MITRATECH

Information Security: Attaining SOC 2 Compliance

How Mitratech's Alyne GRC platform helped Cutover meet the requirements necessary for SOC 2 certification.

The Company

The Cutover Collaborative Automation platform enables teams to successfully manage IT disaster recovery, cloud migration, and release by interconnecting teams and technology.

The company is based in the UK and works with world-leading organizations including financial services enterprises, as well as in dynamic, high-growth start-ups, amongst many others.

The Cutover platform, developed with decades of experience across financial services, insurance, telcos and more, enables organizations to confidently move towards their unique set of business goals.

Cutover's solution is designed to coordinate and streamline complex processes, multiplayer activities, and critical events across three use cases:

1. **Technology Resilience**
2. **Cloud Migration**
3. **Release**

10,713

Registered users around the world.

60%

Reduction in failed implementation program delays.

19,175

Runbooks created annually.

The Challenge

Cutover procured Mitratech's Alyne GRC platform in February 2021 as the Information Security team was looking for a GRC tool to help them reduce their manual work in obtaining SOC 2 Type 1 certification.

Furthermore, Cutover is already ISO 27001 certified, so the challenge was to leverage on the controls already assessed with the ISO certification, to achieve the SOC 2 Type 1 certification.

Introduction
What is SOC 2?

The AICPA (American Institute of Certified Public Accountants) developed the System and Organization Controls, known as SOC.

SOC 2 is a compliance framework that focuses on the existing security controls within the organization. Its purpose is to assess and address the organization's security risks. It differentiates itself from other SOC reports as it exclusively concentrates on information security.

SOC 2 reports are based on 5 security principles, known as **Trust Services Criteria**:

- **Security**
- **Availability**
- **Processing Integrity**
- **Confidentiality**
- **Privacy**

There are two different types of SOC 2 reports:

Type I: A SOC 2 Type I report focuses on the security guidelines already established inside the organization. It is an accurate description of the company's security controls without testing their effectiveness.

Type II: A SOC 2 Type II report concentrates on the effectiveness of the security guidelines defined by the organization. It describes the company's security controls and attest their efficiency over a period of time. This certification provides a higher level of assurance than Type I that the organization has complied with the requirements on data security and control systems.

Benefits of SOC 2 Certification

For an organization, its SOC 2 report is a compliance confirmation to security controls meeting some or all of the Trust Service Criteria principles, giving it a valuable competitive advantage. It gives all stakeholders and potential customers assurance that their data is handled safely by a SOC 2-compliant organization that has passed the mentioned auditing process.

The SOC 2 Type I report covers the compliance situation of an organization to the relevant security principles on a specific date, whereas, SOC 2 Type II includes the operational effectiveness of the said assets over a specific period of time.

The demand for SOC 2 Type I reports is particularly high as the number of cybercrimes and cyberattacks keeps mounting. Today, businesses are specifically looking for vendors who not only comply but also prove that they are compliant with these security standards, especially for companies in IT and financial services.

Although the SOC 2 Type I report has many benefits, the SOC 2 Type II report provides a higher assurance level. An auditor examines the internal controls, policies, and practices of an organization over a defined period of time to check if all the requirements are satisfied according to the five trust principles of data processing and storage. An organization providing services with a SOC 2 Type II compliance report, strongly communicates that it has the best practices in place regarding data security and control systems.

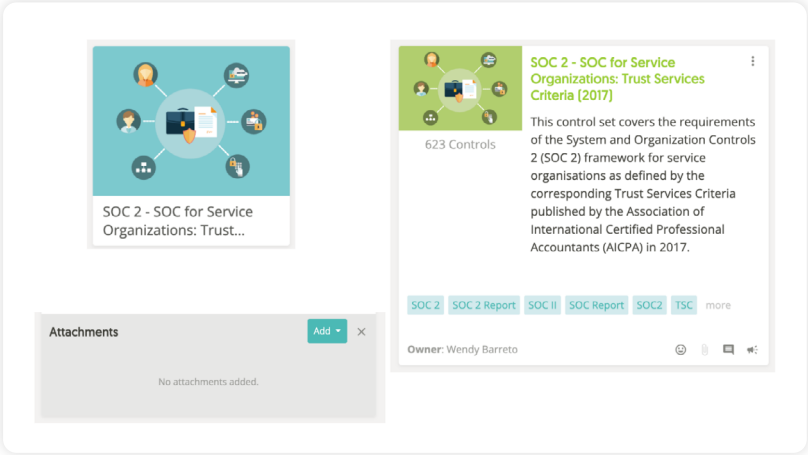
Mitratech's Alyne Solution

With the help of Mitratech's Alyne GRC platform, Cutover ramped up and completely digitalized their legacy certification process. Alyne offers out-of-the-box features that comprehend: Controls, Assessments and Risk Reports.

1. Controls

For **SOC 2** specifically, customers can leverage 625 controls collected in a single 'Control Set' that can be found within the Alyne library under templates, ready for use. Our controls are structured, granular and allow customization.

Control Sets allow customers using Alyne to scope security guidelines and gather the evidence needed for the **SOC 2 Type I** report.

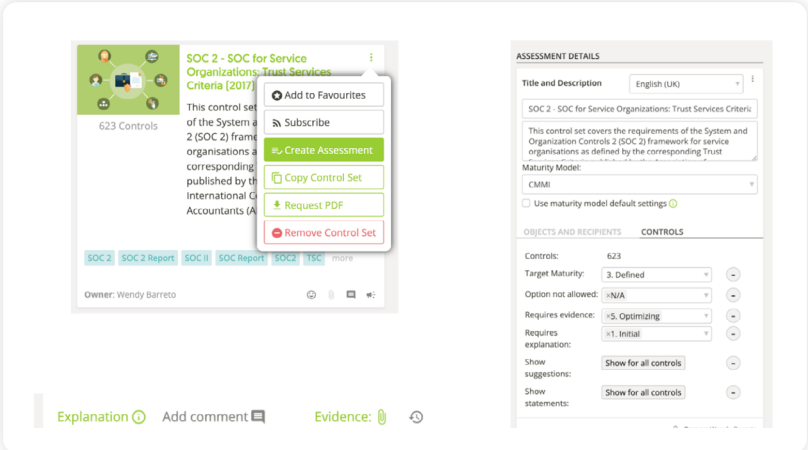


2. Assessments

From the Control Set, an assessment can be easily created and further customized to match the organization's specific needs.

For the **SOC 2 Type I** report, the audit team can leverage the assessment results to execute a gap analysis over a period of time and assess the security guidelines' maturity over time.

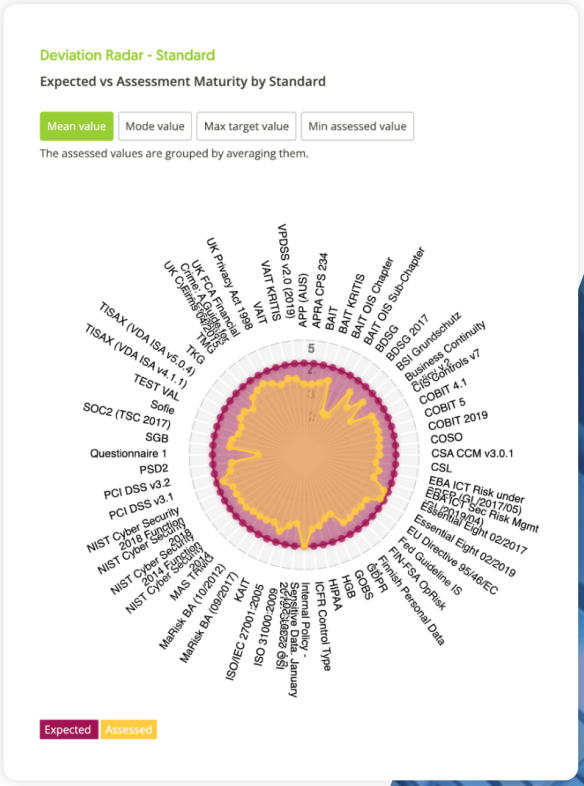
Assessments also allow to collect all the evidence and explanation needed to attest the maturity of the organization's security controls.



3. Risk Reports

Risk Reports allow the audit team to have insights from the assessments' results and a deep overview of risks identified through mentioned assessments. Results are summarized using spider diagrams that can be filtered by different standards and topics.

For the **SOC 2 Type II** report, the platform's 'Reports' functionality can be used to easily identify the potential risks based on the compliance scenario. The identified risks can then be tracked, managed and mitigated under Alyne's Risk Management module, digitizing the organization's risk management process.



Results & Next Steps

Leveraging Mitratech's Alyne GRC platform, Cutover was able to become successfully compliant with the SOC 2 Type I certification after their audit this past 2021. The Trust Service Principles that Cutover attested to achieve their SOC 2 Type I certification were: Security, Availability, and Confidentiality.

Necessary activities to achieve the SOC 2 Type II certification are already in motion, and the required audit is planned for the latter half of 2022.

The SOC 2 Control Set is available for all Alyne customers as an out-of-the-box template within the application. It allows the digitization of the certification process, making it highly customizable and scalable.

Mitratech's Alyne platform has been a valuable tool to help centralize our compliance efforts into one easy-to-use platform. It has been integral to the organization and delivery of our SOC 2 Type 1 audit. We have received great feedback from our auditors on its ease of use.

MITRATECH

cutover