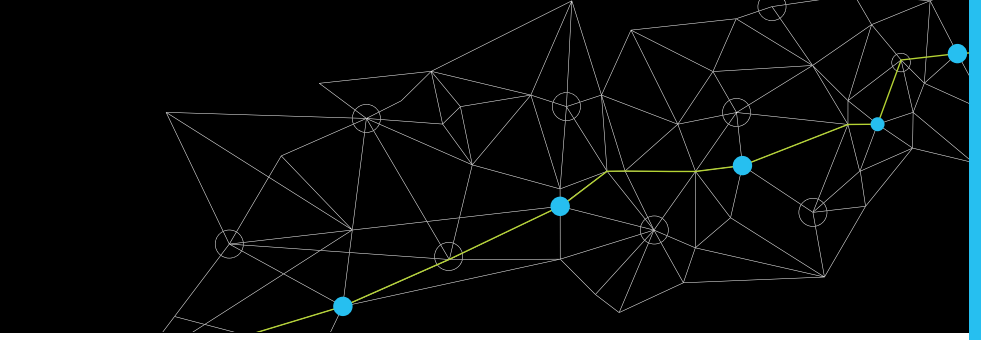

sdvi|rally
ARTICLE

Addressing security standards for a new era with SOC 2 certification

BY CHRIS BRÄHLER

As our industry transitions from software and hardware to SaaS and consumption-based services, media organizations need new standards for identifying the cloud-based vendors that can guarantee the information security essential to their business.

Up to this point, media organizations largely have relied on ISO 27001 or the MPAA, which focus on security generally relating to on-premise systems. While work is underway to expand established security standards to address cloud services, the industry needs more.

Providers of SaaS or cloud-native services need a comprehensive framework by which to document their procedures and policies, and they need external auditing to validate that they are effectively following those procedures and policies. Media companies need a recognized auditing procedure that certifies third-party vendor compliance with (at the least) minimum requirements for information security in the cloud. They need to know that applications haven't just been lifted from the ground into the cloud without appropriate considerations for new and different security requirements.

Developed by the American Institute of CPAs (AICPA) as a framework for assessing a System of Organizational Controls (SOC), SOC 2 addresses all of these needs. Using the five Trust Service Principles" of security, availability, processing integrity, confidentiality, and privacy, this auditing standard defines criteria for managing customer data. Vendors who go through this auditing process must take a very close look at their operations and describe in detail the controls being implemented to address specific aspects of the applicable Trust Service Principles. Related to SDVI, its SOC 2 audit consists of roughly 60 pages of documentation, covering everything from internal security training for employees to process for change control to regular penetration testing and privacy controls.

After reading a SOC 2 report, a media organization can be certain that the vendor is meeting a baseline standard for information security. In addition to certifying the vendor's preparedness to handle data securely, the report simplifies the overall evaluation process for both the vendor and potential customer. It saves time and reduces friction for both parties.

For a media organization considering different vendors, the SOC 2 report signifies that information security is being addressed effectively by the vendor. Upon receiving the report, the organization's internal risk assessment team can confirm with confidence the providers commitment to security, knowing that noted details already have been certified by an independent third party.

Security is among the most common concerns of media organizations migrating to the cloud. While some of these concerns are legitimate, most stem from inexperience with cloud security or a lack of knowledge about how cloud-based services can actually improve an organization's overall security posture. With a vendor's certified SOC 2 report in hand, media organizations don't need to know everything about cloud security; they can be confident that they're doing business with an organization that already does.

For more information about SOC, visit:
www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html

Find out more about the benefits of media supply chain management and SDVI Rally at **www.sdvi.com**