AUGUST 2019

In recent times, there have been some changes in the SOC 2 criteria which resulted in the addition, updating and removal of certain criteria and so we wanted to send out a reminder across our network about these changes. This newsletter includes the additive criteria. In addition, we have included in this newsletter examples of controls (below in table format) we believe a company would minimally be required to have in place to meet the current criteria (including those associated with the additive criteria). Please read the below and reach out to myself or your Assure contact with questions.

Why the change?

The AICPA updated the Trust Services Categories (TSC) (formerly Principles) in order to more closely align with the "Committee of Sponsoring Organizations of the Treadway Commissions Internal Control – Integrated Framework" (COSO Framework). This framework was created to provide further guidance and clarifications that represent a changing environment since the last update in 2007. One of the major updates was the creation of Points of Focus which were designed to aid with the implementation of the COSO Framework. Additionally, the updated COSO Framework includes an appendix that provides guidance specifically addressing smaller entities.

What's Changed?

During the update of the TSC and individual criteria, the AICPA updated, removed and added certain criteria to the categories. Each individual criterion now contains the Points of Focus. There can be numerous Points of Focus that provide information on how organizations can implement controls in order to meet the criteria. Some of these Points of Focus may not be relevant to every entity. The updated TSC does not require that each Point of Focus be specifically addressed.

What hasn't changed?

The Trust Services Categories themselves haven't changed – Security (required), Availability, Confidentiality, Processing Integrity, and Privacy. Depending on the services provided, how those services are provided, the business environment, and customer requirements, organizations should include each TSC relevant to these factors.

Service Commitments

The updated TSC has placed a larger importance on the organization's service commitments. These commitments are typically found in customer contracts, service level agreements, the organization's website, or other source. These service commitments can include system "uptime" commitments, encryption standards, processing timelines, accuracy of data, or many others.

How to ensure you meet the new TSC?

For those organizations with a SOC report, an internal assessment of the last SOC report compared to the required controls and new TSC should be completed. This assessment will identify any gaps that management can use in order to evaluate and implement new controls as considered necessary. It should be noted that most of our clients likely already have existing controls meeting the new criteria. Nonetheless, as in every new audit year, we recommend clients perform an internal assessment of their environment.

New Criteria:

The below table details the new criteria created with the updated TSC along with additional information explaining the criteria as well as some implementation tips:

	CONTROL ENVIRONMENT	*ADDITIONAL INFORMATION*	*PRACTICAL IMPLENTATION GUIDANCE*
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	This criterion establishes oversight and responsibility to an *independent* group of individuals separate from management. This provides the entity with an unbiased review of the organization and decision making.	Not all organizations have a board of directors. Additionally, some board of directors may not be independent from management. In these examples, the organization may have a reasonable basis to exclude this criterion.
	COMMUNICATION AND INFORMATION		
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Gathering information and communicating the information to stakeholders is essential to effectively supporting internal controls. Relevant information may come from internal or external sources.	This criterion can be met utilizing a number of controls including network monitoring, security event logs, incident response policies and procedures. Many of these controls are standard across most organizations so this criterion may already be met.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Creating communication lines is essential to taking the information in CC2.1 to stakeholders.	Properly communicating responsibilities through policies and procedures, training, well-defined job descriptions, delegating security and maintenance planning, as well as standard operating procedures can assist with meeting the criteria and COSO principle.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	This principle requires assistance from outside parties in order to be met.	Communication with external parties could include user requirements for incident notification in order to identify potential issues, documented support operations that give users of the system the ability to obtain or give relevant information, as well as SLA's which document the overall responsibilities of the two parties.

	RISK ASSESSMENT	*ADDITIONAL INFORMATION*	*PRACTICAL IMPLENTATION GUIDANCE*
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	While the old and updated version of the TSC both lay out requirements for risk, the updated COSO principle modifies this requirement by not only identifying risks but also creating a program designed to guide users on how the risk assessment should be performed.	A properly created and maintained risk management program needs to be in place in order to meet this criterion. As the implementation guidance points out, the criteria here requires more than just a risk assessment but a policy which addresses how the risk assessment should be completed.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes can come from numerous places such as changes in external environments, business operations, products and services, leadership, technology, etc. These changes must be taken into account when evaluating an effective internal control environment.	A periodic review of policies and procedures could identify a change that occurred which requires a change in the control environment. Change logging such as application development, infrastructure changes, and others may also create the need to update the controls. Changes in security updates such as anti-virus and patches could also play a role in properly assessing changes.
	CONTROL ACTIVITIES		
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Policies and Procedures are essential to a properly implemented internal control environment and activities. These documents lay the foundation for how the control activities should be implemented, follows, and reviewed.	For example, policies should cover general Information Security, Human Resources, Incident Response, Application Development (if applicable), Data Classification and Retention and Disposal.

	System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Unidentified changes to configurations could result from vulnerabilities that are not addressed timely. These changes need to be captured and evaluated as they occur.	Network monitoring could be the primary tool used in identifying changes. Standard configuration standards and alerts for when those standards have changed are another method to detect and monitor for changes. Vulnerability assessments or scans should be performed periodically to detect potential vulnerabilities within the system. These assessments or scans may be conducting internally or utilizing a third party.
	Risk Mitigation	***ADDITIONAL INFORMATION***	***PRACTICAL IMPLENTATION GUIDANCE***
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	During the risk assessment or through a Disaster Recovery Policy creation or review, the organization must identify the potential sources for business interruptions and properly address those interruptions. Different responses are required depending on the nature of the interruption. Natural disasters or malicious attempts to disrupt the operations may require different procedures to continue processing or providing services.	The first step in mitigating risk is to identify what the risks are. Therefore, a thorough risk assessment must be conducted. From this risk assessment, management can consider the possible responses. Disaster Recovery or Business Continuity Plans must be in place to mitigate the risks associated with various outages or interruptions. Additionally, management may consider the acceptance or transfer of risk by obtaining appropriate insurance policies which can financially protect the organization.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Vendors and business partners may play a critical role in your control environment. This could be hosting operations of your application or data, providing customer support, application development or other services you rely upon to adequately provide your products or services to customers.	Assessing key vendors and business partners is important to determining risks associated with those provided services. These assessments could be completed during the overall organizational risk assessment.

	ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY		
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	Properly defining the products and services along with the expectations of the processing objectives is critical to ensuring the products or services are delivered as required within an SLA, website declarations, sales information, or other documents which communicates how and when the products and services will be delivered.	If Processing Integrity is being included in your report, the individual products and services will need to be evaluated in order to determine what the specific requirements are. This can be done internally or by performing a walkthrough by the auditor.

Control Examples

The below table contains examples of controls required to be in place in order to achieve the updated SOC 2 criteria. It is our opinion that these controls or the equivalent will need to be included to achieve an unqualified ("clean") audit opinion. In order to achieve the updated criteria, Companies should evaluate their control environment against the below while paying particular attention to the new criteria. Assure is happy to have a discussion surrounding these items.

Assure ID	Criteria Met	Item Name	Control	Notes
01.01	CC5.3	Information Security Policy	The Company has an Information Security Policy that describes the security posture and practices of the Company	Numerous templates are available online. Assure also has several templates which can help you create this document.
01.02	CC1.3	Organization Chart	Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. Responsibility for Security, Availability, Processing Integrity, Confidentiality and Privacy has been delegated.	This is key to providing appropriate lines of communication and a hierarchy which can show proper segregation of duties.
01.04	CC1.4; CC1.5	Employee Manual or Handbook	The Company has an employee handbook that describes management's philosophy, operating style, and provides HR policy guidance to employees.	This is important to communicate the requirements expected of employees as well as managements "tone at the top."
01.05	CC1.1	Ethics Policy or Code of Conduct	The Company has a code of conduct or ethics policy that guides employees on the Company's principles and conduct.	This item may be included in the employee handbook or in a separate policy.
01.07	CC1.3; CC2.2; CC7.4	Job Descriptions	The Company has documented job descriptions that describe the roles and responsibilities of the position.	Job descriptions should be in place for all key positions and may be included for other positions as well. A common source for creating a job description is the ad that is used when trying to hire a new employee.
01.08	CC4.1	Management Meetings	Management meetings are held on a regular basis to discuss operational issues.	These meetings should be on a set frequency with minutes maintained in order to provide evidence to the auditor.

Assure ID	Criteria Met	Item Name	Control	Notes
01.09	CC9.1	Insurance Policies	The Company maintains insurance policies to mitigate losses and transfer certain identified risks.	Insurance policies are important for several reasons such as providing funding in order to resume operations in the event of an interruption. This can also help to transfer risks associated with operating in a specific industry.
01.10	CC3.1	Risk Management Program	The Company has a risk management program to address security and business-related risks.	A risk management program lays out how the risk assessment should be performed, the timing, the individuals, and other information needed to conduct a proper risk assessment.
01.11	CC3.2; CC3.3; A1.2	Risk Management Meetings	Risk Committee meetings are held periodically to monitor the controls of the company.	Management or independent individuals should meet on a regular basis to review the risk program and risk assessment. This meeting should be formally documented with meeting minutes in order to provide evidence to the auditor.
01.44	CC3.2; CC3.3; CC9.2	Risk Evaluation Completed	The Company completes a risk assessment and updates the list of identified risks periodically.	The risk assessment must include an assessment of fraud such as fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur, whether internal or external.
01.25	CC1.2	Board of Directors	A Board of Directors is in place to provide governance on Company directions and operations.	If no *independent* board of directors, this criteria may be excluded
02.03	CC6.2; CC6.3	Hiring Checklist	New hire checklists are used to ensure new staff receive the appropriate level of access to information systems and facilities.	This must include giving the appropriate level of access. It may include a listing of assets, codes, and keys to the employee. It cannot solely include the collection of

Assure ID	Criteria Met	Item Name	Control	Notes
				typical HR files such as W4s, I9s, identification, etc.
02.07	C1.1	Confidentiality or Non-Disclosure Agreement (NDA) Used	Confidentiality agreement must be in place with employees to ensure proprietary or confidential information is not disclosed to unauthorized parties.	This may be included in the employee handbook.
02.08	CC1.1; CC1.5	Employee Evaluations	Employee evaluations are performed on a regular basis against individual objectives derived from the Company's goals, established standards, and specific job responsibilities.	Employee evaluations should be utilized to communicate areas of excellence as well as areas of improvement. These evaluations should be conducted on a set frequency and also should be formally documented in order to provide evidence to the auditor.
02.10	CC1.5	Disciplinary Process	There is a formal discipline policy for employees who are suspected of rule infractions or violations of company policies.	This may be included in the employee handbook or could be in a separate policy.
02.11	CC6.2; CC6.3	Termination Checklist	Management utilizes and retains termination checklists as confirmation of the revocation of system and facility access privileges as a component of the employee termination process.	Must include termination of access rights and return of company assets such as computers, keys, etc.
07.01	CC7.5	Backup and Recovery Policy	Management maintains documented backup schedules, policies, and procedures.	Documented backup policies are integral in order to set the standard by which backups are conducted.
07.08	A1.3	Restore testing	Restores from backups can be performed to verify that system components can be recovered from backup media.	Data integrity checks upon backup may be a substitute for this control.

Assure ID	Criteria Met	Item Name	Control	Notes
08.01	A1.1	Network and System Monitoring	A monitoring application is utilized to monitor network devices and critical systems.	Network monitoring is a good line of defense to detect unauthorized changes as well as required changes in the case of increased capacity or other requirement.
08.04	CC4.2; CC7.2; CC7.4	Incident Response Policy and Procedures	The Company has a Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches.	A well documented security incident response plan will make the company more agile in the instance of an attack or security breach.
08.30	CC7.3	Incident Response Collection of evidence	The Incident Response Procedures documents the required procedures for evidence collection.	
08.08	CC5.2	Antivirus Protection	Antivirus software scans production servers on a real-time basis.	Antivirus software is a good line of defense in order to mitigate common or newly identified vulnerabilities.
08.09	CC5.2; CC6.8	Antivirus updated daily	Antivirus software is configured to automatically update servers and personal computers on a daily basis.	In order to ensure the organization has addressed common or newly identified vulnerabilities, the antivirus software must have the most recent virus definition library.
09.01	CC6.1	Account Management and Password Policy	Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards.	This policy is the baseline requirement for establishing minimum standards when accessing the network, applications, or other systems.
09.03	CC6.1	Password Complexity Settings	Passwords must conform to minimum requirements as enforced by the network operating system. Password complexity standards are established to enforce control over access control software passwords.	Minimum requirements in password settings should be implemented in order to mitigate attacks from easily-guessed passwords or programs designed to gain access utilizing inadequate passwords.

Assure ID	Criteria Met	Item Name	Control	Notes
09.04	CC2.1; CC7.2	Security Event Logging	Network security event logging is configured to log specific events on the network domain.	Logging events on the network should be in place in order to identify and correct any anomalies or potential attacks. These logs should be reviewed or alerts should be setup to alert individuals responsible for network security.
09.05	CC6.1	Administrative Access Controlled	Network domain administrator rights are restricted to specific network operations personnel.	Administrators have a large amount of access and authority to make changes. By allowing unqualified individuals or those that don't require access, harmful changes could be made or malicious acts could be introduced whether intentionally or unintentionally.
09.06	CC6.1; CC6.3	Security Groups Used	Security groups have been configured and are enforced by the network operating system and servers to ensure access is restricted to sensitive data stored on the network.	Similar to administrator rights being restricted, layers of separation among employees and others who have access to the network should be in place. This segregation should be based upon the principle of least privilege.
09.10	CC6.2; CC6.3	Termination Procedures	Termination procedures are in place for the removal of access to all systems upon notification of the termination.	Prompt removal of access rights is critical when an employee is terminated. Depending on the circumstances of their exit, an employee may wish to do harm to the organization. This limits that person’s ability.
1.52	CC9.2	Vendor Risk Management	The entity assesses the risks that vendors and business partners will fail to meet the entity’s requirements.	Assessing key vendors should be done periodically to ensure they are meeting organizational requirements. This could be included with the risk assessment 1.44 above

Assure ID	Criteria Met	Item Name	Control	Notes
10.01	CC5.1	Firewall Utilized	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	Firewalls provide a great level of defense against certain attacks. These should be in place at all organizations.
10.03	CC5.1	Controlled Administrative Access: Communication Devices	Management restricts the ability to administer the firewall systems and network communications equipment to certain personnel.	Firewalls should only be managed by those with knowledge with the equipment being deployed. Therefore, only those individuals should be granted access.
12.01	CC7.5	Disaster Recovery Plan (DRP) Documented	Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations.	Disaster Recovery or Business Continuity Plans should be in place. A well-defined policy will define responsibilities and outline steps in order to resume operations.
12.03	CC7.5; A1.3	DRP Testing	Certain aspects of the disaster recovery plan are tested on an annual basis.	Once a documented plan is in place, tests should be performed periodically in order to ensure the plan is operable. These could include simple tabletop exercises or full transfer of data to backup or offsite facilities.
13.01	C1.1	Data Classification Policy	Policies and procedures are in place to guide personnel on their responsibility for the classification of data and documents.	Classifying data is the first step in determining the different levels of protection over the data. This policy should be well-defined in categorizing the potential sources of information.
13.04	CC6.5	Data Destruction Procedures	Documented procedures are in place to ensure all media are physically destroyed rendering all sensitive information unreadable before being discarded or recycled.	Depending on the organization or client requirements, documents, media, physical equipment, and other items should be disposed of properly in a manner which is appropriate for the given format.