broadly covers the following reporting structure:

- **CC1 – Control Environment**
- **CC2 – Communication and information**
- **CC3 - Risk Assessment**
- **CC4 - Monitoring Activities**
- **CC5 – Control Activities**
- **CC6 - Logical and Physical Access Controls**
- **CC7 - System Operations**
- **CC8- Change Management**
- **CC9 - Risk Mitigation**



Additional principle-specific criteria.

A - Additional Criteria for Availability
C- Additional Criteria for Confidentiality

TYPICAL SCOPE OF WORK (SOW)

Cybersecurity Risk Management Examination

- Usually addresses an entity-wide cybersecurity risk management program or
- A Portion of the Entity's Cybersecurity Risk Management Program

The cybersecurity risk management examination may be limited to any of the following:

One or more specific business units, segments, or functions of an entity:

- when those units, segments, or functions operate under an entity-wide cybersecurity risk management program or
- when those units, segments, or functions operate under an independent cybersecurity risk management program

One or more specific types of information used by the entity:

In those situations, the description is tailored to disclose only information about the portion of the cybersecurity risk management program (that is, the particular business unit, segment, or type of information) within the scope of the engagement. Likewise, when evaluating whether the description is presented in accordance with the description criteria, consideration would be given to whether the description addresses all relevant aspects of the portion of the cybersecurity risk management program within the scope of the engagement. For example, if the engagement addresses only one specific business unit, and that unit's cybersecurity risk management program relies on aspects of the entity-wide program, the description would also include disclosure of those aspects of the entity-wide program relevant to that business unit.

OUR PROJECT EXECUTION METHODOLOGY

Key steps in SOC engagement

Plan	Deliver	Access	Report
Understanding the client entity and environment	Understanding and verifying documentation of existing internal controls	Evaluate Samples	Evaluate additional info
Define scope, expectations and project roles	Perform Walkthrough	Analyze Samples for effectiveness	Request clarifications
Readiness Assessment if required	Assess Risks	Request additional info	System Description and Management Assertions is drafted through inputs from the audit team by the client management
Kick off meeting with Stakeholders	Identifying the control objectives and controls in place		Issue draft report
Preliminary interviews / questionnaires conducted to gain understanding of requirements	Conduct Interviews		Incorporate Management comments and Issue final report
Client information request list prepared and distributed	Request Samples		Ongoing support
Analysis of client-prepared information performed and client feedback provided	Validation of the implementation of controls		Answer questions to Management and User Auditors
Project timeline (including estimates of client hours) / plan created	Test results communicated and exceptions are resolved, if possible		
Update Plan based on client discussions			

ACCEDERE

VALUE DELIVERY

Knowing how much extra value and assurance a SOC reports can deliver, many clients find that it makes sense to take steps to ensure a more successful outcome, including hiring experts who are skilled in helping organizations be more thorough and thoughtful in how they approach their engagement. Preparing for a SOC engagement is a matter of clear thinking and smart planning. Working with a cyber security specialized consulting specialists such as ours, helps you dig into areas such as cloud security, data security, incident response, change management processes and much more.

We provide end to end process for SOC Engagements. With the rapid Cloud adaption and increased use of IoT, Big Data and Analytics, Cloud Security and Privacy concerns are on the rise. We can conduct integrated SOC engagements with privacy engagements or use your existing implemented best practices to evaluate your environment and to reduce the duplicate efforts and save costs for you.

Some of the advantages of working with us are:

A
End to end process for SOC Reporting & Attest Services
Project management methodology consistently applied to each engagement

B
Efficient service delivery with minimal disruption to operations
Our engagements are executed by senior experienced professionals

C
15 years of Information Security & Cyber Security experience
Reduced time to complete assignments

D
Licensed CPA & Security Professionals to execute projects & provide attest reports
Prompt services with engagements completed in record time

E
Ongoing support. We are with you whenever you need us
Our services are competitively priced than BIG names to provide higher ROI

To discuss your specific need please email info@accedere.us