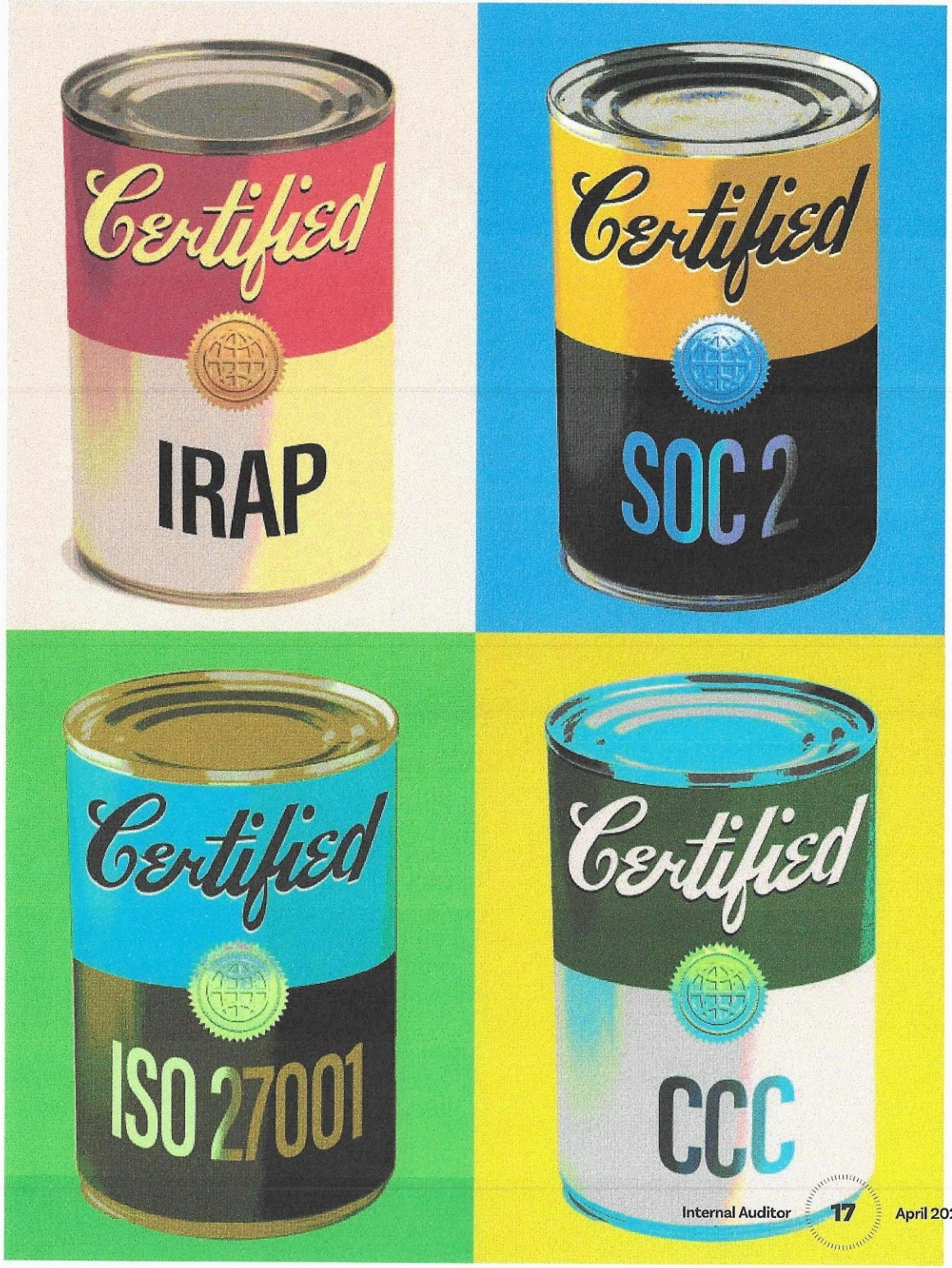

tech

Clear Cloud Compliance

Software services platforms can provide assurance to clients by integrating global data security standards into their operations.

Prashant Vadlamudi and Raymond W. Cheung

The number of cloud-based software-as-a-service providers has grown significantly, and so have the associated data security threats. Recent high-profile security breaches targeting companies such as T-Mobile and Uber, and a surge of ransomware attacks, have broken the trust business customers once had in hardware and software companies, before the cloud was everywhere.

These customers have become smarter concerning risks to their data and have increased scrutiny and compliance requirements for SaaS providers. They have good reason to be concerned. In 2022 alone, 48% of organizations were victims of ransomware attacks, according to The State of SaaS Ransomware Attack Preparedness report from data protection platform company Odaseva. Of the organizations that use SaaS platforms, about 52% had their enterprise defenses

penetrated — and only half of those organizations could fully recover all their data.

It is critical for organizations and vendors alike to implement controls that will minimize vulnerabilities for a ransomware attack and for internal auditors to assess the effectiveness of those controls. It is also why business customers increasingly expect SaaS providers to attain various certifications attesting to a sound approach to data confidentiality, integrity, and availability.

The Compliance Alphabet Soup

In assessing their SaaS vendor's security posture, organizations must make sense of the wide array of attestations and certifications in system and organizational controls. These range from Trust Services Criteria, or SOC 2, standards for data management compliance, to ISO 27001 for information security management, to the Payment Card Industry Data Security Standard. Other requirements and regulations include the Infosec Registered Assessors Program, Information System Security Management and Assessment Program, Cloud Cybersecurity Controls, and the European Cloud Code of Conduct.

Across the myriad controls laid out within these certifications and standards, there are many common attributes, such as annual cybersecurity training for employees, strong passwords that expire frequently, and restrictions on who in the organization is allowed to have administrator level accounts. Last year, Cisco compiled these commonalities into its Cloud Controls Framework, consisting of approximately 200 controls, on which cloud providers may build additional guidelines. Vendors such as Amazon, Microsoft, and Oracle have their own cloud security frameworks.

Baked-in Requirements

Many data security certifications, originally designed to comply with the U.S. Sarbanes-Oxley Act of 2002, continue to evolve. Initially, these certifications were viewed as "check-the-box" exercises. Over time, however, many companies realized the value of baking the requirements into their operations and making them central to how they do business.

Across the myriad controls laid out within these certifications and standards, there are many common attributes, such as annual cybersecurity training for employees, strong passwords that expire frequently, and restrictions on who in the organization is allowed to have administrator level accounts.

SaaS vendors should examine asset management controls and integrate the requirements of the certifications to their systems and personnel. Several certification frameworks have control requirements related to asset management and establish criteria for inventorying, monitoring, and managing an organization's assets.

A company that takes a cursory approach may satisfy auditors who are likely to observe a mere snapshot of what is in the cloud environment at a particular time. In contrast, a company with a more security-minded approach will go above and beyond the basic requirements, drilling into the asset inventory, carefully cataloging

all assets and identifying vulnerabilities. If the company determines that a security patch or update is needed, it already has a well-documented inventory, allowing it to more quickly evaluate who has been affected.

Imagine a Venn diagram in which one bubble represents security and another represents certification. The more security certification requirements are integrated into software practices and security tools, the greater the overlap.

Holistic Compliance

Cisco already is realizing the benefits of having a holistic compliance structure in place. A year ago, SOC 2 and ISO 27001 had not yet been implemented for the company's enterprise services division, which meant each cloud team had to individually demonstrate its enterprise services controls for each standard. By applying the CCF, the enterprise services were SOC 2 and ISO 27001 certified. Additionally, a shared control

AUDITING CLOUD VENDORS

With cloud vendors, internal auditors need to assess two areas:

1. What type of data backup and restoration does the vendor maintain and how robust is it?

2. What controls are being implemented to address trust within the vendor's organization? Is the customer looking to implement zero trust?

From here, the SaaS provider can share with the audit team the implementation solutions the vendor uses to protect itself. Combining the necessary controls and the industry-accepted certification standards will allow for a more in-depth defense strategy.

responsibility between the SaaS engineering teams and the enterprise services evolved. While the SaaS engineering teams focused on their set of controls, the enterprise services team could leverage the SOC 2 and ISO 27001 controls, which reduced the required effort and time.

The framework also has enabled expansion into new markets by shortening the path to achieving incremental certifications. In Australia, for example, Cisco products already in compliance with SOC 2 and ISO 27001 can more seamlessly achieve the country's IRAP certification.

Evolving With Automation

Any compliance framework must be designed to evolve alongside advancing technology and shifting security challenges. One of the best ways to build an agile and evolving framework is through automation.

The growing trend to address this evolution has been to add an automation layer to the application stack. The automation layer provides connections and reusable components that link applications and systems of records, as well as key governance, maintenance, and developer capabilities. This addition not only frees employees from manual and repetitive work, but also reduces the chance of human error and speeds up processes.

> Delivering a common set of services and technologies requires a ***new way of thinking, planning, engaging, staffing, operating, and automating.***

To secure management buy-in with automation, a best practice is to assess the organization's return on investment. This involves conducting due diligence surrounding the solution, what issues will be remediated, and the possible cost associated with continuing to work with the problem rather than fixing it. This assessment will give senior management the information necessary to make an informed decision on adding an automation layer to the application stack.

Automating controls can confer advantages and disadvantages. One advantage is that automation can reduce compliance strain on engineering teams, which typically bear responsibility for control implementation and maintenance. When controls are automated, engineers can spend their time on business-building initiatives, rather than compliance.

Another advantage is that automation converts the compliance monitoring process from a point-in-time check to a near-real-time activity. Manual monitoring could miss a compliance failure, elevating an organization's risk. Deploying artificial intelligence and machine learning to enable real-time monitoring can improve security and reduce risk.

One disadvantage of automating controls is that the solution would have to be compatible with the organization's security requirements. In addition, there may be challenges in knowledge transfer of the automated solution. For example, if the team is not prepared to thoroughly embrace the solution, shadow systems may be used instead, which could affect performance.

A Roadmap for Assurance

For SaaS providers, delivering a common set of services and technologies requires a new way of thinking, planning, engaging, staffing, operating, and automating. This is especially true when aiming for enterprisewide value and outcomes.

Cisco's CCF is an example of an approach to solving compliance issues centrally for all company products, enabling product teams to subscribe to a shared service stack. Having a common framework offers a roadmap for SaaS providers seeking to provide assurance to clients and auditors alike.

Prashant Vadlamudi, CIA, CISSP, CDPSE, CISA, is head of Global Cloud Compliance at Cisco in San Jose, Calif.

Raymond W. Cheung, CPA, CISA, CISM, CITP, is a partner at Crowe in San Francisco.