SOC 2 Certification – We're Almost There!

Devolutions

AN ALARMING 54% OF ORGANIZATIONS STILL USE SPREADSHEETS AND PAPER TO HANDLE PRIVILEGED CREDENTIALS

Recently, we highlighted that we have added 2FA to Devolutions Cloud, and we plan on expanding 2FA across all of our products in the coming months.

Today, we take a deeper look at another major security development that we're working on: SOC 2 certification.

What Is SOC 2?

Developed by the AICPA, SOC 2 is internationally-recognized for its rigorous auditing procedure, which verifies that a service provider's systems are configured to ensure security, processing integrity, availability, confidentiality, and/or privacy of customer data. It also includes an examination of internal controls, exploring whether a service provider has established a solid foundation for information security. SOC 2 requires long-term and lasting internal practices, thereby ensuring constant data security. Put simply, SOC 2 is designed to diminish security risks.

SOC 2 compliance presents organizations with major advantages over their competition by demonstrating well-defined enforcement of internal information security policies, procedures, and practices — such as those related to password management protocols, as well as various technical, physical and organizational security controls. Once in place, these measures will allow your company to detect security threats, mitigate their impacts, and implement post-incident corrective measures to prevent similar issues from emerging in the future. A growing number of tech companies consider SOC 2 compliance certification mandatory.

Our SOC 2 Plan

Here at Devolutions, our goal is to achieve SOC 2 compliance by the end of this year. As you may know, it is a long and complex process. To get ahead of the curve, we are already using the Committee of Sponsoring Organizations (COSO) framework to comply with all SOC 2 requirements. This framework helps ensure that when we go to production with a new feature or a bug fix, we don't unintentionally introduce anything negative into the environment that would create vulnerabilities or diminish user experience. We are also using the COSO framework to guide our SSO and (upcoming) 2FA offerings.

The whole SOC 2 procedure is monitored and assessed by third-party auditors to independently verify that the measures in place meet all the necessary trust criteria. Here are the trust criteria:

1. Control Environment

Control environment refers to the collective set of standards, processes, and structures that specify the basis for carrying out internal control across the organization. Having a strong control environment demonstrates commitment to integrity and ethical values, while improving exercise oversight responsibility, establishing structure, authority and responsibility, demonstrating commitment to competence, and enforcing accountability. The resulting control environment has an extensive impact on the overall system of internal control.

2. Risk Assessment

Risk assessment refers to identifying, monitoring and analyzing known and unknown activities, such as unusual system activity, authorized and unauthorized system changes, and any modifications made to user permission levels. The "unknown" can be monitored by knowing what normal activity looks like and then determining what constitutes unusual activity.

3. Control Activities

Control activities are all the actions and controls established through internal policies and procedures that have been put in place to meet all your internal control objectives. Control activities are performed at various stages within business processes. They can be preventive or detective, and they may include a series of manual and automated activities, such as authorizations and approvals, verifications, reconciliations, and business performance reviews.

4. Information & Communication

Information & Communication refers to what and how relevant information is captured, which ultimately support employees in carrying out their duties in an efficient, secure and compliant manner. The quality of information and effective communication throughout an organization can greatly impact your ability to meet internal control objectives.

5. Monitoring Activities

Monitoring activities refer to the capacity of an organization to create detailed audit trails that capture who, what, when, where, and how a security breach occurred. It is of great importance to know the source and extent of an attack when it comes time to make a quick and proper security incident response. Audit trails are the best way to get the information you need to carry out your security controls and to react quickly and properly when facing a security breach.

When a security breach happens, you need to demonstrate that your company had set up proper anomaly alerts, and that appropriate procedures were in place to respond quickly and take corrective action. You must therefore determine what activities may constitute a threat for your company – like unauthorized data modification, permissions or configuration – and then implement adequate monitoring controls. This will ensure that you'll be alerted the moment threats or security incidents happen, so you can take immediate action to prevent the security breach and mitigate data loss.

Looking Ahead

We have always been focused on establishing and maintaining strong, enterprise-grade information security processes and policies. Achieving SOC 2 compliance by the end of this year will further demonstrate our capacity, competence and commitment in this area. We will be providing updates on developments — stay tuned!

Your Experience?

If your organization has achieved SOC 2 compliance – or if (like us) you are on the way – please comment below and share your experience, insights and advice.