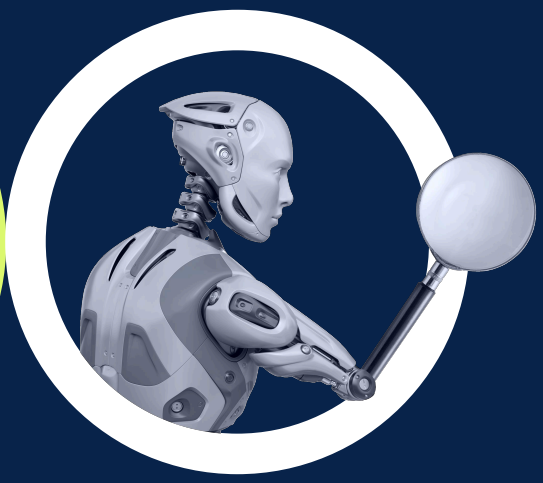


6clicks

SOC 2 compliance:
The complete guide

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

6clicks.com

Contents

01

Introduction

Safeguarding personal and sensitive data is a critical priority for all organizations, regardless of their size, structure, or industry. By upholding information security, organizations can enhance customer trust and effectively eliminate or mitigate threats to their reputation and business continuity.

Various standards and frameworks such as SOC 2 provide requirements and best practices for managing and protecting customer information from unauthorized access, use, distribution, alteration, and destruction. Whether you're preparing for a SOC 2 audit or assessing the security of a new vendor or service provider, learning about the process of SOC 2 compliance is a necessity to maintain the reliability and trustworthiness of your data processing activities and ensure the stability of your operations.

In this guide, we will provide an overview of SOC 2 and a step-by-step guide on how your organization can achieve compliance with the framework. We will also discuss the framework's structure and requirements as well as its importance and benefits to organizations. Finally, learn to leverage the 6clicks platform in streamlining SOC 2 compliance.

What is SOC 2?

SOC 2, or the System and Organization Controls 2 by the American Institute of Certified Public Accountants (AICPA) is a cybersecurity framework and compliance standard that provides guidance for implementing security controls based on specific principles or "Trust Services Criteria" (TSCs) to safeguard customer data.

A SOC 2 report is a document that validates your organization's implementation of these controls and is a requirement for achieving SOC 2 compliance. Compliance with SOC 2 is a voluntary procedure but is often required in sectors such as finance and healthcare to ensure that organizations storing, processing, and managing customer data within digital environments are equipped with robust security measures to fortify their data handling practices.

Essentially, SOC 2 aims to foster trust between companies or service providers and their customers through proactive cybersecurity risk management. Here are some of the advantages of incorporating the SOC 2 framework into your organization's cybersecurity strategy:

Strengthened security posture

Implementing robust security controls and procedures safeguards data and prevents operational disruptions.

Improved customer trust

A SOC 2 attestation report serves as tangible evidence for an organization's commitment to and capacity for enhanced data security.

Streamlined regulatory compliance

SOC 2 controls align closely with the requirements of the Digital Operational Resilience Act (DORA) and the Healthcare Insurance Portability and Accountability Act (HIPAA), facilitating regulatory compliance.

Greater competitive advantage

Being SOC 2 certified means you have undergone a rigorous independent audit and met strict security standards, positioning your organization ahead of competitors.

Effective risk management

By prioritizing information security, your organization can proactively mitigate risks ranging from third-party vulnerabilities to data breaches and prevent potential financial losses and reputational damage.

02

The 5 Trust Services Criteria

The SOC 2 framework consists of five Trust Services Criteria: Security, Availability, Confidentiality, Processing Integrity, and Privacy. During a SOC 2 examination, these criteria are used to evaluate the suitability and effectiveness of an organization's controls. Let's take a look at each set of criteria in detail:

Security

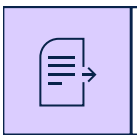
The Security principle or Trust Service Criteria encompasses the protection of information against unauthorized access as well as systems and system resources from being damaged or compromised. Organizations may choose to align their controls with the other TSCs but the Security criteria is a mandatory component in every SOC 2 report.

Under the Security criteria are 9 Common Criteria (CC), which are core components that apply across all Trust Services Criteria. These Common Criteria detail a set of requirements an organization must meet upon developing and implementing controls:

Common Criteria	Objective
CC1: Control Environment	Establish an organizational framework following standards of conduct for integrity, security, and accountability through strong governance and effective oversight.
CC2: Communication and Information	Ensure that staff fully understand security objectives and their corresponding roles and responsibilities, and that security information—such as incidents—is communicated to external stakeholders in a timely and effective manner.
CC3: Risk Assessment	Identify, analyze, and prioritize security risks based on their likelihood and potential impact and implement risk response measures
CC4: Monitoring Activities	Continuously monitor and evaluate the performance of security controls and take corrective actions for any identified issues and nonconformities.
CC5: Control Activities	Put in place processes, systems, and tools to mitigate risks.
CC6: Logical and Physical Access Controls	Enforce security measures to limit digital and physical access to sensitive data to authorized users only.
CC7: System Operations	Maintain the proper functioning of IT systems and set up mechanisms for restoration and recovery in the event of disruptions.
CC8: Change Management	Establish a formal process for requesting, evaluating, testing, approving, and documenting system changes.
CC9: Risk Mitigation	Implement measures for preventing, detecting, and responding to the occurrence of risks.

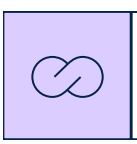
Based on these guidelines, organizations can then design and implement their own controls to meet the Security criteria. Example controls include:

CC1: Information security policies covering remote access, the principle of least privilege, awareness and training, and more



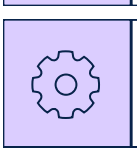
CC2: Internal and external communication mechanisms and incident response procedures

CC3: Risk assessment procedures



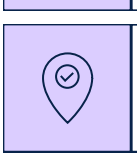
CC4: Internal audits and continuous control monitoring using cloud security posture management (CSPM) tools

CC5: Technical controls such as multi-factor authentication, secure configuration, and patch management

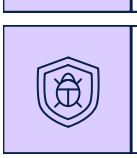


CC6: Logical controls such as identity and access management (IAM) and physical controls like surveillance systems

CC7: Technical controls such as vulnerability management, security information and event management (SIEM) systems, and data backups



CC8: Administrative and technical controls such as secure software development life cycle (SDLC) processes, testing and validation, and version control



CC9: Preventive and detective controls such as firewalls, intrusion detection and prevention systems (IDS/IPS), and endpoint protection

Essentially, the Security criteria involves establishing comprehensive compliance, operational, and cybersecurity measures to maintain the security of information and the resilience of information systems.

Availability

Other TSCs are considered additional criteria because they build upon the framework established by the Security criteria. Aside from common criteria, organizations can align their controls with additional criteria such as the Availability (A1) criteria. This particular set of criteria focuses on ensuring the accessibility of information and the reliability of critical systems and system resources.

Meeting the Availability criteria entails identifying threats to information availability, implementing measures to secure, monitor, and maintain data centers, and determining system capacity and the minimum performance level needed to support business operations and data processing requirements.

Business continuity and disaster recovery plans, data redundancy and failover mechanisms, server performance monitoring, and capacity management are some examples of controls you can put in place to satisfy the Availability criteria.

Confidentiality

The principle of Confidentiality (C1) deals with protecting confidential information whether at rest, in use, or in transit. Confidential information refers to highly restricted data that can only be accessed by authorized individuals or organizations. This includes legally protected, sensitive, or proprietary information such as government contracts, legal documents, and employee records.

Safeguarding confidential information in the context of SOC 2 means ensuring proper data classification, securing the flow of information across all channels and endpoints, and enforcing secure data handling practices throughout the life cycle of data, including storage, transmission, processing, retention, and deletion.

Implementing controls such as confidentiality and data handling policies, data encryption, and role-based access control can help organizations meet the Confidentiality criteria.

Processing Integrity

The Processing Integrity (PI1) criteria addresses the capacity of an organization's systems for complete, valid, accurate, timely, and authorized data processing activities. This involves preserving the integrity of information by ensuring data remains secure and unchanged when processing inputs and outputs as well as during storage and retrieval.

To fulfill criteria for processing integrity, Organizations can put in place automated logging and monitoring systems to detect processing errors and ensure transaction integrity, along with quality assurance procedures to validate the accuracy, completeness, and reliability of processed data.

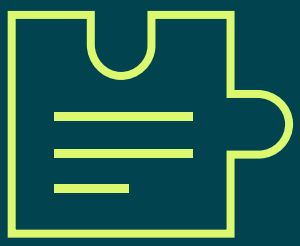
Privacy

Lastly, the Privacy principle covers an organization's efforts in safeguarding private data or personal information that is not meant for public disclosure. It requires organizations to align with the following criteria:

Additional Criteria	Objective
P1: Notice	Clear and accessible information on the organization's privacy practices and objectives, including how personal data is collected, used, stored, and shared, must be provided to data subjects.
P2: Choice and Consent	The organization must inform data subjects of their right to accept or decline the collection, use, retention, disclosure, and disposal of their personal information—along with the corresponding consequences—and must obtain their explicit consent for any related activity.
P3: Collection	The collection of personal information must be limited only to necessary data required for business operations and in alignment with the organization's privacy objectives.
P4: Use, Retention, and Disposal	The use of information must be restricted to its intended purpose and personal data must be securely stored and disposed of when no longer needed.
P5: Access	The organization must grant data subjects the right to request access to as well as correct or delete their stored personal information.
P6: Disclosure and Notification	Explicit consent must be obtained by the organization from data subjects before disclosing any personal information to third parties.
P7: Quality	Develop procedures for preserving data quality to keep stored information accurate, complete, relevant, and reliable.
P8: Monitoring and Enforcement	Put in place mechanisms for monitoring compliance with privacy policies and objectives, including response protocols for privacy breaches.

Organizations can meet these requirements through controls such as internal and public-facing privacy policies to ensure transparency, well-defined third-party data-processing agreements (DPA) to guarantee vendor compliance, and data validation systems to maintain data quality.

03



SOC 2
compliance process

Now that you understand what SOC 2 is all about, there are a series of steps you need to take before you can go through a SOC 2 examination or audit and attain compliance.

Before the audit

1. Define the scope and objectives for implementation

Before you start implementing SOC 2, first you need to identify what type of SOC 2 report you're aiming for so you can align your efforts, as the examination process and evidence requirements differ for each. A SOC 2 Type 1 report evaluates the design and implementation of controls at a single point in time, while a Type 2 report assesses control effectiveness over a specific time period, ranging between 3 and 12 months. You also need to determine the relevant Trust Services Criteria applicable to your organization and define the outcomes you want to achieve with compliance. Then, identify the systems, processes, and resources necessary for implementation.

	SOC 2 Type 1 Report	SOC 2 Type 2 Report
Scope	Control design and implementation	Control effectiveness over a period of time
Assessment Period	Point-in-time assessment	Continuous assessment
Evidence Requirements	Security policies, configurations, and documentation	Logs, reports, and historical data showcasing operational effectiveness
Applicability	Best for companies looking to prove compliance quickly	Best for mature companies requiring a deeper level of assurance for their customers
Audit Timeline	5 to 8 weeks	3 to 12 months

2. Identify compliance gaps

Compare your existing security controls with the requirements set out by SOC 2. Performing a gap assessment will help you identify any deficiencies in your controls, policies, and procedures so you can develop a remediation plan.

3. Implement controls

After identifying all compliance gaps, you can proceed to implement the necessary controls to address them. This means updating or establishing additional policies, utilizing new tools and technologies, and refining existing processes and procedures. Ensure a balanced implementation of administrative, technical, and physical controls for a comprehensive compliance strategy.

4. Testing and external audit preparation

To verify that controls are properly implemented and functioning optimally, you need to conduct testing activities along with an internal audit that simulates an actual SOC 2 examination. Run vulnerability scans and penetration tests to uncover security vulnerabilities. Conduct an internal audit and engage relevant departments such as security and compliance teams. Collect evidence of control implementation including audit findings, control reports, policy documents, and other technical documentation. For SOC 2 Type 2 reports, historical data such as access logs, security incident reports, and records of change request approvals are necessary to demonstrate control effectiveness over time.

5. Select an auditor

Once your controls and evidence requirements are all set, you're now ready to go through the SOC 2 examination. Seek a certified public accountant or CPA firm to conduct an independent audit of your security controls, policies, and operational effectiveness to assess compliance with your selected Trust Services Criteria.

During the audit

The SOC 2 examination process takes between five weeks and two months for Type 1 and three months to a year for Type 2. During the audit, it is important to communicate and cooperate effectively with the auditors. Be proactive in answering questions and provide supporting information promptly upon request for a smoother and faster process.

After the audit

Once the SOC 2 examination is completed, you will receive a SOC 2 attestation report containing complete findings from the audit. If there are no major issues identified, it confirms that you have achieved SOC 2 compliance and have successfully demonstrated a robust security posture. Some best practices to follow at this stage include:

Developing an action plan to address any areas of non-compliance

Continuously monitoring security controls to detect and address issues proactively

Sharing audit findings with customers, partners, and regulators to strengthen trust

Regularly updating policies and procedures to align with evolving threats and regulatory requirements

Conducting periodic audits and risk assessments to maintain a consistent security posture

Renewing your SOC 2 report annually to maintain trust and compliance

04

The 6clicks **SOC 2 solution**

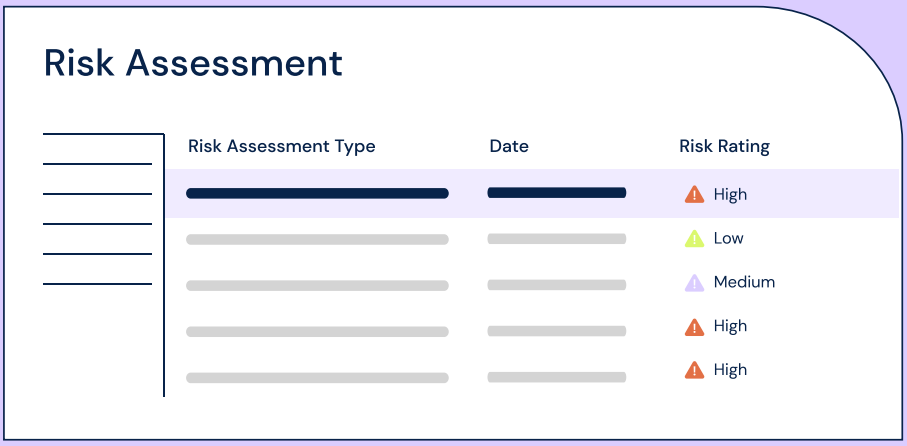
To help you streamline the SOC 2 compliance process, 6clicks provides an all-in-one platform with built-in content and functionality to support your organization from planning and control implementation to becoming audit-ready and building stakeholder trust. Our SOC 2 solution equips you with powerful capabilities such as:

Content Library

Download the SOC 2 framework for free including ready-to-use risk libraries, control sets, and assessment templates.

Risk management

Identify and manage risks, conduct risk assessments, and create risk treatment plans using a systematic risk register.

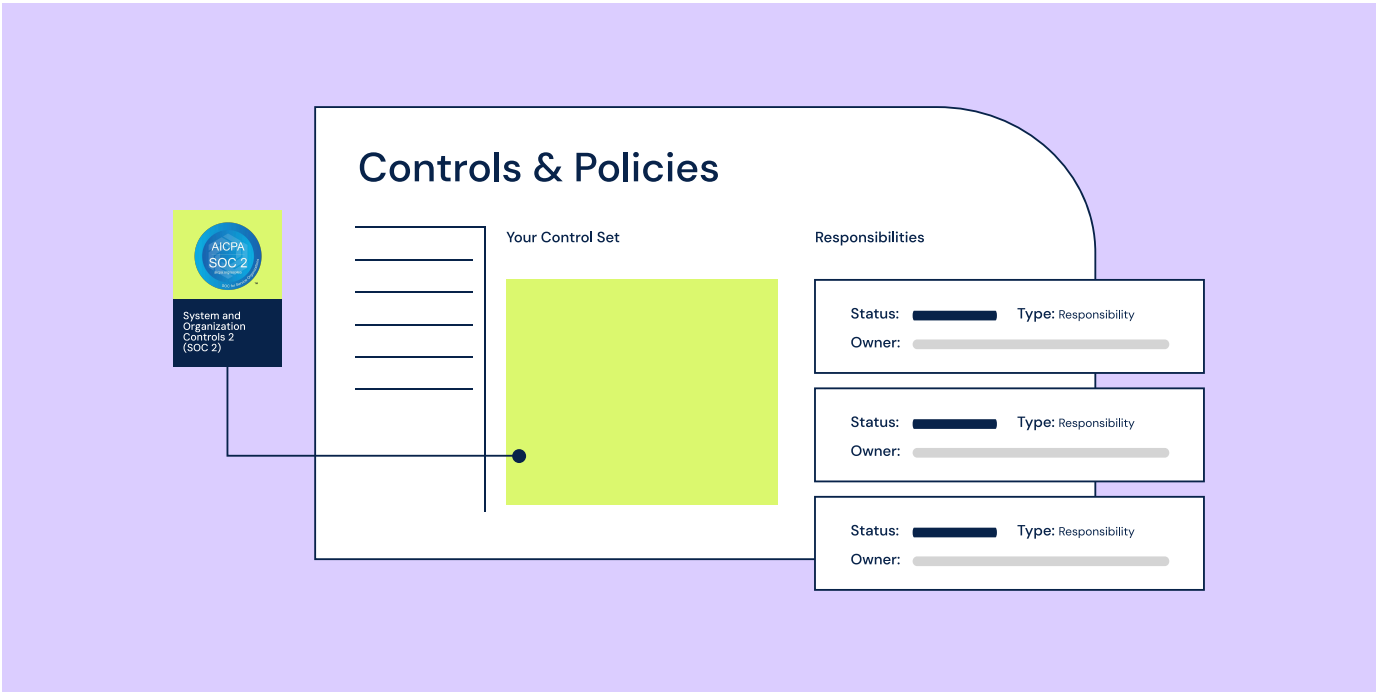


AI-powered gap analysis

Use 6clicks' AI engine, Hailey, to automate the mapping of your security controls to SOC 2 requirements and identify compliance gaps within seconds.

Control implementation

Set up your security controls and policies, assign tasks and responsibilities, and use continuous control monitoring to gain real-time visibility into control effectiveness.

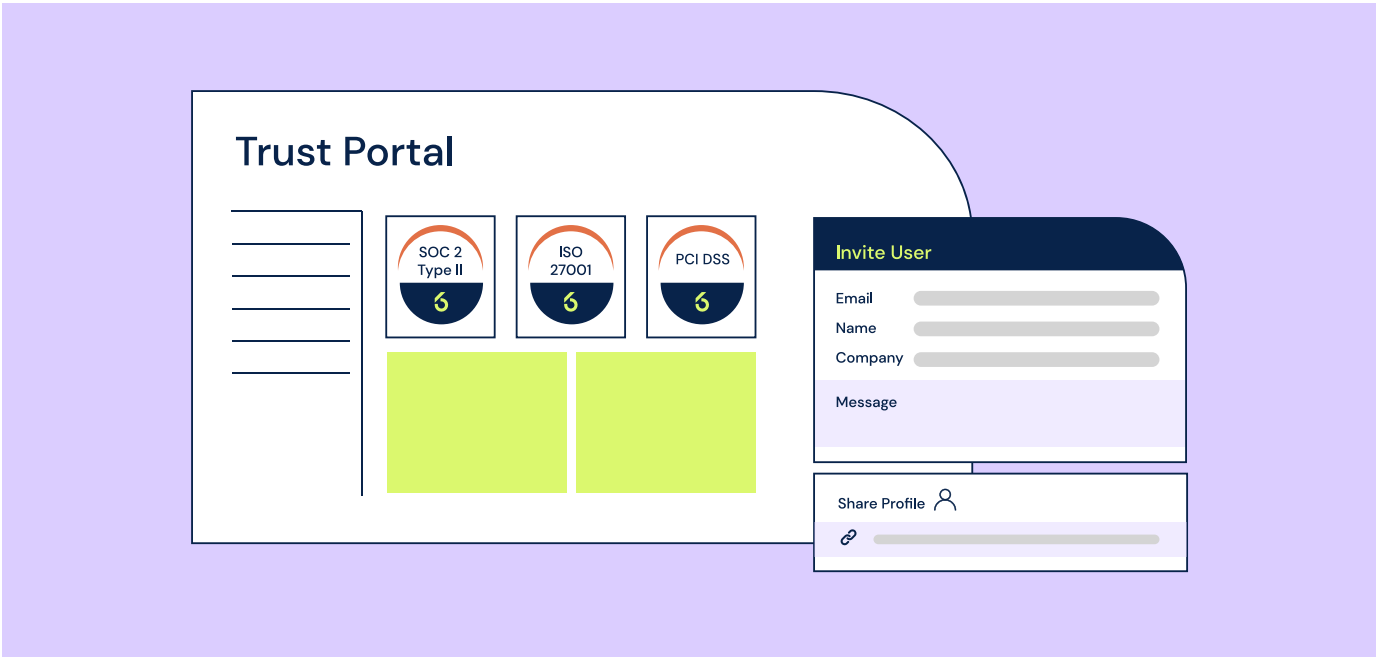


Audit and assessment

Perform audits and assessments to validate compliance and use turnkey templates and AI-powered responses to expedite the process.

Trust Portal

Enhance assurance by making your SOC 2 attestation, internal audit reports, and other evidence of compliance publicly accessible using the 6clicks Trust Portal.



Customer Reviews

> The 6clicks solution simplifies and strengthens risk, compliance, and control processes across entities and can grow and adapt as the organization changes and evolves."

Michael Rasmussen
GRC 20/20 Research LLC

> The ability to work closely with the 6clicks team to configure the tool for our needs has been invaluable."

Joe Kelly
VP of IT and Data Security, Lumine Group

LUMINE

Learn more about 6clicks

Book a demo

Ready to build resilient cyber GRC programs powered by AI? Explore the 6clicks platform today.

Book a demo

See 6clicks in action

Watch exclusive demonstrations of our AI and cyber capabilities through our on-demand webinars.

Watch webinar

Explore helpful resources

Get access to the latest cybersecurity, risk, and compliance news and thought leadership by industry experts.

Read blog

6clicks

6clicks is transforming cyber risk and compliance management with its AI-powered platform, featuring the pioneering Hub & Spoke architecture tailored for federated businesses, advisors, and managed service providers (MSPs). As the first platform to introduce an AI engine specifically designed for GRC, 6clicks delivers a smarter approach to managing cyber risk and compliance. The 6clicks business model is channel-aligned, and SaaS licensing is transparent and straightforward with unlimited user access and access to frameworks. With sales and support operations presence across APAC, EMEA, and NA, and private cloud hosting options on Microsoft Azure, 6clicks equips cyber leaders and professionals to build resilient, trusted, and scalable cyber risk and compliance programs, disrupting traditional GRC solutions and setting a new standard in the industry.

Request a demo