FEATURE

SOC Reports for Cloud Security and Privacy

Ashwin Chaudhary, CPA, CISA, CRISC, CISM, CGEIT, CCSK, CISSP, ITIL, PMP
Is the chief executive officer of Accedere Inc., a Certified Public Accountant (CPA) firm focusing on System and Organization Controls reporting, cloud data security and privacy. He can be reached at Ashwin.Chaudhary@accedere.io.

Cloud adoption has increased by leaps and bounds, adding to the already increasing types of cyberrisk. The costs of doing business in the digital age are rising. Cloud service abuse ranks among the greatest cybersecurity threats. To illustrate the potential magnitude of this threat, consider how a virtual machine (VM) could use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server.[1] A malicious hacker would not necessarily need to go to such lengths to pull off that sort of feat, though. If a multitenant cloud service database is not designed properly, a single flaw in one client's application could allow an attacker to get not just that client's data, but every other clients' data as well.

Data security and privacy are increasingly challenging in today's cloud-based environments. Providing independent third-party assurance, such as a System and Organization Controls (SOC) 2 report, helps address these concerns and helps cloud service providers (CSPs) stay ahead of the competition. This assurance also helps organizations mitigate data security and privacy risk.

Increasing Cloud Factor

Forbes indicates that "83% of enterprise workloads will be in the cloud by 2020."[2] With this cloud forecast, many CSPs are in for involvement in a large market. In 2017, there were 19,188 CSPs with US$134 billion in funding.[3]

"As cloud becomes increasingly mainstream through 2022, it will dominate ever-increasing portions of enterprise IT decisions."[4] This cloud shift represents both risk and opportunity. It has been predicted that public cloud services spending will reach US$370 billion in 2022.[5] **Figure 1** shows some finance-related cybersecurity trends.

Cloud Security Challenges

Cloud services can provide organizations, including federal agencies, with the opportunity to increase the flexibility, availability, resiliency and scalability of cloud services, which organizations can, in turn, use to increase security, privacy, efficiency, responsiveness, innovation and competitiveness. However, many organizations, especially those in regulated sectors such as finance and healthcare,

Figure 1—Cybersecurity Trends

Data security and privacy are increasing challenges in today's cloud-based environments.

The biggest financial consequence is lost business and customers:

- **US$6T** Approximate size of cybercrime market
- **US$158** Average cost per lost or stolen record
- **US$3M** Average cost of a data breach
- **3rd** Biggest risk of doing business

Based on information sourced from World Economic Forum.

“BECAUSE LAWS IN ONE LOCATION MAY CONFLICT WITH AN ORGANIZATION’S POLICIES OR MANDATES (E.G., LAWS OR REGULATIONS IN ANOTHER LOCATION), AN ORGANIZATION MAY DECIDE THAT IT NEEDS TO RESTRICT THE TYPE OF CLOUD SERVERS IT USES, BASED ON THE STATE OR COUNTRY.”

face additional security and privacy challenges when adopting cloud services.

Cloud platform hardware and software are evolving to take advantage of the latest hardware and software features, and there are hundreds or thousands of virtualized or containerized workloads that are spun up, scaled out, moved around and shut down at any instant, based on business requirements. In such environments, organizations want to be able to monitor, track, apply and enforce policies on the workloads, based on business requirements, in a consistent, repeatable and automated way.

In other words, organizations want to maintain consistent security protections and to have visibility and control for their workloads across on-premises private clouds and third-party hybrid/public clouds to meet their security and compliance requirements.

This is further complicated by organizations’ needs to comply with security and privacy laws applicable to the information that they collect, transmit or hold, which may change depending on whose information it is (e.g., European citizens’ information under the EU General Data Protection Regulation [GDPR]), what kind of information it is (e.g., health information compared to financial information), and in what state or country the information is located. Additionally, an organization must be able to meet its own policies by implementing appropriate controls dictated by its risk-based decisions about the necessary security and privacy of its information.

Because laws in one location may conflict with an organization’s policies or mandates (e.g., laws or regulations in another location), an organization may decide that it needs to restrict the type of cloud servers it uses, based on the state or country. Thus, the core impediments to broader adoption of cloud technologies are the abilities of an organization to protect its information and virtual assets in the cloud and to have sufficient visibility into that information to conduct oversight and ensure that the organization and its CSP are complying with applicable laws and business practices.

In addition, there are technical challenges and architectural decisions that must be made when connecting two disparate clouds. An important consideration revolves around the type of wide area network connecting the on-premises private cloud and the hybrid/public cloud, because it may impact the latency of the workloads and the security posture of the management plane across the two infrastructures.[6]

Misconfigured Cloud Servers

A major challenge to cloud security is misconfigured cloud servers. To save costs, organizations are moving to the cloud rapidly without proper security controls such as architecture design, access controls, vulnerability assessment or penetration testing.

Some leading reports indicate this trend.

> *In 2018, the media sector topped the chart with 40 percent of publicly disclosed incidents. Half of these incidents involved misconfigured cloud servers and other improperly configured systems that leaked data or allowed a remote attacker to exploit the asset.*[7]

“Attackers are targeting users of cloud services and misconfigured cloud servers are exposing customer and employee data.”[8] Organizations should check and monitor settings on cloud service architecture and not maintain default settings. Third-party cloud vendors should be vetted for high-security standards before choosing to do business with them. Organizations should always ensure awareness of who controls each component of the cloud infrastructure and define policies for where

and how security measures are deployed. The same security policies that would be employed for classic IT infrastructure should be implemented with CSPs.

Vendor (Third-Party) Risk

Managing third-party risk is an important aspect in the overall risk management process. Cloud providers are third parties that store or process valuable information.

> *From a cybersecurity perspective, third-party risks frequently involve a set of threats that may exceed the scope of the organization's risk management activities. Some organizations focus too narrowly on risks. For example, when hosting data in the cloud, most organizations ask the vendor for attestations or some evidence of cybersecurity capability.*[9]

> "THE SAME SECURITY POLICIES THAT WOULD BE EMPLOYED FOR CLASSIC IT INFRASTRUCTURE SHOULD BE IMPLEMENTED WITH CSPS."

IoT and Cloud

Connected devices and cyberphysical systems are becoming more prevalent in enterprise environments. As the cloud environment expands to encompass these technologies, the connected world depends on devices to manage, orchestrate and provision data. By 2023, the number of connected devices is forecast to reach 20 billion. This increase in volume is a growing challenge for service providers tasked with trying to keep their networks secure and for enterprises and critical infrastructure entities deploying and managing devices.

Insecure data flow from the edge to the cloud is a concern of the Internet of Things (IoT) model of data processing. Data processing can be done either at the edge or at the cloud. Edge computing provides a way to allow applications and services to gather or process data to the local computing devices, away

from centralized nodes, enabling analytics and knowledge generation to the logical extremes of the network. Although edge computing enhances instantaneous response and subsequent decision-making (e.g., use of machine learning [ML] to make autonomous decisions), it also results in a distributed, unsafe and uncontrollable disarray of data, which can become critical when taking into account the amount and the sensitivity of data that are transmitted. Limited processing and storage capabilities of some endpoints may restrict security features such as authentication, encryption and integrity protection mechanisms, jeopardizing both access control and the confidentiality or integrity of data transmitted to the cloud. Even when security features are enabled, faulty implementation can have a great impact on the security of the entire model.[10]

Distributed denial-of-service (DDoS) botnet attacks are another top IoT risk.

The Mirai botnet exploited a vulnerability in IoT devices to launch a DDoS attack against a critical Domain Name System (DNS) server that disrupted a number of the Internet's biggest websites, including PayPal, Spotify and Twitter.

According to the Open Web Application Security Project (OWASP), both aspects of security in this convergence are facing challenges from each other. Cloud web interface is listed as one of the attack surfaces of IoT, while some top security risk factors include service and data integration, which is linked to the security of IoT devices.[11]

> MANY ORGANIZATIONS ARE STORING SIGNIFICANT AMOUNTS OF DATA IN DISTRIBUTED AND HYBRID CLOUD AND EVEN UNMANAGED ENVIRONMENTS, INCREASING CHALLENGES FOR REGULATORY COMPLIANCE.

Security Responsibilities in the Cloud
At a high level, security responsibility maps to the degree of control any given actor has over the architecture stack.

The US National Institute of Standards and Technology (NIST) defines "cloud stack" as:

- **Software as a Service (SaaS)**—The CSP is responsible for nearly all security, because the cloud user can only access and manage their use of the application and cannot alter how the application works. For example, a SaaS provider is responsible for perimeter security, logging/monitoring/auditing and application security, while the consumer may be able only to manage authorization and entitlements.
- **Platform as a Service (PaaS)**—The CSP is responsible for the security of the platform, while the consumer is responsible for everything they implement on the platform, including how they configure any offered security features. The responsibilities are, thus, more evenly split. For example, when using a Database as a Service, the provider manages fundamental security, patching and core configuration, while the cloud user is responsible for everything else, including which security features of the database to use to manage accounts or even authentication methods.
- **Infrastructure as a Service (IaaS)**—Just like PaaS, the provider is responsible for foundational security, while the cloud user is responsible for everything he or she builds on the infrastructure. Unlike PaaS, this places far more responsibility on the client. For example, the IaaS provider will likely monitor its perimeter for attacks, but the consumer is fully responsible for how their virtual network security is designed and implemented based on the tools available on the service.[12]

Amazon's Shared Responsibility Model
Some SaaS providers believe that if they are hosting their application on Amazon Web Services (AWS), they are automatically compliant just because AWS may be. This may be applicable to other IaaS or PaaS providers. SaaS CSPs may also need to review the exact controls in the SOC reports and examine whether the relevant controls and criteria are covered in those SOC reports. Availability of an SOC report should not be just a checkbox for third-party (vendor) risk compliance.

This customer/AWS shared responsibility model[13] also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls. AWS can help relieve the customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that previously may have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS, which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required.

Data Governance in the Cloud
Governance issues also relate to regulatory compliance, security, privacy and similar concerns impacting today's organizations. Today's data management and storage landscape, where data entropy and data sprawl are rampant, has far-reaching consequences for data security.

Many organizations are storing significant amounts of data in distributed and hybrid cloud and even unmanaged environments, increasing challenges for regulatory compliance. A data inventory and data flow are often recommended. With increasing

IoT devices and data lakes in the cloud, the visibility and control are invariably lost, resulting in data sovereignty challenges. Disruptive technologies such as blockchain (distributed ledger) have emerged as candidates for financial institutions to reform their businesses. The speed and cost of doing business using distributed ledger technology are expected to improve by simplifying back-office operations and lowering the need for human intervention. However, a number of security concerns around this new technology remain.

Data Encryption and Anonymization

Privacy mandates such as the EU General Data Protection Regulation (GDPR) recommend data anonymization, which can be another form of encryption. Without a proper data governance program, organizations may face challenges in meeting these privacy compliance mandates. Data encryption is also mandated for the US Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

Cloud Assurance for CSPs

There are several approaches for CSPs to provide assurance to their customers that would provide them with confidence in using the CSP's services.

Cloud STAR Certification Roadmap

The Cloud Security Alliance (CSA),[14] in collaboration with the American Institute of CPAs (AICPA), developed a third-party assessment program of CSPs called the CSA Security Trust Assurance and Risk (STAR) Attestation. The STAR is the industry's most powerful program for security assurance in the cloud. STAR encompasses key principles of transparency, rigorous auditing and harmonization of standards. The STAR program provides multiple benefits, including indications of best practices and validation of the security posture of cloud offerings.

SOC 2 for Cloud CSA STAR Attestation

The SOC 2+ Framework allows an SOC 2 to report on any additional controls over and above the trust services criteria controls for security, availability, confidentiality, processing integrity and privacy.

Taking advantage of this framework, STAR Attestation provides a framework for Certified Public Accountants performing independent assessments of CSPs using SOC 2 engagements with the CSA's Cloud Controls Matrix (CCM).

Cloud Controls Matrix

The CCM is the only meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations. CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to cloud computing. CCM is currently considered a *de facto* standard for cloud security assurance and compliance.

Level 2 CSA STAR Attestation

The STAR Attestation is positioned as STAR Certification at Level 2 of the Open Certification Framework, and STAR Certification is a rigorous third-party independent assessment of the security of a cloud service provider (**figure 2**). STAR Attestation is based on type I or type II SOC attestations supplemented by the criteria in the CCM.

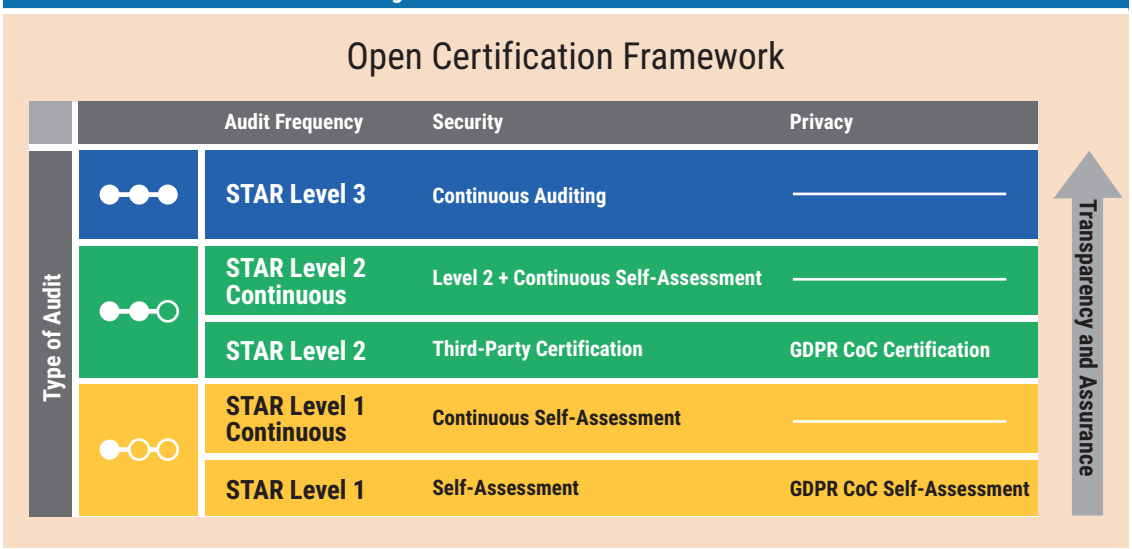
This assessment:

- Is based on a mature attestation standard
- Allows for the immediate adoption of the CCM as additional criteria and the flexibility to update the criteria as technology and market requirements change
- Does not require the use of any criteria that were not designed for or readily accepted by the CSP
- Provides for robust reporting on the service provider's description of its system and on the service provider's controls, including a description of the service auditor's tests of controls in a format very similar to the current SSAE 18 reporting, thereby facilitating market acceptance[15]

STAR Attestation builds on the key strengths of SOC 2 because it:

- Is a mature attest standard (it serves as the standard for SOC 2 and SOC 3 reporting)

Figure 2—STAR Certification Framework



- Provides for robust reporting on the service provider's description of its system and on the service provider's controls, including a description of the service auditor's tests of controls in a format very similar to the current SSAE 18 reporting, thereby facilitating market acceptance
- Provides evaluation over a period of time rather than a point in time
- Provides recognition with the AICPA logo

CSA Continuous Assessment (Level 2 and 3 Continuous)

STAR Level 2 Continuous builds on top of the STAR Level 2 requirement of third-party assessments and improves it by allowing the CSP to demonstrate a higher level of assurance and transparency with the addition of a continuous self-assessment.

In STAR Level 2, a CSP is assessed by a third party through one of the Level 2 programs against a determined and appropriate scope. The Level 2 programs, including STAR Certification, STAR Attestation and C-STAR, are based on varied but demanding cloud security criteria of the CSA CCM, the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27001 standards, or the AICPA Trust Services Criteria (TSC), applied toward the CSP's assessment scope.

Level 3 Continuous Certification is a highly selective cloud security assessment program, extending the assurance level of a cloud service beyond the trust given by the certification cycle of ISO/IEC 27001 and the audit period of AICPA SOC 2 type II reports.

STAR Level 3 Continuous requires all continuous assessments to be performed under the supervision of a third-party auditor. This differs from Level 2 Continuous, which requires a frequently submitted self-assessment on top of Level 2 by the CSP itself.

SOC 2 vs. ISO 27001/27017

Many CSPs may also have adopted ISO 27001/27017 for their cloud environment. How SOC compares to this standard is provided in **figure 3**.

C5 Cloud Controls

In February 2016, the Bundesamt fur Sicherheit Institute (BSI), or the German Federal Office for Information Security, established the Cloud Computing Compliance Controls Catalog (C5) certification after it noted the rise in cloud computing in Germany.[16] With the C5, the BSI redefined the bar that CSPs should meet when dealing with German data. The establishment of the C5 elevated the demands on CSPs by combining the existing security standards (including international certifications such as ISO 27001) and

Figure 3—Comparison of ISO 27001 and SOC 2 Type II Report

Area	ISO 27001/27017	SOC 2 Type II
Standard	International Standard ISO/IEC 27001, Second Edition 2013-10-01, ISMS—*Information security management systems*	Trust Services Principles and Criteria for Security, Availability, Process Integrity, Confidentiality and/or Privacy
Governing body	American National Standards Institute (ANSI) ANSI-ASQ National Accreditation Board (ANAB)	AICPA
Purpose	Assist organization's management in establishment and certification of ISMS that meets specified requirements and is able to be certified as best practice	Assist service organization's management in reporting to customers that it has met established security criteria that ensure that the system is protected against unauthorized access
Applicability	Statement of Applicability (SOA) of controls	System description by management
Certificate/reporting statement for controls	A point in time, i.e., as on a date	Period of time, i.e., for the period ended XXXX (date)
Objective	Establish, implement, maintain and improve the information security management system (ISMS)	Measure a service organization against specific security principles and criteria
Reporting cycle	Recertified every three years	Attestation provided every year (or six months)
Audit frequency	Surveillance audit conducted annually	Continuous monitoring during the period
Certified/attested by	ISO Accredited Registrar Certification	Attestation by a licensed CPA
Nature of testing	Design effectiveness	Design effectiveness and operating effectiveness
Controls in report	Details of controls not provided	Details of controls provided
Focus	Organization's ability to maintain an ISMS	Technology and the processes behind the applicable trust services criteria of the specific service
Report	Single-page certification	A report containing the auditor's opinion, management's assertion, description of controls, user control considerations, tests of controls and results
Difficulty to achieve	Moderate	Higher
Structure	Information security framework	Principles and criteria

requiring increased transparency in the data processing. C5 controls can be applied globally.

C5 is intended primarily for professional CSPs, their auditors and customers of the CSPs. The catalog is divided into 17 thematic sections (e.g., organization of information security, physical security). C5 makes use of recognized security standards, such as ISO 27001, the Cloud Controls Matrix of the CSA and BSI publications, and it uses these requirements wherever appropriate.

A SOC 2 report proves that a CSP complies with the requirements of the catalog and that the statements made on transparency are correct. This report is based on the internationally recognized

> IN VIEW OF THE RECENT INCIDENTS AND FAILURE OF THE EU SAFE HARBOR AND THE PRIVACY SHIELD, PRIVACY LAWS ARE NOW CHANGING AND MAY BECOME MORE STRINGENT.

attestation system of the International Standard for Assurance Engagements (ISAE) 3000, which is used by public auditors. When auditing the annual financial statements, the auditors are already onsite, and auditing according to C5 can be performed without much additional effort.

Privacy Compliance for Cloud

Privacy has grabbed the attention of boards of directors (BoDs) as regions look to implement privacy regulation and compliance standards similar to GDPR. Privacy is the new buzzword, and the potential impact is very real. Personal data are processed for political and economic reasons without users' consent, as happened in the Cambridge Analytica event.[17] In view of the recent incidents and failure of the EU Safe Harbor and the Privacy Shield, privacy laws are now changing and may become more stringent. After GDPR, new privacy laws are being enacted such as the US California Consumer Privacy Act (CCPA), US New York Privacy Act (NYPA) and the Brazilian General Data Protection Law. It may be prudent for organizations to be more proactive and adopt measures for privacy governance.

To demonstrate privacy-related controls, organizations can include the privacy criteria as part of the scope of their SOC 2 report.[18] Additionally, controls for any other specific laws can be included as additional subject matter. The following describes the AICPA Privacy Criteria broad requirements. Many of these requirements match to legislation such as GDPR. In the wake of new privacy mandates, organizations are encouraged not only to include privacy criteria in their SOC 2 report, but also to demand including them in their vendors' SOC 2 report to mitigate risk.

SOC 2 Description for Privacy

A SOC 2 report contains a description of services that the service provider provides. When the description includes privacy, service organization management discloses the service commitments and system requirements identified in the service organization's privacy notice or in its privacy policy that are relevant to the system being described.

When making such disclosures, it may also be helpful to report users if service organization management describes the purposes, uses and disclosures of personal information permitted by user entity agreements.

Principal System Requirements

System requirements are the specifications about how the system should function to do the following:

- Meet the service organization's service commitments to user entities and others (such as user entities' customers)
- Meet the service organization's commitments to vendors and business partners
- Comply with relevant laws, regulations and guidelines of industry groups, such as business or trade associations
- Achieve other objectives of the service organization that are relevant to the trust services categories addressed by the description

Requirements are often specified in the service organization's system policies and procedures, system design documentation, contracts with customers, and government regulations.

The following are examples of system requirements:

- Workforce member fingerprinting and background checks established in government banking regulations
- System edits that restrict the values accepted for system input, which are defined in application design documents
- Maximum acceptable intervals between periodic review of workforce member logical access as documented in the security policy manual

- Data definition and tagging standards, including any associated metadata requirements, established by industry groups or other bodies, such as the Simple Object Access Protocol (SOAP)
- Business processing rules and standards established by regulators (e.g., security requirements under HIPAA)

Data

Disclosures about the data component include types of data used by the system, transaction streams, files, databases, tables, and outputs used or processed by the system. When the description addresses the confidentiality or privacy categories, other matters that may be considered for disclosure about the data component include the following:

- The principal types of data created, collected, processed, transmitted, used or stored by the service organization and the methods used to collect, retain, disclose, dispose of or anonymize the data
- Personal information that warrants security, data protection or breach disclosures based on laws or commitments (e.g., personally identifiable information [PII], protected health information [PHI], payment card data)
- Third-party entity information (e.g., information subject to confidentiality requirements in contracts) that warrants security, data protection or breach disclosures based on laws or commitments

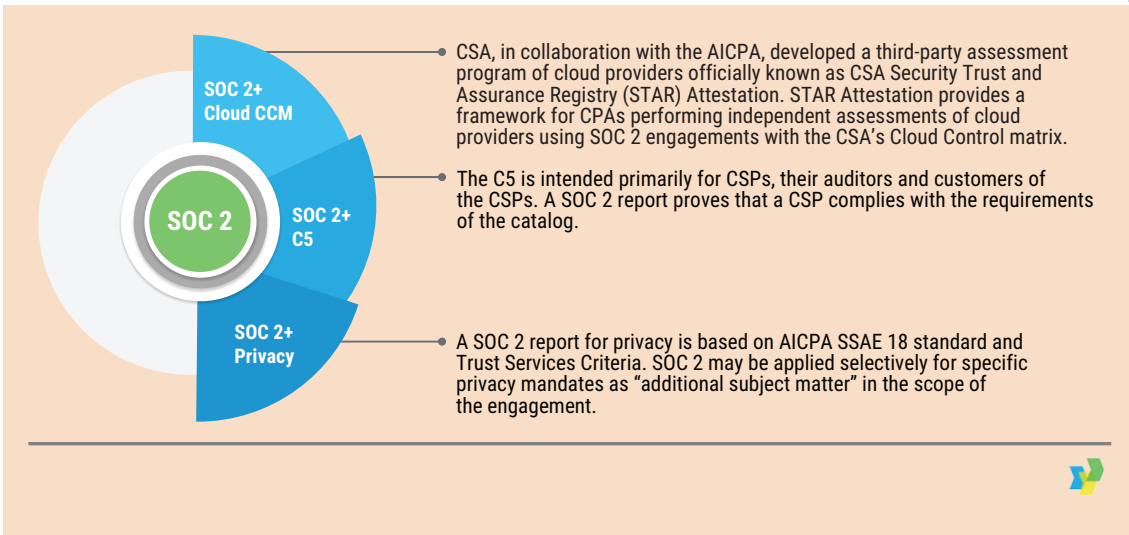
> “REQUIREMENTS ARE OFTEN SPECIFIED IN THE SERVICE ORGANIZATION’S SYSTEM POLICIES AND PROCEDURES, SYSTEM DESIGN DOCUMENTATION, CONTRACTS WITH CUSTOMERS, AND GOVERNMENT REGULATIONS.”

AICPA Trust Services Criteria (TSC) for Privacy

With approximately 50 points of focus, the TSC organizes the privacy criteria as(**figure 4**):[19]

- **Notice and communication of objectives**—The entity provides notice to data subjects about its objectives related to privacy.
- **Choice and consent**—The entity communicates choices available regarding the collection, use, retention, disclosure and disposal of personal information to data subjects.
- **Collection**—The entity collects personal information to meet its objectives related to privacy.
- **Use, retention and disposal**—The entity limits the use, retention and disposal of personal information to meet its objectives related to privacy.

Figure 4—SOC 2 With Cloud and Privacy Controls



> IT MAY BE IMPORTANT FOR ORGANIZATIONS TO REVISIT THEIR EXISTING RISK MITIGATION STRATEGIES AND ADOPT METHODS THAT MAY BETTER ALIGN WITH TECHNOLOGICAL CHANGES AND CURRENT LAWS.

- **Access**—The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.
- **Disclosure and notification**—The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators and others to meet its objectives related to privacy.
- **Quality**—The entity collects and maintains accurate, up-to-date, complete and relevant personal information to meet its objectives related to privacy.
- **Monitoring and enforcement**—The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints and disputes.

Cloud Security and Privacy for User Organizations

To protect data in the cloud and to maintain continuity of services, cloud users, at a minimum, should consider implementing the following controls. Implementing these controls should help the organization stay compliant with the laws of the land and manage the risk:

- Include cloud security and privacy risk as part of the risk management life cycle.
- Create a secure architecture using the concept of security by design.
- Document the data flow and implement data security controls.
- Implement and review role-based access controls (RBAC).
- Perform vulnerability assessment (VA)/penetration testing of the cloud applications and environment.
- Evaluate SOC reports with relevant controls of the CSPs.
- Implement secure access methodology, e.g., Transport Layer Security (TLS), multifactor authentication (MFA).
- Implement resiliency controls.
- Follow a Deming Cycle approach to cloud security and privacy.
- Perform periodic internal audits of the hybrid environment using SOC reports for cyberrisk.

Conclusion

In view of the current threat landscape, specifically relating to cloud adoption and the challenges discussed previously, it may be important for organizations to revisit their existing risk mitigation strategies and adopt methods that may better align with technological changes and current laws.

Data governance and privacy programs that align with organizational goals can help define and advance the maturity road map. Continuous monitoring and assurance programs can address weaknesses and provide better visibility to the organization's stakeholders.

Endnotes

1 Bartunek Group, "Nine Top Threats to Cloud Computing Security," 26 February 2013, *https://bartunekgroup.com/9-top-threats-to-cloud-computing-security/*
2 Columbus, L.; "83% of Enterprise Workloads Will Be in the Cloud by 2020," *Forbes*, 7 January 2018, *https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#22fc3beb6261*
3 Crozdesk, "SaaS and Cloud Startup Report 2018," 20 November 2017, *https://crozdesk.com/software-research/saas-and-cloud-startup-report-2018*

4 Liu, S.; "Public Cloud Software-as-a-Service (SaaS) Revenue Worldwide From 2016 to 2027 (in Billion U.S. Dollars)," Statista, 6 December 2018, *https://www.statista.com/statistics/477742/public-cloud-software-revenue-forecast/*

5 IDC, "Worldwide Public Cloud Service Spending Forecast to Reach $210 Billion This Year, According to IDC," 28 February 2019, *https://www.idc.com/getdoc.jsp?containerId=prUS44891519*

6 National Institute of Standards and Technology, "Trusted Cloud," Special Publication (SP) 1800-19B, USA, November 2018, *https://www.nccoe.nist.gov/sites/default/files/library/sp1800/tc-hybrid-nist-sp1800-19b-preliminary-draft.pdf*

7 IBM Security, *X-Force Threat Intelligence Index 2019*, February 2019, *https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf*

8 Cloud Security Alliance, "Top Threats to Cloud Computing: The Egregious 11," 2019, *https://cloudsecurityalliance.org/download/artifacts/top-threats-to-cloud-computing-egregious-eleven/*

9 Haller, J.; C. Wallen; "Managing Third Party Risk in Financial Services Organizations: A Resilience-Based Approach," Carnegie Mellon University, Pittsburgh, Pennsylvania, USA, September 2016, *https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_473742.pdf*

10 Open Web Application Security Project, "OWASP Internet of Things Project," *https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project*

11 *Ibid*.

12 Cloud Security Alliance, "Security Guidance: For Critical Areas of Focus in Cloud Computing v4.0," 2017, *https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf*

13 Amazon Web Services, "Shared Responsibility Model," *https://aws.amazon.com/compliance/shared-responsibility-model/*

14 Cloud Security Alliance, *https://cloudsecurityalliance.org/*

15 Cloud Security Alliance, "CSA Security Trust Assurance and Risk (STAR)," *https://cloudsecurityalliance.org/star/*

16 Federal Office for Information Security, "Compliance Controls Catalogue (C5)," Germany, *https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html*

17 *Wired*, "The Cambridge Analytica Story, Explained," *https://www.wired.com/amp-stories/cambridge-analytica-explainer/*

18 American Institute of Certified Public Accountants, "System and Organization Controls: SOC Suite of Services," *https://www.aicpa.org/soc*

19 American Institute of Certified Public Accountants, "Trust Services Criteria," 2017, *https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf*