

Lazarus Alliance

Lazarus Alliance Performs Annual SOC 1 Type 2 Audits for Column5

Column5's continuing partnership with Lazarus Alliance demonstrates its ongoing commitment to proactive cyber security and compliance.

Scottsdale, AZ, September 10, 2018 (Newswire.com) -

Lazarus Alliance, a leading cyber security, governance, risk, and compliance (GRC) firm, is continuing to work with [Column5](#), the world's elite consulting firm dedicated to providing leading edge solutions leveraging the SAP Enterprise Performance Management Suite. Lazarus Alliance performs Column5's annual SSAE 18 SOC 1 Type 2 audits and helps ensure that the company maintains proactive cyber security between audits.



"The Lazarus Alliance team continues to be an effective partner to Column5. Their depth of experience and productized tool ITAM from Continuum GRC help us maintain compliance in a cost effective manner," said Ian Thurbon, CEO of Column5.

The Service Organization Control 1 (SOC 1) report is part of the AICPA SOC reporting framework, which includes SOC 1, SOC 2, and SOC 3 reports. Unlike the SOC 2 and SOC 3, which address non-financial controls, SOC 1 reports utilize the SSAE 18 attestation standard to address controls relevant to user entities' internal control over financial reporting.

"It is imperative for service organizations to maintain appropriate controls between audits because the cyber security threat landscape changes daily."

— MICHAEL PETERS
CEO, LAZARUS ALLIANCE

SOC 1 Type 2 reports cover a period of time of no less than six months. They describe the service organization's system and test the design and operating effectiveness of key internal controls over the specified time period. The report is used by the organization's customers and their auditors to plan and perform an audit of their financial statements. In general, a new report

is issued annually.

"The SOC 1 Type 2 report helps service organizations meet their clients' audit and compliance needs," said Michael Peters, CEO of Lazarus Alliance. "An SOC 1 attestation is not a one-time report. It's an annual commitment because a lot can change in a company in a year. Additionally, it is imperative for service organizations to maintain appropriate controls between audits because the cyber security threat landscape changes daily."

Lazarus Alliance utilizes the proprietary [Continuum GRC IT Audit Machine \(ITAM\)](#), a cloud-based GRC automation solution, to navigate Column5 through the SOC 1 audit process and maintain data security and governance between audits. The ITAM is a complete GRC solution that integrates IT governance, policy management, risk management, compliance management, audit management, and incident management. It helps create, measure, monitor, and manage IT governance programs based on leading control frameworks such as GDPR, FedRAMP, COSO, SSAE 18 SOC 1, AT 101 SOC 2, CJIS, DFARS, ISO 27001, NIST 800-53, and CSF.

"All organizations have pain points related to the SOC 1 reporting process, and ITAM takes that pain away," Peters noted. "By automating the compliance process with ITAM, we can quickly design a customized process to help our clients benchmark and compare their internal controls against industry best practices."

Source: [Lazarus Alliance](#)

Related Files

- [lazarus-alliance-corporate-digital-brochure](#)
- [Continuum-GRC-Overview-2018](#)

Additional Links

- [AICPA SSAE-18 SOC 1, SOC 2 & SOC 3 audit services from Lazarus Alliance](#)
- [SSAE 18 Audit \(SOC 1\) AT 101 \(SOC 2 and SOC 3\) audit software modules from Continuum GRC](#)