

Thriving in 2030: The future of compliance and risk management

By Travis Howerton

May 27, 2024

Disponible en: <https://www.securitymagazine.com/articles/100707-thriving-in-2030-the-future-of-compliance-and-risk-management>

In 2030, organizations of all sizes must expect the technology landscape to be dramatically different. As cloud-native applications take over, ephemeral technology will be a larger component of infrastructure, regulatory demands will increase and there will be a critical need for speed that many organizations are not currently prepared to meet. Understanding the future of compliance and risk management is essential for any organization aiming to thrive in the hyper-speed era ahead.

Prepare for evolving technologies

The past decade has seen profound changes in the technology landscape — containers revolutionized application deployment and Kubernetes emerged as the de facto standard for deploying and operating containerized applications. Microservices, containers and pods can all be created, destroyed and replaced as needed by Kubernetes, scaled automatically based on defined metrics that ensure the ephemeral workloads have the resources they need to function effectively. These ephemeral workloads improve scalability and efficiency, while also enabling faster deployment and improved reliability, but these benefits come with new compliance and risk considerations.

It can be difficult to know exactly what is running and where at any given time but that information may be needed to meet compliance and security requirements. Similarly, ephemeral technology requires organizations to rethink how and where critical data is stored. Traditional compliance and risk management approaches are dependent on a clear understanding of IT infrastructure and where data is located, but modern computing environments can make it challenging to track assets, enforce access controls and ensure data security. As organizations leverage cloud and ephemeral technologies more heavily, they must anticipate regulations catching up to address these challenges.

3 essential strategies to thrive in 2030

Even as the cloud poses new challenges, organizations can streamline compliance processes through automation capabilities and cultural changes.

1. Implement continuous controls monitoring and compliance as code

Continuous controls monitoring (CCM) is a technology-based approach that automates the process of monitoring and validating the effectiveness of internal controls within an organization. This represents a significant shift from traditional, sample-based testing methods, which relied on periodic audits or reviews of controls to evaluate whether they

were effective. Unfortunately, these methods represented only a moment in time, a metric that doesn't accurately reflect the state of controls in ephemeral environments.

CCM streamlines audits and outcomes by providing real-time assessment, analysis and reporting about an organization's security controls. This also makes it easier to comply with cyber incident disclosure mandates. Organizations that combine CCM with effective communication and reporting further enable stakeholders to make informed decisions regarding risk mitigation efforts, improving overall cybersecurity posture.

The National Institute of Standards and Technology (NIST) developed the Open Security Controls Assessment Language (OSCAL) to provide machine-readable representations of control catalogs, control baselines, system security plans and assessment plans and results. This standard is the US government's shift toward compliance as code, which enables compliance automation. By automating compliance processes, organizations can eliminate manual tasks, improving efficiency and reducing the risk of human error. And because compliance requirements are machine-readable, it's easier to integrate them into development and operations workflows, maintain audit trails and demonstrate compliance with regulations during audits. Compliance as code, together with CCM, enables organizations to deliver applications to market faster, secure in the knowledge that they are compliant.

2. Generate on-demand, audit-ready documentation

In ephemeral environments, where there is limited visibility as apps and services spin up and down quickly, traditional documentation simply isn't possible. CCM and compliance as code enable organizations to generate documentation on demand. This ensures that the documentation accurately reflects the state of the environment at the moment it is generated, reducing the risk of non-compliance and audit failures. In addition, auditors have access to the information they need for the point in time required, which streamlines the audit process and reduces disruptions and burdensome data calls. In today's complex environments, on-demand documentation is critical to maintaining compliance and security.

3. Create a unified security, risk, and compliance strategy

In the past, security, risk and compliance (GRC) efforts operated in silos, resulting in inefficiencies, inconsistencies, and limited visibility into risks across the organization. By creating a unified strategy that integrates these areas into a cohesive framework, organizations can improve both their security posture and risk management capabilities as well as streamline compliance. To do so, begin by defining the organization's security priorities, risk tolerance levels, and compliance requirements, setting goals for each area. While CCM, compliance as code, and on-demand documentation all enable this strategy, creating a culture that values communication and collaboration across security, risk, and compliance teams is vital to success.

Today's actions improve future outcomes

The move towards ephemeral environments and cloud computing presents challenges and opportunities for compliance and risk management. By embracing automation, focusing on continuous controls monitoring, compliance as code, on-demand documentation and a unified security, risk and compliance strategy, organizations can navigate this evolving landscape and ensure compliance in cloud, hybrid and on-premises environments. All the efforts organizations make today towards these goals will prepare them to thrive in 2030 and beyond.