Compliance Report

Project: Project

Company: Tenant
Date: 14 June, 2023
Framework: Soc2

Table of contents

Overview

- Project Metrics 4
- Control Status 5

Project Metrics

The following page displays a quick overview of your compliance project along with key metrics.

Completion Progress

The project is 0.0% complete

Implemented

The project has implemented 0.0% of controls

Evidence

The project is 0.33% complete with evidence collection

Total Controls

The project has a total of 61 controls

Total Policies

The project has a total of 25 policies

Control Status

The table below displays the completion status of each applicable control within your project. Typically a control is considered complete if it is 100% implemented and has evidence attached. However each framework may have other requirements that are not represented in the table.

ID	Name	Status
514	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	0%
515	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	0%
516	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	0%
517	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	0%
518	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	0%
519	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	0%
520	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	0%
521	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	0%
522	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	0%

ID	Name	Status
523	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	0%
524	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	0%
525	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	0%
526	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	0%
527	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	0%
528	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	0%
529	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	0%
530	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	0%
531	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	0%
532	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	0%
533		0%

ID	Name	Status
	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
534	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	0%
535	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	0%
536	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	0%
537	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	0%
538	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	0%
539	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.	0%
540	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	0%
541	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	0%

ID	Name	Status
542	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	0%
543	The entity identifies, develops, and implements activities to recover from identified security incidents.	0%
544	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	0%
545	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	0%
546	The entity assesses and manages risks associated with vendors and business partners.	0%
547	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	0%
548	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	0%
549	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	0%
550	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	0%
551	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	0%
552	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.	0%
553		0%

ID	Name	Status
	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	
554	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	0%
555	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	0%
556	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	0%
557	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	0%
558	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	0%
559	Personal information is collected consistent with the entity's objectives related to privacy.	0%
560	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.	0%

ID	Name	Status
561	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	0%
562	The entity retains personal information consistent with the entity's objectives related to privacy.	0%
563	The entity securely disposes of personal information to meet the entity's objectives related to privacy.	0%
564	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	0%
565	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	0%
566	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	0%
567	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	0%
568	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	0%
569	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	0%

ID	Name	Status
570	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	0%
571	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	0%
572	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	0%
573	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	0%
574	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	0%