Allocadia
Marketing Performance Management

ALLOCADIA 2016 SOC2 COMPLIANCE OVERVIEW

Summary

Enterprise-class organizations require assurance from their partners and service providers that information assets transferred to them during the course of business will be handled with as much care as the data's owners. As an enterprise software provider, Allocadia is deeply committed to the integrity, privacy, and security of client data and have demonstrated this commitment through the successful completion of an independent SOC 2 audit on July 31st, 2016.

The Service Organization Control (SOC) audit demonstrates that an independent firm has audited an organization's security control objectives and activities, and tested those controls for efficacy and fitness-for-purpose. Allocadia worked with Deloitte to complete the SOC 2 audit and deliver a successful report on the effectiveness of Allocadia's information risk management program.

Comprehensive Examination of Controls

The SOC 2 audit process is grounded in an examination of an organizations' Information Risk Management & Security Policies, Procedures, Practices, Methods, and Systems. The final SOC 2 report is issued to organizations that have verified audited controls in place which align to sound risk governance criteria, and established trust principles. This independent audit ensures that the organization meets the stringent requirements set forth by the AICPA and CICA for Security controls, and that the controls have been implemented in a manner which provides compliance assurance.

Applications and software developed by a SOC 2 organization, by definition, must be developed following audited processes and controls. This assures that applications and code are developed, reviewed, tested, and released against the standards set forth in the Security Trust Services Principle.

Successful Completion

To achieve compliance against the SOC 2 security trust principle, the following areas of Allocadia's Information Risk & Security Program were audited by Deloitte:

- **Infrastructure**: The physical components of the Allocadia system, including network and hardware security assurance.
- **Software**: The software services and operating software of the Allocadia system.
- **People**: The personnel involved in the operation and use of the Allocadia system, as well as the process by which 'human security' is maintained.
- **Procedures**: The automated and manual procedures involved in the secure operations of the Allocadia system.

- **Data Assets**: The security of information assets used and supported by the Allocadia system from both the clients' and Allocadia's data- and net-flow contexts.

At the conclusion of the SOC 2 Audit process, Deloitte issued the final SOC 2 report, with no exceptions or recommendations, noting that:

a. *"The controls stated in the description [of the system] were suitably designed to provide reasonable assurance that the applicable trust services criteria would be achieved."*
b. *"The controls tested…provide reasonable assurance that the applicable trust services criteria were achieved."*

By attaining alignment to the SOC 2 standards, and by ensuring that our processes have been audited against established security criteria, Allocadia continues to demonstrate its commitment to data security and to the defense of our clients' most valued assets: their data.

Contact

For further information about Allocadia's SOC 2 compliance, please reach out to:

Ryan Marples
CTO
ryan.marples@allocadia.com

Sabino Marquez
CISO
sabino.marquez@allocadia.com