FLANK

PROTECTING YOUR PERIMETER

CASE STUDY: FIMSA

HOW FLANK HELPED WITH FISMA COMPLIANCE

FOR A MAJOR CLINICAL RESEARCH COMPANY IN NORTH AMERICA

FLANK
PROTECTING YOUR PERIMETER

GOAL

Assist a major clinical research company (client) based in North America to become compliant with the **Federal Information Security Modernization Act (FISMA)** as required for reporting to the **Department of Health and Human Services (HHS) – National Institutes of Health (NIS) division.** Additionally, FISMA compliance, which includes the issuance of an official Security Assessment Report (SAR) would be highly valuable in attracting additional business from other federal agencies and private sector companies.

Challenges & Needs:

The client had no prior experience with federal compliance reporting, along with never having performed any type of meaningful compliance assessment. Their last assessment was a SAS 70 audit performed in 2007, which only covered a specific I.T. function within their broader information security platform.

Additional Challenges Included the Following:

- **NO COMPLIANCE CULTURE:** Other than performing a SAS 70 audit years ago (which is now an extremely antiquated auditing framework), the client had no real compliance culture. They had no experience in identifying, scoping, and assessing their compliance needs for FISMA.

- **MISSING INFOSEC POLICIES AND PROCEDURES:** A mixture of information security policies and procedures were in place, but they were old, poorly written, could not be mapped to the current FISMA framework, which is based on NIST SP 800-53. Additionally, a lack of interest was exhibited by subject matter experts who were charged with the task of re-writing and developing new information security policies.

- **WEAK INTERNAL CONTROLS RELATING TO CORE FISMA REQUIREMENTS:** Notable gaps and deficiencies existed with the client's internal controls when mapped against the prescriptive requirements found within NIST SP 800-53.

- **LACK OF TECHNICAL UNDERSTANDING OF CRITICAL COMPLIANCE TOOLS & SOLUTIONS:** With the NIST SP 800-53 controls requiring an enormous number of technical tools to be procured and implemented, the client needed help! Specifically, they needed answers to their following questions: (1). What tools did they need and why? (2). Who were the top, reputable vendors? (3). What were the costs and implementation time-frames?

- **LACK OF PROJECT MANAGEMENT EXPERIENCE:** The client felt overwhelmed with the amount of work that had to be done, and was having extreme difficulties in putting together a project management plan that was scalable and accurate. They needed a trusted provider with toolsets for monitoring the entire FISMA process from beginning to end. They also needed accountability for personnel that were not delivering for the project.

FLANK
PROTECTING YOUR PERIMETER

OUR SOLUTION

FLANK brought in a team of **dedicated federal compliance experts with years of FISMA experience**; personnel with a wide-range of capabilities for solving the clients needs. Within the first two weeks of the engagement, FLANK implemented a **"battle plan" for FISMA success**, which included the following measures:

- Successfully defined project scope and client participation.
- Identified all control gaps and recommendations for remediation.
- Set up demo web sessions with software vendors for critical security tools.
- Completely reviewed all InfoSec documentation and began authoring new policies & procedures.
- Established contact and working relationships with all in-scope third-party vendors (i.e., managed security services providers)

Challenges Solved:

- Implementation of a true compliance framework.
- Complete development of all Required information security policies and procedures.
- Successful remediation of all in-scope required controls.
- Security Assessment Report (SAR) and System Security Plan (SSP) issued to client, allowing them to showcase compliance to the Department of Health and Human Services (HHS) – National Institutes of Health (NIS) division.

Value Created:

- A "Security First Mindset" where personnel take information security seriously, and now have the tools and resources for protecting organizational assets.
- Implementation of a mature compliance framework where personnel are aware of roles & responsibilities.
- The ability to successfully obtain additional federal & private sector contracts with FISMA compliance.

Contact us Today for More Information **Phone**: 1-800-203-1643 **Email:** info@flank.org