Journal of Accounting, Finance, Economics, and Social Sciences
Vol 6, No 2, July – December 2021, pp. 19-29
Received: Jul 2021 | Revised: Oct 2021 | Accepted: Dec 2021
DOI: https://doi.org/10.62458/jafess.160224.6(2)19-29

SOC for Cybersecurity & SOC 2® for Service Organizations – An empirical study on industry's perspective

Anil K. Makhija*

ABSTRACT

Businesses across the globe have been going digital. A paradigm that has been accelerated due to pandemic. This has resulted into creation of a complex cyberspace. Further, organizations have become linked and dependent on each other, due to increased outsourcing as well as shift towards cloud computing. This has also led to creation of various industry standards and frameworks that help organizations evaluate their own and their provider's practices related to system reliability, information security and cybersecurity. Amongst these, SOC2 for service organizations and SOC for Cybersecurity are two leading reports that help organizations assess system reliability and cybersecurity. AICPA recognizes it has that there is confusion amongst the applicability of these reports, and therefore it has created some guidance on how these two reports are different and how they can be leveraged by organizations. This guidance provides an inside-out perspective driven by purpose of these reports and the methodology used to create these reports. The industry (practitioners, implementors and vendor managers, CXOs) perspective on the applicability and distinction of these reports was not yet available. This research brings out industry (practitioners, implementors and vendor managers, CXOs) perspective on the applicability and distinction of these reports. Findings indicate that SOC2 demand and usefulness is perceived high whereas SOC for Cybersecurity demand and usefulness is perceived low by the industry. Findings of this research also indicate that industry excepts AICPA to simplify SOC2 reports and make them easier to understand.

Keywords: SOC2, SOC for Cybersecurity, systems reliability, AICPA, trust services criteria

INTRODUCTION

Technology has been enabler for businesses to improve their operational efficiencies and effectiveness. With the growing reliance on technologies, companies have adopted to outsourcing their work to service providers across the globe. Companies that outsource their work are interested to understand how effective are the systems reliability controls, both in terms of design and operating effectiveness. SOC2 report framework, from AICPA, is one such mechanisms that has helped user organizations to get assurance on systems reliability controls of the outsourced work/functions. AICPA introduced SOC for Cybersecurity in 2017, though the adoption of SOC for Cybersecurity has been much lower as compared to SOC2. the Aim of this research is to get perspective of industry practitioners on SOC2 and SOC for Cybersecurity. Industry practitioners, from user organizations, service provider organizations and service auditor companies have been interviewed through a survey questionnaire. Those practitioners are in the roles of CxOs, Vendor Managers, Service Auditors and Compliance professionals. They were interviewed on both the demand as well as usefulness of SOC2 and of SOC for Cybersecurity. They were also asked about any improvement suggestions for both these reports.

LITERATURE REVIEW

Cyberspace & Cybersecurity

Organizations across the world have been undergoing significant digital shift during the last decade. This digital shift has accelerated even further during the times of covid-19 pandemic. One of the effects of this shift has also been the increased exposure of almost every organization to the cyberspace risks. Cyberspace risks have always been there. However, pandemic driven increased digital reliance, has led to an increase in this exposure. Cyberattacks have been going up and at the same

* Anil K. Makhija, B.E., PGDIM, MBA, Assistant Professor, CamEd Business School
Email: anil@cam-ed.com

time, there is a trend that managers disclose only less severe cyberattacks or disclose them when investors and other stakeholders already suspect that an attack has happened. Thus, cybersecurity topic is getting immense attention these days. Exponential growth of internet connections has not only led to an increase in cybersecurity incidents, the impact of such incidents has also gone up significantly. There is a strong realization on the part of governing boards within many organizations that keeping their organization secure in the cyberspace shall come under the purview of corporate governance (Amir et al., 2018; Jang-Jaccard & Nepal, 2014; Von & von, 2018).

Concepts of information security and cyber security have significant overlap and are closely related. General security objectives for cyber security consist of confidentiality, integrity and availability, which are very similar to the objectives of information security (Von & Van, 2013).

According to the international standard, ISO/IEC 27002 (2013), information security is the preservation of the confidentiality, integrity and availability of information. As per this explanation, information can be printed or it can be written on paper or it can be stored electronically. It can be transmitted by electronic means, shown on various medias or conveyed in conversations and so on (ISO/IEC 27002, 2013).

Value of information is driven by the characteristics it possesses. Three characteristics of information, that make information valuable for organizations are known as CIA triangle or confidentiality, integrity, and availability. However, in the constantly changing environment, in addition to these three elements, accuracy, authenticity, utility and possession are the additional characteristics of the information that need to be protected (Whitman & Mattord, 2012).

There is significant overlap in the scope of information security and cyber security. Preserving the confidentiality, integrity and availability of information in the cyber space is what comes under the purview of cyber security. According to the international standard, ISO/IEC 27032 (2012), cyberspace is a very complex environment, created by interactions amongst people, software and services over the internet by means of technology devices and networks connected to it (ISO/IEC 27032, 2012).

Information security focuses on protecting the information from possible harm resulting from various threats and vulnerabilities. Cyber security focuses on protecting the cyberspace, protecting those who function in the cyberspace and protecting any of their assets that can be reached via the cyberspace. Boundaries of cyber security and of the risks protected by it are wider than those of information security (Reid & Van, 2014).

Increasing adoption of outsourcing and shift towards cloud computing has led to increased usage of third-party vendors. This has created a need to not only ensure internal controls for information and cyber security within the organization, but also to assess and evaluate the validity (both design and operating effectiveness) of the internal controls put in place by these third-party providers (Fanning, 2014).

Standards and Frameworks for managing Information Security and Cybersecurity

Over the last 30 years, many industry standards have been rolled out to help IT Governance and information security. Most of them contain elements to help organizations address IT security and Information Security. The most popular ones related to information security are ISO 27001, BS7799, PCI-DSS, ITIL and COBIT (Susanto et al., 2012).

AICPA, in 2010, rolled out SOC for Service Organizations. These reports were designed to help service organizations that provide services to other entities. SOC repots help build trust and confidence in the services performed and controls related to the services. These reports are created by an independent CPA. Of these reports, SOC 2® report is of particular interest in the context of security, availability, processing integrity, confidentiality or privacy (SOC for Service Organizations: Information for Service Organizations, n.d.).

AICPA's SOC 2® - SOC for Service Organizations

AICPA's SOC 2® - SOC for Service Organizations: Trust Services Criteria (SOC 2® - SOC for Service Organizations: Trust Services Criteria, n.d.) provides detailed information and assurance about the controls at a service organization relevant to security, availability and processing integrity of systems that are used by service organization to process the user's data, and confidentiality and privacy of the information that is processed by these systems, as indicated in Figure 1. Privacy criteria was added as a dedicated section in 2016 (Giulio et al., 2017). A SOC 2® report is a restricted use report and is of two types.

- Type 1 report is about management's description of a service organization's systems and suitability of design of controls
- Type 2 report is about management's description of a service organization's systems and suitability of design and operating effectiveness of controls.

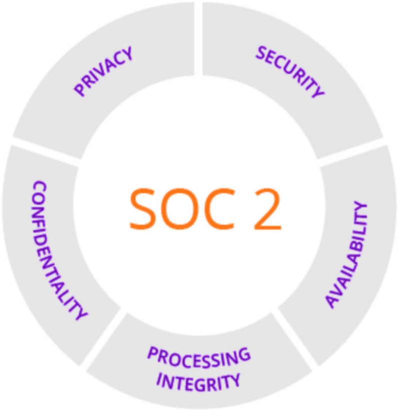


Figure 1: Soc Criteria

High-profile breaches and cybersecurity incidents at Equifax, Sony, and Target have increased the cybersecurity focus of both the professionals as well as the regulators. Cybersecurity risk management has taken a strategic dimension and strategy, IT management, cybersecurity investment, and improving the internal controls are considered integral part of it (Janvrin & Wang, 2019).

Some of the academic research suggests Cybersecurity practices and policies being reactive and not able to address the challenge of rapidly evolving cyber threats. It is also recommended that addressing this will require rapid transformation in computing and systems architecture (Sheldon & Vishik, 2010). Research also indicates that cybersecurity strategy (CSS) also has a significant role in managing the cyberthreats. It will have three broad components of formulation, implementation, and evaluation. Some of the research has proposed a holistic cybersecurity implementation framework to implement CSS (Atoum et al., 2014). There has been research indicating that developing cybersecurity culture and awareness and making IT Audits and Information Security audits address cyber threats, risks and attacks is necessary. Holistic cybersecurity models, combining the best practices from Cybersecurity Framework of NIST and few other models have been proposed (Sabillon et al., 2017). In order to assess the cybersecurity maturity, Cybersecurity Capability Maturity Model, consisting of four levels and based on three dimensions of people, process and technology have also been introduced (De Bruin & von Solms, 2015). Researchers have also recommended some industry specific cybersecurity frameworks, such as SHIELD framework for telco environment which offers security as a service or Buildings Cybersecurity Framework (BCF) for residential, small commercial, large commercial, and federal buildings (Gardikis et al., 2017; Mylrea et al., 2017). Earlier research has also indicated that while mobile financial services are an enabler for financial inclusion to provide banking to the unbanked, lack of resilient cybersecurity governance is a challenge and having a robust cybersecurity framework implemented can help address this challenge (Ambore et al., 2017). Emergence of multiple frameworks to manage cybersecurity risks has also created a challenge of how those frameworks have to be implemented and optimized so as to existing resources are not strained or mis utilized. To address that, researchers have proposed models that guide how various elements / factors within an organization, such as people, process and technology can be leveraged to the objective of cybersecurity risk management programs in compliance with NIST Cybersecurity framework (Teodoro et al., 2015). Managing cyber risk is therefore extremely important for businesses to ensure their sustenance and reliability. Managing cyber risks using a systematic approach is extremely important (Kosub, 2015).

AICPA's SOC for Cybersecurity

In 2017, in response to these growing challenges, the American Institute of Certified Public Accountants (AICPA, 2017; Eaton et al., 2019) developed an entity-level voluntary cybersecurity reporting framework that firms can use to disclose useful information to stakeholders about their cybersecurity risk management program and its effectiveness. The framework consists of the following three components that aim to assist stakeholders in monitoring a firm's cybersecurity risk management program:

- Description Criteria
- Control Criteria
- Attestation Guidance

SOC for Cybersecurity also consists of Type 1 Report and Type 2 report. Type 1 report, which is also referred to as a point-in-time report, describes the service organization's system and verifies whether the controls are suitably designed to meet the specified control objectives. Type 2 report, which is also referred to as a specific point-in-time report, includes same information as the Type 1 report and additionally includes management assertion and an auditor's opinion on operating effectiveness of the controls.

SOC 2® and SOC for Cybersecurity reports have similar structure. Management has the flexibility of choosing the scope of SOC 2® relating to products and services assessed. However, the assessment has to be based on Trust Services Criteria. In case of SOC for Cybersecurity, objectives are defined by the management. The report then provides an assessment on entity's cybersecurity risk management program and the effectiveness of controls to meet those objectives.

CURRENT CHALLENGES & RESEARCH OBJECTIVES

Current Challenges / Open Issues

Ever since the release of SOC for Cybersecurity in 2017, there have been questions about distinction between SOC2 examination and SOC for Cybersecurity examination. AICPA has made an attempt to clarify these differences and categorized them into audience, subject matter and scope of each of the report.

- One of the key differences explained by AICPA is that while a SOC for Cybersecurity report would contain an opinion about the effectiveness of controls within a cybersecurity risk management program, it would not include the details of the tests performed to evaluate this effectiveness and neither would it include the results of those tests. Such information about details of tests conducted and the results of those tests are included in SOC 2 report.
- To measure and evaluate the cybersecurity risk management program's effectiveness, in SOC for Cybersecurity, management can choose the control criteria to be used. Management has the option to use AICPA Trust Services Criteria for security, availability, and confidentiality as control criteria. Whereas, a SOC 2 examination can only be performed using the AICPA trust services criteria.
- SOC 2 reports are restricted use (for specified users) reports whereas SOC for Cybersecurity are for general use (for general users).

Despite this guidance from AICPA, which are provided more from an inside-out perspective, leveraging the purpose and methodology to create these reports, there is a need to understand the industry perspective on these two reports.

RESEARCH OBJECTIVES

Hence the research involves conducting a survey, based on interview/questionnaire, of practitioners and implementors (in the organizations that provide the services) and vendor managers and CXOs (in the recipient of service organizations). The geographical coverage would be organizations in North America, Europe, and Asia. The interview would focus on gathering empirical information on the following dimensions (which will then be analyzed and presented as research findings):

- How are these two reports, namely SOC 2 and SOC for Cybersecurity, perceived by organizations, especially the provider organizations (practitioners and implementors) and receiver organizations (vendor managers, CXOs)?
- Which of these two reports they find more useful, in which context and why?
- What improvements can be made in these two reports?

METHODOLOGY

This research aims to understand how the two reports, namely SOC2 and SOC for cybersecurity are perceived by the practitioners in the industry, both on the service provider side as well as user organization side. It also aims to get their perspective on the usefulness of these reports and what improvements they can recommend in these reports to make them more meaningful and useful from their perspective.

A survey questionnaire was designed to understand the following dimensions:

- Demand / Requirements for SOC2 reports
- Demand / Requirements for SOC for Cybersecurity reports
- Usefulness of SOC2 reports
- Usefulness of SOC for Cybersecurity reports
- Suggested improvements in SOC2 reports
- Suggested improvements in SOC for Cybersecurity reports
- Other industry certifications that are considered important / relevant in addition to SOC2 and SOC for Cybersecurity

Information Technology & Services companies and outsourcing services providers who provide SOC2 and / or SOC for cybersecurity reports to their client organizations, leading banks and financial services companies (user organizations) who request SOC2 and SOC for Cybersecurity reports from their vendor partners and auditing companies that are involved as service auditors were identified as entities in the scope of the survey. Professionals working in these organizations involved directly with the compliance programs, working as implementers or working as service auditors were reached out.

Out of total 140 persons reached out;

- 106 persons provided their responses, mostly through on-call interviews though some preferred to respond offline after the survey objectives and questions were explained to them
- 13 persons responded that they would not feel comfortable in sharing the details
- 2 persons responded that they do not have sufficient details to be able to provide meaningful responses
- 19 persons did not respond to the survey request

Distribution of survey respondents with respect to geographic coverage and organization size (measured in terms of headcount) is shown in Table 1 and 2 and Chart 1 and 2. The coverage is across all geographies of the world and organization size wise distribution is also uniform.

Table 1: Survey Respondents- Geographic Distribution

Geographic Coverage - Based on Place of Work	Count	% Distribution
Asia	37	35%
Australia & New Zealand	7	7%
EMEA (Europe, Middle East, Africa)	26	25%
Americas (USA, Canada, LATAM)	36	34%
Total	106	100%

Chart 1: Survey Respondents- Geographic Distribution

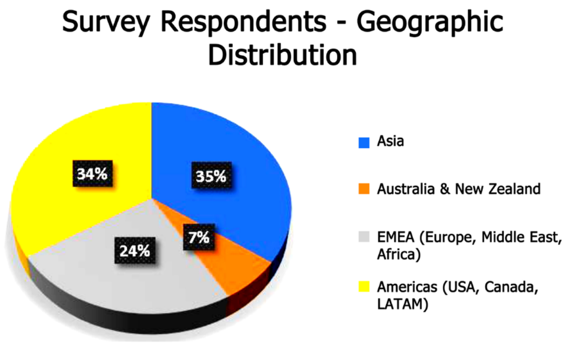
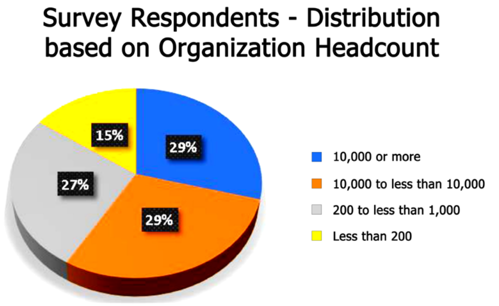


Table 2: Survey Respondents – Distribution based on Organization Headcount

Organization Headcount	Participants	% Participants
10,000 or more	31	29%
1000 to less than 10,000	31	29%
200 to less than 1,000	28	26%
Less than 200	16	15%
Total	106	100%

Chart 2: Survey Respondents – Distribution based on Organization Headcount



RESULTS

SOC2 Demand & SOC for Cybersecurity Demand Comparison

From the survey responses, it is evident that SOC2 demand is considered as "high", considering all the survey responses. Demand for SOC for Cybersecurity is tending towards "very low". This is shown in Table 3A and Table 3B. There are significant number of respondents who believe that there is no demand for SOC for Cybersecurity or they don't have a perspective on it. The pattern of "high" demand for SOC2 and "very low" demand for SOC for Cybersecurity is consistent across the functions/roles of vendor management, service auditors, compliance professionals, CxOs and others. This is reflected in the tables, from Table 4A and 4B onwards till Table 8A and 8B.

All Participants

Table 3A: SOC2 Demand – All Participants

SOC2 Demand	Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	16	15%
4- High	53	50%
5- Very High	37	35%
There is No Demand for it	0	0%
I don't have a perspective on it	0	0%
Total	106	100%

Table 3B: SOC for Cybersecurity Demand – All Participants

SOC for Cybersecurity Demand	# Participants	% Participants
1- Very Low	47	44%
2- Low	17	16%
3- Medium	11	10%
4- High	2	2%
5- Very High	0	0%
There is No Demand for it	24	23%
I don't have a perspective on it	5	5%
Total	106	100%

Vendor Management Function

Table 4A: SOC2 Demand – Vendor Management Team

SOC2 Demand	Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	1	7%
4- High	5	33%
5- Very High	9	60%
There is No Demand for it	0	0%
I don't have a perspective on it	0	0%
Total	15	100%

Table 4B: SOC for Cybersecurity Demand – Vendor Management Team

SOC for Cybersecurity Demand	# Participants	% Participants
1- Very Low	4	27%
2- Low	1	7%
3- Medium	5	33%
4- High	0	0%
5- Very High	0	0%
There is No Demand for it	5	33%
I don't have a perspective on this	0	0%
Total	15	100%

Service Auditors

Table 5A: SOC2 Demand – Service Auditors

SOC2 Demand	Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	0	0%
4- High	10	45%
5- Very High	12	55%
There is No Demand for it	0	0%
I don't have a perspective on it	0	0%
Total	22	100%

Table 5B: SOC for Cybersecurity Demand – Service Auditors

SOC for Cybersecurity Demand	# Participants	% Participants
1- Very Low	10	45%
2- Low	3	14%
3- Medium	2	9%
4- High	0	0%
5- Very High	0	0%
There is No Demand for it	7	32%
I don't have a perspective on this	0	0%
Total	22	100%

Compliance Professionals

Table 6A: SOC2 Demand – Compliance Professionals

SOC2 Demand	Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	1	5%
4- High	11	55%
5- Very High	8	40%
There is No Demand for it	0	0%
I don't have a perspective on it	0	0%
Total	20	100%

Table 6B: SOC for Cybersecurity Demand – Compliance Professionals

SOC for Cybersecurity Demand	# Participants	% Participants
1- Very Low	7	35%
2- Low	6	30%
3- Medium	0	0%
4- High	0	0%
5- Very High	0	0%
There is No Demand for it	7	35%
I don't have a perspective on this	0	0%
Total	20	100%

CxOs

Table 7A: SOC2 Demand – CxOs

SOC2 Demand	Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	7	37%
4- High	8	42%
5- Very High	4	21%
There is No Demand for it	0	0%
I don't have a perspective on it	0	0%
Total	19	100%

Table 7B: SOC for Cybersecurity Demand – CxOs

SOC for Cybersecurity Demand	# Participants	% Participants
1- Very Low	8	42%
2- Low	6	32%
3- Medium	3	16%
4- High	2	11%
5- Very High	0	0%
There is No Demand for it	0	0%
I don't have a perspective on this	0	0%
Total	19	100%

Others

Table 8A: SOC2 Demand – Others

SOC2 Demand	Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	7	23%
4- High	19	63%
5- Very High	4	13%
There is No Demand for it	0	0%
I don't have a perspective on it	0	0%
Total	30	100%

Table 8B: SOC for Cybersecurity Demand – Others

SOC for Cybersecurity Demand	# Participants	% Participants
1- Very Low	18	60%
2- Low	1	3%
3- Medium	1	3%
4- High	0	0%
5- Very High	0	0%
There is No Demand for it	5	17%
I don't have a perspective on this	5	17%
Total	30	100%

SOC2 Usefulness & SOC for Cybersecurity Usefulness Comparison

From the survey responses, it is evident that SOC2 usefulness is considered as "high", considering all the survey responses. Usefulness of SOC for Cybersecurity is tending towards "low". This is shown in Table 9A and Table 9B. There are significant number of respondents who don't have a perspective on usefulness of SOC for Cybersecurity. The pattern of "high" usefulness of SOC2 and "low" usefulness of SOC for Cybersecurity is consistent across the functions/roles of vendor management, service auditors, compliance professionals, CxOs and others. This is reflected in the tables, from Table 10A and 10B onwards till Table 14A and 14B.

All Participants

Table 9A: SOC2 usefulness – All Participants

SOC2 Usefulness	# Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	30	28%
4- High	55	52%
5- Very High	21	20%
It's not useful	0	0%
I don't have a perspective on it	0	0%
Total	106	100%

Table 9B: SOC for Cybersecurity usefulness – All Participants

SOC for Cybersecurity Usefulness	# Participants	% Participants
1- Very Low	27	25%
2- Low	34	32%
3- Medium	18	17%
4- High	6	6%
5- Very High	0	0%
It's not useful	0	0%
I don't have a perspective on it	21	20%
Total	106	100%

Vendor Management Function

Table 10A: SOC2 usefulness – Vendor Management Team

SOC2 Usefulness	# Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	1	6%
4- High	7	47%
5- Very High	7	47%
It's not useful	0	0%
I don't have a perspective on it	0	0%
Total	15	100%

Table 10A: SOC for Cybersecurity usefulness – Vendor Management Team

SOC for Cybersecurity Usefulness	# Participants	% Participants
1- Very Low	9	60%
2- Low	3	20%
3- Medium	3	20%
4- High	0	0%
5- Very High	0	0%
It's not useful	0	0%
I don't have a perspective on it	0	0%
Total	15	100%

Service Auditors

Table 11A: SOC2 usefulness – Service Auditors

SOC2 Usefulness	# Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	0	0%
4- High	14	64%
5- Very High	8	36%
It's not useful	0	0%
I don't have a perspective on it	0	0%
Total	22	100%

Table 11B: SOC for Cybersecurity usefulness – Service Auditors

SOC for Cybersecurity Usefulness	# Participants	% Participants
1- Very Low	12	55%
2- Low	4	18%
3- Medium	3	14%
4- High	1	5%
5- Very High	0	0%
It's not useful	0	0%
I don't have a perspective on it	2	9%
Total	22	100%

Compliance Professionals

Table 12A: SOC2 usefulness – Compliance Professionals

SOC2 Usefulness	# Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	3	15%
4- High	15	75%
5- Very High	2	10%
It's not useful	0	0%
I don't have a perspective on it	0	0%
Total	20	100%

Table 12B: SOC for Cybersecurity usefulness – Compliance Professionals

SOC for Cybersecurity Usefulness	# Participants	% Participants
1- Very Low	0	0%
2- Low	10	50%
3- Medium	2	10%
4- High	2	10%
5- Very High	0	0%
It's not useful	0	0%
I don't have a perspective on it	6	30%
Total	20	100%

CxOs

Table 13A: SOC2 usefulness – CxOs

SOC2 Usefulness	# Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	7	37%
4- High	8	42%
5- Very High	4	21%
It's not useful	0	0%
I don't have a perspective on it	0	0%
Total	19	100%

Table 13B: SOC for Cybersecurity usefulness – CxOs

SOC for Cybersecurity Usefulness	# Participants	% Participants
1- Very Low	4	21%
2- Low	8	42%
3- Medium	5	26%
4- High	2	11%
5- Very High	0	0%
It's not useful	0	0%
I don't have a perspective on it	0	0%
Total	19	100%

Others

Table 14A: SOC2 usefulness – Others

SOC2 Usefulness	# Participants	% Participants
1- Very Low	0	0%
2- Low	0	0%
3- Medium	19	63%
4- High	11	37%
5- Very High	0	0%
It's not useful	0	0%
I don't have a perspective on it	0	0%
Total	30	100%

Table 14B: SOC for Cybersecurity usefulness – Others

SOC for Cybersecurity Usefulness	# Participants	% Participants
1- Very Low	2	7%
2- Low	9	30%
3- Medium	5	17%
4- High	1	3%
5- Very High	0	0%
It's not useful	0	0%
I don't have a perspective on it	13	43%
Total	30	100%

OVERALL COMPARISON - DEMAND

Based on the responses from survey respondents, overall demand on a scale of 0 to 5, with 5 representing “very high” and 1 representing “very low” and 0 representing no demand, the demand for SOC2 is 4.2 and the demand for SOC for Cybersecurity is 1.21. The underlying data, captured based on responses to the survey, is shown in Table 15A and 15B.

Table 15A: SOC2 quantified demand

Role Category	SOC2 Demand						
	1-Very Low	2- Low	3- Medium	4- High	5-Very High	0- No Demand	Weighted Score
Vendor Management	0	0	1	5	9	0	4.53
Auditor / Service Auditor	0	0	0	10	12	0	4.55
Compliance Professional	0	0	1	11	8	0	4.35
CxO (USER ORGNIZATION)	0	0	7	8	4	0	3.84
Others	0	0	7	19	4	0	3.90
Overall Total	0	0	16	53	37	0	4.20

Table 15B: SOC for Cybersecurity quantified demand

Role Category	SOC for Cybersecurity Demand						
	1-Very Low	2- Low	3- Medium	4- High	5-Very High	0- No Demand	Weighted Score
Vendor Management	4	1	5	0	0	5	1.40
Auditor / Service Auditor	10	3	2	0	0	7	1.00
Compliance Professional	7	6	0	0	0	7	0.95
CxO (USER ORGNIZATION)	8	6	3	2	0	0	1.95
Others	18	1	1	0	0	5	0.92
Overall Total	47	17	11	2	0	24	1.21

OVERALL COMPARISON - USEFULNESS

Based on the responses from survey respondents, overall usefulness on a scale of 0 to 5, with 5 representing “very high” and 1 representing “very low” and 0 representing “not useful”, the usefulness of SOC2 is 3.92 and the usefulness of SOC for Cybersecurity is 2.11. The underlying data, captured based on responses to the survey, is shown in Table 15A and 15B.

Table 15A: SOC2 usefulness- quantified

Role Category	SOC2 Usefulness						
	1-Very Low	2- Low	3- Medium	4- High	5-Very High	0- No Demand	Weighted Score
Vendor Management	0	0	1	7	7	0	4.40
Auditor / Service Auditor	0	0	0	14	8	0	4.36
Compliance Professional	0	0	3	15	2	0	3.95
CxO (USER ORGNIZATION)	0	0	7	8	4	0	3.84
Others	0	0	19	11	0	0	3.37
Overall Total	0	0	30	55	21	0	3.92

Table 15B: SOC for Cybersecurity usefulness-quantified

Role Category	SOC for Cybersecurity Usefulness						
	1-Very Low	2- Low	3- Medium	4- High	5-Very High	0- No Demand	Weighted Score
Vendor Management	9	3	0	3	0	0	1.80
Auditor / Service Auditor	12	4	0	4	0	0	1.80
Compliance Professional	0	10	2	2	0	0	2.43
CxO (USER ORGNIZATION)	4	8	5	2	0	0	2.26
Others	2	9	5	1	0	0	2.29
Overall Total	27	34	12	12	0	0	2.11

CONCLUSION

SOC2 report is based on trust principles/criteria and it is performed under the AICPA attestation standard, AT 101. SOC2 is a restricted use report. Entities that outsource tasks and functions to service providers are interested in getting an assurance over non-financial controls revolving around systems reliability. SOC2 has been widely used report by user organizations that are outsourcing their work. With the increase in cybersecurity threats and risks, AICPA launched SOC for Cybersecurity in 2017. There have been some user organizations which have started utilizing SOC for cybersecurity internally to assess effectiveness of their cybersecurity risk management programs. It is evident from the findings of this survey, in which 106 participants representing various functions / roles such as CxOs, Vendor Managers, Service Auditors, Compliance professionals, that industry is seeing very low demand when it comes to SOC for Cybersecurity. Demand for SOC2 is very high. In terms of usefulness, usefulness of SOC for Cybersecurity is low whereas usefulness of SOC2 is high.

In terms of possible improvements, there were very limited or no suggestions on how SOC for Cybersecurity reports can be improved. For SOC2 report, there were significant number of participants, 46%, who suggested that SOC2 report needs to be simplified further for it to be more meaningful and useful. An equal number of survey respondents suggested making reports easier to understand. An overwhelming number of participants (70 percent), out of those who had a perspective on SOC for Cybersecurity report, suggested that there is lack of clarity on whether just the SOC2 report suffices since their view was that cybersecurity risks and cybersecurity risk management programs will have significant bearing on SOC2 report as well.

In terms of recommended actions, AICPA shall evaluate how to bring more clarity on SOC for Cybersecurity both in the user organizations and the service provider organizations.

LIMITATIONS AND FUTURE RESEARCH SUGGESTIONS

One of the limitations of this research was that a small percentage (5 percent) of the participants did not have any perspective on SOC for Cybersecurity. Another limiting factor is that there is very limited past research on SOC2 implementations and SOC2 effectiveness and almost no research on SOC for Cybersecurity. With the accelerating shift towards digital and increased reliance on cloud, systems reliability is one of the most important topics. More research can be conducted on how effective is SOC2 (and SOC for Cybersecurity) vis a vis actual systems availability and reliability as observed in the user organizations. The challenge with that would be the willingness of user organizations to share their actual availability and reliability data.

REFERENCES

Ambore, S., Richardson, C., Dogan, H., Apeh, E., & Osselton, D. (2017). A resilient cybersecurity framework for Mobile Financial Services (MFS). *Journal of Cyber Security Technology, 1*(3-4), 202–224. doi:10.1080/23742917.2017.1386483

American Institute of Certified Public Accountants (AICPA). (2017). SOC for Cybersecurity: Helping You Build Trust and Transparency. Durham, NC: AICPA. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-cybersecurity-brochure.pdf

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23*(3), 1177–1206. doi:10.1007/s11142-018-9452-4

Atoum, I., Otoom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security, 22*(3), 251–264. doi:10.1108/imcs-02-2013-0014

De Bruin, R., & von Solms, S. H. (2015). Modelling Cyber Security Governance Maturity. 2015 IEEE International Symposium on Technology and Society (ISTAS). doi:10.1109/istas.2015.7439415

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and Cybersecurity Risk Management. *Current Issues in Auditing*. doi:10.2308/ciia-52419

Fanning, K. (2014). Cloud Software: How to Validate Third-Party Vendors. *Journal of Corporate Accounting & Finance, 25*(5), 25–30. doi:10.1002/jcaf.21968

Gardikis, G., Tzoulas, K., Tripolitis, K., Bartzas, A., Costicoglou, S., Lioy, A., … Kourtis, A. (2017). SHIELD: A novel NFV-based cybersecurity framework. 2017 IEEE Conference on Network Softwarization (NetSoft). doi:10.1109/netsoft.2017.8004228

Giulio, C. D., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R., & Bashir, M. N. (2017). IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers. 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). doi:10.1109/ccgrid.2017.137

International Organization for Standardization. (2012). Information technology — Security techniques — Guidelines for cybersecurity (ISO/IEC 27032:2012).

International Organization for Standardization. (2013). Information technology — Security techniques — Code of practice for information security controls (ISO/IEC 27002:2013). https://www.iso.org/standard/54533.html

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. doi:10.1016/j.jcss.2014.02.005

Janvrin, D. J., & Wang, T. (2019). Implications of Cybersecurity on Accounting Information. *Journal of Information Systems, 33*(3), A1–A2. doi:10.2308/isys-10715

Kosub, T. (2015). Components and challenges of integrated cyber risk management. Zeitschrift Für Die Gesamte Versicherungswissenschaft, 104(5), 615–634. doi:10.1007/s12297-015-0316-8

Mylrea, M., Gourisetti, S. N. G., & Nicholls, A. (2017). An introduction to buildings cybersecurity framework. 2017 IEEE Symposium Series on Computational Intelligence (SSCI). doi:10.1109/ssci.2017.8285228

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. 2014 Information Security for South Africa. doi:10.1109/issa.2014.6950492

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). 2017 International Conference on Information Systems and Computer Science (INCISCOS). doi:10.1109/inciscos.2017.20

Sheldon, F. T., & Vishik, C. (2010). Moving Toward Trustworthy Systems: R&D Essentials. *Computer, 43*(9), 31–40. doi:10.1109/mc.2010.261

SOC 2®- SOC for Service Organizations: Trust Services Criteria. (n.d.). AICPA. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

SOC for Service Organizations: Information for Service Organizations. (n.d.). AICPA. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html

Susanto, H., Almunawar, M.N., Tuan, Y.C. (2012). Information security challenge and breaches: novelty approach on measuring iso 27001 readiness level. *Int. J. Eng. Technol. 2* (1), 67–75

Teodoro, N., Goncalves, L., & Serrao, C. (2015). NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements. 2015 IEEE Trustcom/BigDataSE/ISPA. doi:10.1109/trustcom.2015.402

23. Von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? Information and Computer Security, 26(1), 2–9. doi:10.1108/ics-04-2017-0025

Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. doi:10.1016/j.cose.2013.04.004

Whitman ME, Mattord HJ. Principles of information security. 4th ed. Course Technology, Cengage Learning; 2012

Yang, L., Lau, L. and Gan, H. (2020), "Investors' perceptions of the cybersecurity risk management reporting framework", *International Journal of Accounting & Information Management, 28(1)*, pp. 167-183. https://doi.org/10.1108/IJAIM-02-2019-0022