CUSTOMER CASE STUDY

How Iceberg Helped a Large Insurance Provider Stay CM-6 Compliant using NIST SP 800-53

Iceberg
Delivering Risk Intelligence

"As a company entrusted with delivering Medicare and/or Medicaid, rigorous adherence to NIST SP 800-53 is the best way to ensure adherence with CMS best practices.

And the most efficient and effective way to ensure that rigorous adherence is to work with a company like Iceberg Networks that can plan and evolve your configuration management system to match the threats it and changes it faces."

BACKGROUND

Since 1929 this organization has provided healthcare coverage to members, allowing them to live free of worry, and free of fear. This company offers a personalized approach to healthcare based on the needs of the communities where their members live and work. They work closely with hospitals and doctors in the communities they serve to provide quality, affordable healthcare, while providing nationwide healthcare coverage that opens doors for more than 107 million members in all 50 states, Washington, D.C., and Puerto Rico.

THE CHALLENGE

This large Insurance provider in the south eastern part of the USA offers individual and family, Medicare, vision, and dental insurance plan options. They needed a way to effectively and efficiently report on compliance to the CMS (Centers for Medicare & Medicaid Services) which requires periodic reporting to ensure members are compliant. The CMS requires its member agencies to manage their information security risks and provides its own set of recommended controls based on NIST SP 800-53. In the practice area of Configuration Management, specifically for the CM-6 control, CMS requires that member agencies demonstrate they are following best practices to securely configure their information technologies.

While CM-6 compliance is important to all CMS members, the ability to demonstrate the organization has effective measures to protect against a data breach by assembling all the evidence for a reporting package can be incredibly costly and inefficient. It is common to have an arduous CM-6 compliance process and in this instance, the organization undertook quarterly reviews which required approximately 75 people to be commandeered from other projects to complete the review. The reviews required a lot of spreadsheets as well as paper documents to be printed out, signed by hand, then scanned back into the system.

The manual processes of tracking through Excel, SharePoint and email were neither scalable nor efficient and such outdated methods were unable to provide clear visibility or a real-time view of critical information. As a result, the process offered little insight into the risks presented to the organization.

Iceberg Networks
Toll Free: 855-595-0808 • info@icebergnetworks.com
www.icebergnetworks.com

OUR SOLUTION

The insurance firm engaged Iceberg Networks to help them achieve continuous monitoring outcomes that would serve the business well. They needed to ensure the organization remains compliant and continues to maintain CMS best practices based on NIST SP 800-53. This client chose RSA Archer as the underlying technology to help them achieve compliance. Iceberg's role was to set up the program to ensure success.

All federal agencies are required to adhere to NIST SP 800-53 standards. And, although it may not be a regulatory requirement for businesses in the private sector to follow its guidelines, doing so demonstrates a company's credibility and readiness to shoulder the immense responsibility of safeguarding its clients' information. That immense level of responsibility is especially true for insurance companies who deliver Medicare and Medicaid services and wish to stay in-line with CMS best practices. Such companies are asking to be entrusted with their clients' most sensitive and personal information. A willingness to not only adhere to but remain current with NIST SP 800-53 standards must be a cornerstone of the business' governing principles – and Iceberg provided the expertise and know how to support this.

THE RESULTS

After a 6-month engagement with Iceberg the organization realized many benefits including streamlined and efficient reporting for CM-6 compliance and a maturing configuration management process. This resulted in:

A More Efficient, Scalable Solution

- They were able to manage millions of configuration items across multiple devices through an automated system leveraging a relational database to handle and filter the items.
- The new method allowed the organization to avoid the quarterly surges in resource requirements and create a smaller, dedicated team to manage the compliance.

Minimized Risk of Misconfiguration

- Ensured the right controls were in place to prevent a vulnerability from being exploited into a breach.
- Automated configuration management to filter prioritized items, allowing to remediate top priorities quickly.

Visibility

- Automation and reporting helped to contextualize the threat landscape to prioritize remediation efforts and communicate those risks to executives.
- The executives needed to know their digital environment was safe. Leveraging automation and reporting in the solution helped to contextualize the threat landscape (as it relates to security configuration management) to ensure priority and communication of remediation efforts.

Minimizing the Need for Escalation

- Automating the compliance of security configuration management in a solution helped to manage internal Service Level Agreements while minimizing the costly need for approval escalation (due to SLAs not being met).

Iceberg helped this organization stay current with security configuration while remaining compliant with NIST SP 800-53. Iceberg ensured the organization would remain compliant and continue to demonstrate CMS best practices through automation and configuration.

As a company entrusted with delivering Medicare and/or Medicaid services, rigorous adherence to NIST SP 800-53 ensures organizations stay in line with CMS best practices. And the most efficient and effective way to ensure that rigorous adherence is to work with a company that can guarantee your information security system will evolve to match the threats it faces.

ABOUT ICEBERG

Iceberg Networks plans, deploys, and manages successful programs for Integrated Risk Management (IRM). By providing trusted, aggregated, and transparent risk intelligence, organizations can make more confident and effective business decisions.

Icebergs' team of experienced management consultants, subject matter experts and software developers offer a full lifecycle of IRM related professional services including executive management workshops, strategy sessions, implementation & integration, and support services.

Iceberg Networks is head-quartered in Ottawa, Canada with offices throughout North America. Our core values are Honesty, Approachable, Accountable, Pursuit of Excellence, Collaborative, and Empathetic.

Iceberg Networks
Toll Free: 855-595-0808 • info@icebergnetworks.com
www.icebergnetworks.com