SECURISEA

Think, Before You Adopt: Five questions you should ask before adopting a new SOC2 Control

Introduction

Our goal for this document is to help security-minded professionals responsible for safeguarding their organizations' most sensitive data think strategically about how, and when, to design and adopt a new SOC2 Control. By asking strategic questions early in the process, we hope to help you save valuable time, money, and avoid preventable headaches when considering the adoption of new SOC2 controls for your business.

Question 1: Why are we adopting a new SOC 2 control?

The obvious answer is - to bolster our organization's cybersecurity defenses and enhance our overall security posture. The deeper question is - Is this in response to a newly identified risk or outside threat? Is there a new requirement to achieve certification? Was there an issue in your last audit? The number of controls you put in place will depend on the number of Trust Services Criteria you include in your audit, and the complexity of your infrastructure and organization. Having a clear and honest discussion with your team about why you are considering adding additional controls from the very beginning makes the process much smoother and more efficient.

Question 2: What Are Our Specific Security Objectives?

Before adopting a new SOC 2 control, you must first identify your specific security objectives and priorities. This involves understanding the unique risks facing the organization, the sensitivity of the data it handles, and the potential impact of security breaches on its operations and reputation. By clarifying these objectives you can ensure that the adopted SOC 2 control addresses the most pressing security concerns and aligns with broader strategic goals.

SECURISEA

Question 3: Does the Control Address - and Meet - Our Existing Compliance Requirements?

In addition to enhancing security, SOC 2 controls must also address compliance requirements relevant to the organization's industry and geographic location. Before adoption, organizations should carefully evaluate whether the proposed control adequately addresses applicable regulatory mandates, industry standards, and contractual obligations. This ensures that the organization remains compliant while bolstering its security posture through SOC 2 adoption.

Question 4: How Will the Control Impact Our Operations and User Experience?

While security is paramount, organizations must also consider the potential impact of adopting a new SOC 2 control on their operations and user experience. This includes evaluating whether the control introduces new complexities or inefficiencies that could disrupt business processes or degrade customer satisfaction. By conducting thorough impact assessments, organizations can proactively mitigate any adverse effects and ensure a seamless transition to the new control.

Question 5: What Metrics Will We Use to Measure Effectiveness?

Measuring the effectiveness of SOC 2 controls is essential for ongoing improvement and assurance of compliance. Before adoption, organizations should define key performance indicators (KPIs) and metrics to assess the control's efficacy in mitigating risks and achieving security objectives. These metrics should be measurable, actionable, and aligned with organizational goals, allowing for continuous monitoring and optimization of SOC 2 compliance efforts.

Final Thoughts

Adopting a new SOC 2 control is a significant undertaking that requires careful deliberation and planning. More controls does not always equal better security. By asking these five critical questions before adoption, organizations can ensure that the control in question was designed for a reason, effectively addresses security risks, complies with regulatory requirements, and won’t disrupt your day to day operations during implementation. Additionally, by establishing clear metrics for measuring effectiveness and impact, organizations can drive continuous improvement and enhance the overall security posture through the SOC 2 compliance.certification.

SECURISEA

Simplifying security compliance
since 2006

LEARN MORE