Compliance Report

Project: Demo

Company: Acme
Date: 02 May, 2023
Framework: Soc2

Contact: bmarshall735@gmail.com
Generated by: Gapps

Table of contents

Overview

Project Metrics

The following page displays a quick overview of your compliance project along with key metrics. For more information, please view the project within the console.

Completion Progress

The project is 3.79% complete

Implemented

The project has implemented 5.08% of controls

Evidence

The project is 5.76% complete with evidence collection

Total Controls

The project has a total of 33 controls

Total Policies

The project has a total of 1 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. Please view the project in the console for more details.

ID	Name	Status
1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	0%
2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	25.0%
3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	0%
4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	0%
5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	0%
6	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	100.0%
7	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	0%
8	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	0%
9	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
10	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%
11	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	0%
12	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	0%
13	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%
14	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%
15	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%
16	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	0%
17	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	0%
18	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%
19	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%
20		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.	
21	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%
22	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%
23	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	0%
24	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%
25	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%
26	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%
27	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%
28	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
29	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%
30	The entity identifies, develops, and implements activities to recover from identified security incidents.	0%
31	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%
32	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	0%
33	The entity assesses and manages risks associated with vendors and business partners.	0%