Case Study
How Emagine IT’s Knowledge of Amazon Web Services Simplifies Compliance

Company Name: SOMOS Community Care
Business Type: Non-Profit
Service: Healthcare
Address: 519 8th Ave 14th fl, New York, NY 10018

Emagine IT Services

Emagine IT provides customers with the ability to consolidate their ISO 27001, FedRAMP, FISMA, NIST-Based Cybersecurity Frameworks, HITRUST, penetration testing, and privacy assessments or advisories under a single assessor or advisor, utilizing a coordinated team approach and an advanced purpose-built collaboration platform in order to decrease internal costs for clients.

As one of the top 3PAO’s, Emagine IT’s clients span industries from fintech, governments to healthcare, and over 50% of our clients utilize more than one service. Among those, Emagine IT has assessed and advised some of the most complex AWS-hosted federal and DoD deployments by FedRAMP, FISMA, and/or NIST-Framework Based CSPs.

SOMOS

SOMOS is a network of nearly 2,500 providers in the Bronx, Queens, Manhattan and Brooklyn who have come together to ensure better health care for Medicaid members. SOMOS is one of 25 networks across NY State that have been chosen to lead the statewide health care initiative. SOMOS is the only physician-led network. The goal of SOMOS is to bring you better care and to make it easier for you to stay healthy.
SOMOS was tasked on completing their NIST-based assessment for their AWS workloads by the State of New York and required a third-party assessor with knowledge of AWS to perform a full comprehensive assessment against all NIST 800-53 Moderate security controls.

Emagine IT through their automated and streamlined assessment process capability was able to swiftly prepare all assessment materials and prepare for the assessment whilst ensuring focus on customer data and common challenges found on AWS workloads, such as service misconfigurations, misunderstanding of the CRM, database scanning and more.

“Because of Emagine IT’s knowledge on AWS, we were able to expand on our knowledge and learn how to better secure our customers data”

Diana Estrella
Associate Director of Information Services & Security, SOMOS Community Care

**Challenges**

During the SOMOS assessment, EIT assessors were able to promptly identify standard AWS configurations which required further securing. Some of the key aspects to keep in mind with shared responsibility model:

- Always review the customer responsibility matrix (CRM), but don’t accept it at face value
- Understand that most CRM’s are left open-ended intentionally as compliance regimes are primarily risk-based
- Understanding inherited, shared, and owned controls are vital to deploying compliant workloads

**Actions**

“Emagine IT is one of the most professional firms we have had the pleasure to work with. EIT’s knowledge of AWS services and environment is exceptional.”

Thomas Marushak
Sr. Director of Information Services & Security, SOMOS Community Care

**Customer Responsibility**

**Inheritance**

Only very rarely will a entire control be fully inherited. Most of the times, controls are simply shared.

**Understanding the CRM**

Most Customer Responsibility Matrix (CRM’s) are left open-ended, this is done to give CSPs flexibility from a risk-based standpoint.

**Shared Controls**

Customers usually have the largest challenge with Shared Controls, such as who is responsible for implementation? Operations? Management? CRM’s are improving, but it’s ultimately the customers responsibility to ensure they fully understand their scope of responsibility.

**Future**

Going forward, SOMOS was not only able to better understand the Shared Responsibility Model and AWS Environment more effectively, SOMOS was quickly able to remediate misconfigurations, mitigate risks and successfully complete their assessment with a clean bill of health.

“Emagine IT leverages a custom streamlined and automated processes together to quickly identify AWS misconfigurations, common imprecise implementations to speed along assessments, advisories and technical testing.

**EIT & AWS Benefits**

- Significant experience with AWS Environments, all personnel are AWS Certified, ranging from Solutions Architect Professionals to Security Specialists.
- AWS trained professionals with deep understanding of AWS environments and core technology components
- Experience with significantly technical controls within FISMA, FedRAMP, and other NIST-based cybersecurity frameworks
- Comprehensive understanding of the shared security model
- EIT leverages a custom streamlined and automated processes together to quickly identify AWS misconfigurations, common imprecise implementations to speed along assessments, advisories and technical testing.