UNISYS | Securing Your Tomorrow®

Many Highly Regulated Companies Have Made the Leap to the Cloud — You Can, Too

By Anupriya Ramraj

To achieve cloud-enabled agility, scalability and innovation, you must rethink and rework your approach to compliance and governance.

Businesses like defense contractors, financial services establishments and healthcare organizations that operate in highly regulated industries must meet stringent compliance requirements such as NIST, HIPAA, SOX, NYDFS, GDPR, etc.

Such entities have concerns that the cloud will adversely impact their ability to fulfill both government-imposed and corporate compliance obligations. A breach of sensitive data could be catastrophic, leading to lost credibility or declining revenue for the business; it could even impact national security. Such entities may think that the cloud is less secure and less regulated. This leads them to conclude that they may not be able to meet their strict standards in a cloud environment.

But businesses should know that compliance is not a cloud roadblock. Instead, their resistance to cloud adoption can probably best be classified as a mental block.

Many highly regulated companies have made the leap to the cloud. You can, too. Here's how:

Rethink and Rework Your Compliance and Governance

The cloud delivers agility, scalability and innovation. But to enjoy these benefits and remain compliant, you can't just carry over your legacy compliance and governance practices.

Legacy environments are hardware-oriented and highly manual. To deploy a new firewall, for example, a network engineer would typically go through procurement and change advisory boards, with the deployment and configuration process potentially spanning weeks.

But in cloud environments, everything is software-defined. As a result, they are highly dynamic, and things move much faster. For example, a firewall could be deployed and configured with a few clicks by a cloud engineer. With speed, there is more risk the firewall could be incorrectly configured and, left undetected, could lead to a security breach. If you don't have automation as part of your deployment and operations, you will be at risk.

Cloud security posture management is important, as 62% of breaches are caused by cloud misconfiguration, per a Cybersecurity Insiders report. Ensure that every layer of the stack adheres to security and compliance standards. The application and data layer are equally vulnerable, and there are specific requirements that apply. For example, you need to evaluate your cloud data store locations to meet GDPR compliance requirements. Or, you may have to pick one of the landing zones with stricter controls, which many cloud providers make available for government agencies and their partners (e.g., Azure Government).

Demonstrating compliance while being able to move quickly calls for controlled agility.

Anupriya Ramraj
Anupriya, Vice President, Cloud Solution Management for Unisys, has over 25 years of leadership experience in software engineering and product management. She is responsible for expanding Unisys' cloud portfolio and accelerating clients' cloud journeys, including migrations, security, operations, and cloud-native adoption.

Leverage the Power of Automation and Well-Architected Frameworks

Much has been written about the cloud talent gap, especially the acute skills shortage for cloud security specialists. We recently worked with a defense contractor that is subject to frequent audits by the military and has to adhere to NIST and FedRAMP standards. Finding someone who understands all the controls and who can use them to check your cloud configuration is a tall order. Leveraging mechanisms such as automated checklists and AI-enabled tooling for remediation allows you to be less dependent on human experts.

Embracing well-architected frameworks offered by cloud services organizations such as Amazon Web Services and Microsoft Azure can also help with reliability, performance and security. Ensure you and your provider well understand the parameters of the shared responsibility model in which you're working.

Embed Security and Compliance Into Every Aspect of Your Cloud Journey

Automate security and compliance and embed it in all aspects of your cloud journey.

DevSecOps is an example of embedding security early in the development life cycle. Ensure the validations performed as part of the life cycle include automated static and dynamic application code and infrastructure as code analysis.

Building a cloud training program for your IT staff is also a great way to strengthen your cloud security and compliance posture.

Embrace Controlled Agility

As cybersecurity challenges increase and concerns over cyberthreats and privacy continue to drive new regulations, governance and control have never been more important. To continue to be a credible and reliable company that earns and keeps the trust of your customers, you need to continually demonstrate that you're doing things in the right way with compliance.

But as a business, you can't simply stand still or just be reactive. You must increase your productivity, visibility and ability to make data-based decisions, and you must continue to evolve your strategy — and deliver innovative solutions fast to address ever-changing market dynamics.

These two seemingly opposing forces — demonstrating compliance while being able to move quickly — call for controlled agility.

With controlled agility, your business and its customers will benefit from agility while having the proper security guardrails in place to ensure compliance. Choosing a proven partner that can provide automation, cloud and cybersecurity solutions — and the guidance and support you need throughout your cloud journey — can help you make controlled agility a reality.

To explore how Unisys can help you achieve controlled agility, visit us online or contact us.

For more information visit www.unisys.com

10/21

21-0508