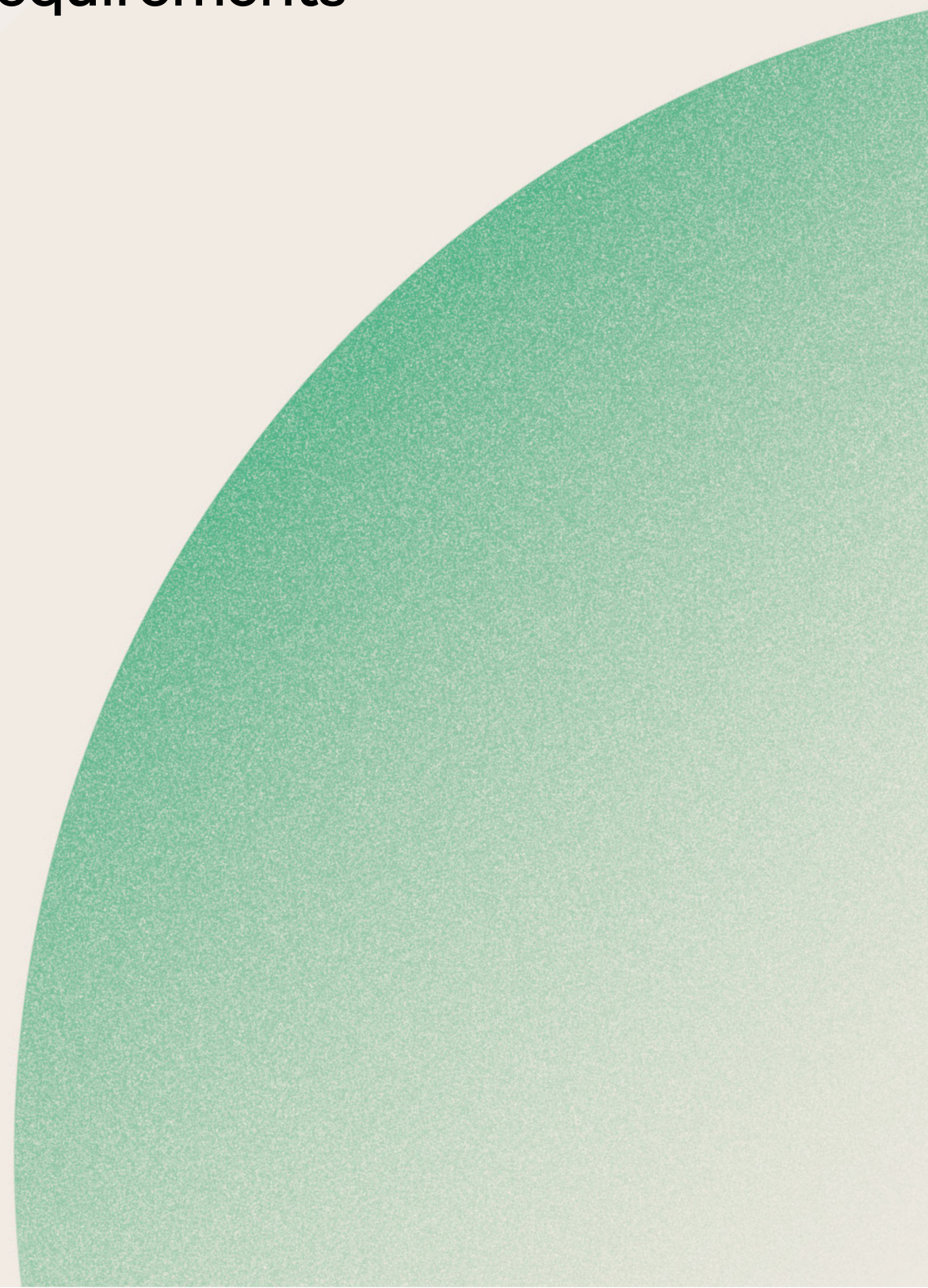
Island

Implementing SOC2 Requirements

Aug 2023



Introduction

SOC2 is a compliance standard developed by the American Institute of CPAs (AICPA) for technology service or SaaS companies that store customer data in the cloud. It is a voluntary standard that aims to ensure that organizations continue to mitigate the risk of data exposure.
SOC2 outlines a set of principles that aims to ensure the safety and privacy of customers' data, compliance with regulations, and the implementation of risk mitigation processes. SOC2 is not a prescriptive list of controls, tools, or processes, but rather a set of criteria required to maintain robust information security. Each company can adopt the practices and processes relevant to their own objectives and operations.

> **The five key categories of SOC2 are: Security, Availability, Process Integrity, Confidentiality, and Privacy**

In order to achieve SOC2 compliance (via an attestation report), an organization must undertake a rigorous process of defining and establishing policies, enforcing them, and providing evidence of their implementation.

How Island can help organizations implement their SOC2 requirements

Every company defines the practices and processes relevant to its domain and particular service offerings. Companies using Island, the Enterprise Browser, throughout their organization, can utilize it to meet the relevant SOC2 controls, ensure the procedures defined as part of the SOC2 process are followed, and present the required evidence to support the SOC2 audit stage.
For instance, the Islandplatform can assist organizations by:

- **Defining granular policies** that control access to sensitive organizational resources
- **Providing full auditing** on usage of organizational web applications
- **Safeguarding the confidentiality** of sensitive information using Island capabilities such as DLP, data masking, screen protection, etc.
- **Enforcing IT endpoint controls set** by the organization, like disk encryption and an active Endpoint Protection Platform
- **Creating a secure workspace** organizations can rely on, especially for sensitive applications and data

Island use cases

This document outlines specific use cases and demonstrates how Island can assist organizations throughout their SOC2 process.

Security Controls

Security is the only category that is mandatory as part of the SOC2 process. It comprises a total of nine common criteria.

Control Environment (CC1)

While the Control Environment criteria mostly deals with company wide controls such as a defined employee training, code of conduct and a clear organizational hierarchy, Island can assist in meeting parts of this criteria by:

- **Prompting employees** to read and acknowledge organizational policies such as a code of conduct, security controls and others and audit their response
- **Providing an easy way** for employees to access their technical training materials from their browser homepage and auditing their online training sessions

Communication and Information (CC2)

As part of this criteria, organizations are required to identify key information from internal and external sources that will allow them to meet their objectives. Companies using the Island browser to protect and monitor usage of critical web applications by their employees, gain unparalleled visibility and insight into such application usage and can derive key metrics from them. Such metrics can include usage patterns and tracking of key operations in applications like Salesforce and other CRM tools, as well as the use of Point-of-Sale apps.

Risk Assessment (CC3)

The CC3 controls are mainly focused on either Financial or Technological risks. A key part of this criteria deals with the organization's risk assessment process, gaining visibility to potential risks and mitigating them. Using Island can help organizations by:

- **Monitoring sensitive applications** for appropriate access and use
- **Securing confidential information** from unauthorized personnel by defining granular access control within specific applications
- **Reducing possible exposure** of sensitive data by applying last mile controls such as download control, blocking copy and screenshot operations as well as leveraging Island's DLP capabilities
- **Reducing employee exposure** to sensitive information by applying data masking
- **Collecting detailed activity logs** for all actions within sensitive web applications, and making end-users aware that their activities are being monitored
- **Reducing the risk of passwords being exposed** by using the integrated Island Password Manager, designed with a zero knowledge architecture

Monitoring Activities (CC4)

Monitoring Activities Controls are designed to ensure that the company has established proactive and reactive monitors on its systems. To optimize monitoring activities control, it is recommended not to rely on one monitoring system only.
Here is how Island can help:

- **Real-time device posture monitoring**, including having an active Endpoint Protection Platform (EPP), enabling disk encryption, having an up-to-date OS version and browser version
- **Activity monitoring on user actions** within applications, including screenshots for key actions and a timeline view of all activity
- **Providing easy access to monitoring** reports through the Island Management Console
- **SIEM integration** for data consolidation between various monitoring systems

Control Activities (CC5)

Control activities are designed to enforce policies related to risk mitigation, relying on the monitoring activities already defined. With most sensitive applications being accessed through the browser, an organization can utilize Island's granular last mile controls for:

- **Blocking or allowing application access** based on a policy, taking into account various risk factors such as the application sensitivity, the end-user's permissions, as well as the network and location the user connects from
- **Validating that all company devices meet** the baseline configuration it has defined. Configuration requirements typically include having an up-to-date OS version, enabling disk encryption and an active Endpoint Protection Platform (EPP)
- **Blocking access or blocking high risk activities** from devices that don't meet the organization's baseline configuration, to minimize potential risk
- **Limiting access to sensitive documents** based on their content to reduce risk of exposure

Logical and Physical Access (CC6)

SOC2 CC6 focuses on controlling logical and physical access to sensitive information by setting guidelines, best practices and enforcement measures to reduce the risk of exposure. Island can help organizations meet this criteria by:

- **Maintaining a list of all active endpoint devices** that access sensitive systems
- **Authenticating the identity of users** and enforcing access policies
- **Enforcing session timeouts** and use of multi-factor authentication for protecting access to sensitive applications
- **Securing applications with Island Private Access** (zero trust network access) for limiting and controlling access
- **Enforce the use of strong encryption** when accessing any sensitive applications
- **Protecting system credentials** by enforcing the use of the Island Password Manager and preventing passwords from being stored anywhere else
- **Protecting access from mobile devices** using Island's mobile browsers

System Operations (CC7)

The System Operations criteria ensures that appropriate measures are in place to detect vulnerabilities and anomalies in infrastructure and software systems. This is generally out-of-scope for Island, as the Enterprise Browser is an endpoint application.
However, Island will collect data that may be valuable in investigating and responding to security incidents (see CC4 above).

Change Management (CC8)

This criteria requires organizations to define an ordered change management process using dedicated tools for this purpose. It's meant to ensure that performing changes to infrastructure, data and other critical components is managed and monitored. Island can assist in meeting parts of this criteria by:

- **Tracking and storing change logs** that audit sensitive changes, ensuring such changes were performed in accordance with the defined procedures
- **Analyzing historic changes** following any incident caused by specific changes
- **Protecting confidential information** accessed during change management procedures (using DLP, download control, data masking etc.)
- **Adding additional layers of identity verifications of users** (e.g., MFA) before allowing them to perform sensitive actions
- **Full auditing of change operations performed through RDP or SSH**, using Island's built in RDP and SSH clients embedded within the browser

Risk Mitigation (CC9)

Risk Mitigation controls ensure that companies take appropriate measures to mitigate the risk of business disruption and proactively manage the risks associated with vendors and third-party business partners. Island can assist in meeting parts of these controls by:

- **Requiring third-party business partners** to use Island when accessing any company applications or sensitive data to provide security controls and activity logging
- **Including Island as part of a business continuity planning** to enable fast recovery of access if provisioned endpoints are unavailable (e.g., recovering from a natural disaster that impacts company facilities)

Additional Controls

While Security is the only mandatory SOC2 category, the standard also defines the following optional categories: Availability, Process Integrity, Confidentiality and Privacy.
Island can further assist companies in meeting the criteria for these categories by:

- **Automatic identification of confidential information**, using integrated DLP scanners for addressing confidentiality risks
- **Noticeable indications on sensitive web pages**, using watermarks, masking, etc.
- **Access controls to block users from gaining access to confidential areas**, even if not supported by the application level
- **Disposal of PII during offboarding process** for addressing employee privacy

Summary

Service organizations are wise to adopt the SOC2 framework to demonstrate their commitment to security and operational excellence. With collaboration across all areas of the organization — from HR to IT to Security to business process optimization — the SOC2 framework should yield positive results that pay dividends for the organization, their customers, and their business partners. Island offers a range of capabilities to help achieve the SOC2 security controls and demonstrate compliance to support attestation.

To learn more about Island, visit www.island.io.