[Use Case]

# How TruOps Empowers SOC 2 Success with Innovation

## INTRODUCTION

In today's complex digital landscape, companies must ensure their cyber resiliency strategy is based on cybersecurity best practices and right fit technology. System and Organization Controls 2 (SOC 2) is a security framework developed by the American Institute of Certified Public Accountants (AICPA) to assess and report on the operating effectiveness of the controls and processes related to security, availability, processing integrity, confidentiality, and data privacy at service organizations. SOC 2 outlines how organizations can best protect customer data from unauthorized access, security incidents, and other vulnerabilities. As major data breaches and security incidents become more common, companies that can demonstrate a strong data security posture gain an advantage over competitors when meeting new customers or business partners with stringent security requirements.

## CHALLENGES

Though the dependence on digital data and systems has enabled organizations to streamline operations and enhance customer engagement and user experience, it has also increased their vulnerability to cyberattacks. Organizations entrusted with sensitive (and valuable) data of hundreds (or tens of thousands) of customers are at risk of a security breach that leads to unauthorized access by bad actors. Compromised financial records, health information, proprietary business intelligence and even email accounts can leave customers vulnerable to fraud and loss.

For companies that provide services such as data hosting, cloud computing, software as a service (SaaS), or other product offerings where data security and privacy are critical linchpins to business operations, SOC 2 compliance demonstrates the commitment to protect customer data. However, businesses that have little to no experience roadmapping and implementing security compliance standards can face the following challenges:

- **Comprehending Complex Compliance Requirements:** Understanding the complex framework of SOC 2 requirements is a daunting task. The SOC 2 framework is based on several controls and criteria that have their own specifications and implementation rules. Compliance with these requirements typically requires a significant investment in time and resources.
- **Conducting Risk Assessments:** Auditing the scope of information systems, software, infrastructure, and processes to identify and mitigate potential risks to the security, availability, confidentiality, and privacy of data can be riddled with obstacles for companies without the guidance of an experienced partner.
- **Ongoing System Monitoring:** Maintaining ongoing SOC 2 compliance requires establishing processes for the continuous monitoring of systems, controls, and security measures, which can put a strain on available resources.
- **Managing Documentation:** Building a document repository of policies, procedures, controls, assessments, and audits is a time-intensive, but necessary, function of maintaining SOC 2 compliance.
- **Preparing for Audit and Response:** Planning for a SOC 2 audit and delivering evidence to auditors to demonstrate compliance can be stressful and overwhelming. This is especially true for companies new to the process.
- **Choosing a SOC 2 Vendor Partner:** Identifying trusted vendors and service providers that meet SOC 2 requirements can be difficult in a noisy marketplace.

## SOLUTION

- TruOps, a leader in innovative cyber risk management solutions, has developed a robust Governance, Risk, and Compliance (GRC) platform to help companies achieve compliance and boost their security posture. TruOps' GRC brings flexibility and scalability in preparing for SOC 2 assessments. TruOps' risk assessment capabilities enable clients to clearly identify, analyze, and prioritize cybersecurity risks according to SOC 2 regulations.
- TruOps supports the customization of SOC 2 compliance frameworks in alignment with specific industry, regulatory, and organizational requirements. Companies can tailor controls, policies, and workflows to reflect their unique security posture and compliance objectives. TruOps also enables businesses to conduct SOC 2 gap analyses and identify areas where their current cybersecurity controls and practices are deficient in meeting SOC 2 guidelines. Armed with this insight, clients can expedite their readiness for SOC 2.
- Monitoring and reporting are activities central to achieving and maintaining SOC 2 compliance. TruOps' GRC features two important functionalities: scheduling and reporting. The TruOps scheduler enables customers to schedule monthly and/or quarterly controls assessments on assets, business processes, and organizations to maintain alignment with the SOC 2 framework. In keeping with SOC 2 risk management best practices, this feature facilitates the continuous monitoring of the effectiveness of implemented cybersecurity controls and the identification of emerging risks.
- Customers benefit from TruOps' out-of-the box KPI dashboards that deliver charts and comprehensive reports. These at-a-glance dashboards support the generation of assessment reports and include graphical representations of the customer's cybersecurity posture, risk levels, and improvement recommendations.
- Key benefits of the TruOps Policy Management module include the ability for companies to convert policy documents into standardized authority documents with controls and citations that can be published after comments and feedback have been incorporated. The final version policies are stored within TruOps as hard copy documents. This document repository gives clients fast and easy access to policy reviews status, user attestation tracking, and policy extensions and renewals. In addition, TruOps' logging capabilities create an audit trail of all SOC 2 assessment activities and changes made within the platform. This feature helps ensure auditability and the integrity of assessment results.
- Clients trust TruOps as a SOC 2 compliance vendor partner because we combine deep industry expertise with advanced technologies and methodologies to conduct SOC 2 assessments and manage compliance activities. TruOps' clients also receive in-depth training and highly responsive support. We provide comprehensive training for each TruOps module, alongside user guides, and high-touch customer support.
- TruOps' native self-service integrations coupled with automation of repetitive security tasks creates a streamlined compliance experience. Risk assessment, policy management, reporting, and audit preparation activities are simplified to provide customers with successful outcomes.

## CONCLUSION

SOC 2 compliance is a critical milestone for companies seeking to validate their commitment to data security. While achieving SOC 2 compliance is challenging and complicated, partnering with the right cybersecurity solution provider can make the journey less intimidating and expedite success. TruOps understands these challenges and delivers the experience, technologies, and methodologies that enable customers to take a proactive – not reactive – approach to cybersecurity and SOC 2 compliance.

Contact us **today to learn more about how TruOps can quickly be implemented and enable your organization to clearly identify, analyze, and prioritize cybersecurity risks according to SOC 2 regulations.**

## ABOUT TRUOPS

TruOps is a powerful GRC that transforms traditionally siloed modules into a risk operations center. Designed to integrate and automate critical GRC functions, TruOps simplifies the security, risk, and compliance processes organizations need to manage and control risk effectively. TruOps meets your organization where it is today and scales to meet evolving cyber risks, whether regulatory, internal, or third-party.

+1 (203) 866 - 8886 sales@truops.com www.truops.com