6 Key Considerations to Achieve Security and Compliance Readiness on AWS

Migrating to Amazon Web Services (AWS) is enabling organizations to expand their critical capabilities faster than ever before.

Since first launching in 2006, AWS has been an advocate for security and the customer role in the Shared Responsibility Model. While the delineation in responsibility is now clear – the complexities are not. The need for sound compliance practices and heightened security readiness are critical to maintaining business continuity.

At SMX, security is in our DNA. For more than a decade, we have been entrusted with designing, building, and running some of the world's most critical AWS workloads. Our proven methodologies for achieving security readiness are based on our 25+ years of experience supporting the Federal Government and Defense communities.

1. Understand Regulatory Requirements

Regulatory compliance requirements have a ripple effect across all aspects of an environment – from the tools selected and solutions built to the data and transactions flowing through an environment. Developing a deep understanding of these requirements, and the reasons behind them, is far more than a paperwork exercise for compliance organizations. Gaps in strategy and execution can lead to costly delays, devastating impacts, and great losses. Be prepared to dig into how a technical implementation will align to requirements and safeguard data. Start by decomposing requirements and mapping existing controls to the solutions, capabilities, and patterns that will support them. Adopting services like AWS Organizations, Control Tower, Config, CloudFormation, and CodePipeline are great ways to elevate capabilities.

2. Do Not Make Assumptions

The Shared Responsibility Model associated with operating workloads in AWS might expose gaps with existing policies, processes, and procedures that did not previously exist. New approaches to things like boundary management, connectivity, identity and access management, encryption, BC/DR, tenancy, and incident response require revisiting practices and account for the shifting mindset that needs to occur in the new model.

- Ensure there is clear separation of duties between those responsible for governance and compliance and those responsible for implementation and management
- Establish a clear, tool-based approval and exception process for waiving governance policies

The goal is to ensure capability coverage and solutions that meet each requirement and account for every piece of the overall puzzle. Security and compliance readiness is only as good as the sum of all parts.

Hope for the Best

Plan for the Worst

3. Design Toward "Well-Architected"

Designing a "Well-Architected" workload is no simple task and scaling those principles into enterprise strategies can seem daunting. Continue asking the question: Does the decision I am making today align to one of the core principles of a Well-Architected environment? Security solutions are only as good as the total strength of each pillar in the AWS Well-Architected Framework.

- **Operational Excellence through Observability:** Leverage AWS security services like CloudWatch, Security Hub, and Amazon Inspector to increase observability levels across infrastructure, environments, and applications
- **Security with Auditability:** Ensure compliance requirements can be successfully met and achieved through delivery of audit evidence and ideally supported by automated patterns and the use of services like AWS Audit Manager, Config, CloudTrail, and IAM
- **Cost Optimization in Security Service Selection:** Promote cost and resource efficiency within security solutions by evaluating on premises tools vs. cloud security services to reduce duplication of capabilities; reuse existing enterprise capabilities where it makes sense and where they align with the changing Shared Security Model—drive toward cloud-native for tightly integrated capabilities and increased cloud value over time

4. Build In Security - Do Not "Bolt On"

Security should be a conversation at each phase of a build and accounted for with every workload deployed. Develop an approach for building security into products, applications, and environments. Security should be an ingredient of a well-architected solution and not an afterthought.

- Implement controls in a layered approach to avoid dependency on any single control. This is commonly referred to as "defense-in depth" – an approach in which security controls are purposefully and thoughtfully layered across a network to protect the data and information within. For example, using Network ACLs provides an additional layer of ingress and egress traffic control across entire subnets within your VPC, while Security Groups act as a firewall protecting individual EC2 instances, or ENIs, and controlling traffic flows in a stateful manner.

5. Plan for Compromise

During a build, it is assumed that something will fail. It is equally important to "secure" assuming a compromise could happen. There is no such thing as a perfect state of security. New vulnerabilities, exploits, nation state attackers, supply chain attacks, and ransomware are emerging on a regular basis. An architecture, security controls, monitoring, and response processes should plan for an incident occurring. And when it does, all mitigations will be in place to handle the situation. Always design with an eye toward the real-world threats and manage operations with the same mindset.

- Developing a Data Classification Strategy that drives components of an operations plan is an important component. Ensure controls, solutions, and processes are in place to manage data, driven by use cases and cloud adoption models.

6. Develop a Security Guardrails Framework

Never stop innovating when it comes to security and do not be complacent with security solutions. The dynamic landscape of emerging cyber threats requires continuous development, delivery, and evolution of security guardrails and practices. Continually verifying and ensuring security measures are in place to broadly support every level of the organization – from Line of Business to application development teams. Elevate capabilities by integrating AWS-native capabilities into solutions. Innovative security services such as AWS Organizations and Service Control Policies, Amazon Detective, Inspector and GuardDuty, AWS Config, Shield, Security Hub, and Audit Manager are available to help achieve the control and confidence needed to run workloads on AWS.

For more information, please contact: solutions@smxtech.com

SMX harnesses the transformative power of technology to achieve mission success as a leader in digital and mission solutions, specializing in secure and advanced cloud, ISR, cyber, data analytics, engineering, space, and IT solutions. Operating in close proximity to our clients across the globe, the SMX team has a shared vision to deliver scalable and secure solutions to assure outcomes for the critical missions of our Government and commercial clients.

Learn more about our current contracting vehicles: www.smxtech.com/contracting-vehicles