University Strengthens IT Security through FISMA Assessment

Customer Case Study

University of Texas Health Science Center receives $44 million in research contracts with help of Cisco Services.

EXECUTIVE SUMMARY

University of Texas Health Science Center at San Antonio

- Healthcare
- San Antonio, Texas
- 5076 employees

Business Challenge:

- Comply with FISMA as required by new externally-funded research projects
- Gain better understanding of what FISMA compliance entails
- Learn best practices for improving research-specific operational security

Network Solution:

- Cisco FISMA Risk Assessment Service brings knowledge and expertise for compliance
- Detailed assessment of security and risk controls identifies areas for improvement
- Assessment documentation developed for funding agency

Business Results:

- Received approval to move forward with multimillion dollar research projects
- Simplified compliance for future projects with reusable assessment template
- Improved overall IT security by addressing deficiencies identified during assessment

Business Challenge

Founded in 1959, the University of Texas Health Science Center at San Antonio is one of the nation’s leading health science universities, having produced approximately 26,000 graduates in the fields of medicine, nursing, dentistry, health professions, and biomedical sciences. With a strong focus on biomedical education and research, the school ranks in the top three percent of institutions worldwide receiving National Institutes of Health funding.

As the director of research systems and technology within the office of the vice president for research, Sara Boettcher, PhD, is responsible for facilitating compliance for research-related activities. “Before starting any new project, researchers have to go through various levels of approvals to meet federal regulations,” she says. “My role is focused on implementing technology systems to refine and optimize that approval process.”

The Federal Information Security Management Act (FISMA) is one such federal regulation. Although Boettcher and her colleagues were well aware of the law’s existence, it was not until the university was awarded a certain federally-funded research contract that they needed to address the issue. “Because FISMA compliance was never required in any of our previous research projects, it was always just looming there in the background as this vague, nebulous concept that none of us really understood,” says Boettcher.

FISMA compliance was required for this contract, however, as it was for a 20-year-long National Children’s Study where the university would collect data on children from the time they were infants until they were young adults. If the university did not meet FISMA regulations, it would lose the opportunity to conduct the study. “We heard nothing but horror stories about how compliance would cost us millions of dollars,” says William Sanns, faculty associate and director of information systems in the department of epidemiology and biostatistics at the UT Health Science Center.

> "Thanks to the Cisco FISMA General Risk Assessment Service, we now have a clear understanding of how to address compliance issues as it relates to our security operations. And more importantly, we can re-use that information across future projects that also require FISMA compliance."

Sara Boettcher, PhD
Director of Research Systems and Technology,
Office of the Vice President for Research
University of Texas Health Science Center

"From armed guards to 24-hour security, we were under the impression that it would require extreme measures."

To add urgency to the issue, the university was awarded two more research contracts that also required FISMA compliance. Boettcher and Sanns needed to act fast.

Network Solution

With contract deadlines quickly approaching, and no in-house experience or expertise with FISMA assessments, the research compliance team at UT Health Science Center decided to look for external assistance.

Boettcher had worked with Cisco Services in the past, and was familiar with the breadth of specialty services Cisco provides. To her and Sanns' relief, they found just the solution they were looking for: the Cisco FISMA General Risk Assessment Service. "After we explained our initial needs, the Cisco Services team responded immediately," says Sanns. "They knew exactly what FISMA compliance entailed, and what needed to be done in order for us to address the research contract's specific requirements. We were very impressed, and knew right then that we were in good hands."

Within a few weeks, a Cisco FISMA expert was onsite to interview various IT contacts, who could provide insight into the university's research-related operational security practices. During this initial phase of the assessment, Boettcher and Sanns learned that meeting FISMA compliance would not be such a daunting task after all. "We figured compliance would be all encompassing," says Boettcher. "But our Cisco Services FISMA expert explained to us that compliance only had to be on a project-by-project basis. We primarily needed to make operational adjustments to facilitate those specific projects."

Throughout the course of Cisco's FISMA assessment, the UT Health Science Center team continued to gain a better understanding of what compliance entailed, learning how FISMA related to other regulatory standards and how those fit into the university's IT operations as well. With a complete set of assessment methods and procedures established to evaluate the FISMA security controls, the Cisco Services consultant made speedy progress in assessing the university's security infrastructure. He then compiled his findings into a detailed, submission-ready assessment report, which identified both security gaps and areas for improvement, as well as recommended approaches to resolving those issues.

"We submitted the report to the agencies, showing them that while we may have areas that fall short, we are proactively addressing those issues with these specific measures," says Sanns. "For the agencies, I think having the Cisco name associated with our report added credibility and reassurance that we knew what we were doing."

Business Results

With Cisco's FISMA compliance report completed and submitted, it didn't take long for the UT Health Science Center to receive the three words they had been waiting for: authority to operate. The immediate benefit of the university's engagement with Cisco was that they were granted approval to proceed with these new research studies, which combined, equated to more than US$44 million worth of funding. However, the advantages of Cisco's FISMA General Risk Assessment extend beyond the scope of those specific projects.

For one, the university now has a methodology and documentation template to work from when future FISMA compliance-required projects come in. "Thanks to the Cisco FISMA General Risk Assessment Service, we now have a clear understanding of how to address compliance issues as it relates to our security operations," says Boettcher. "And more importantly, we can re-use that information across future projects that require FISMA compliance as well, which will eventually be everything with a federal contract."

The UT Health Science Center can also apply the best practices learned from the Cisco FISMA risk assessment to other IT operations as well. "I think this was a great learning opportunity for our IT team in general," says Boettcher. "The engagement will help us further refine and improve research security."

A longtime user of Cisco IP phones and networking equipment, the UT Health Science Center staff had always known that Cisco was a vendor that it could rely on for technical products and solutions. But with the successful assessment of the university's operational security, the research compliance team can now look to Cisco as a strategic partner in improving overall IT security moving forward. "Because at the end of the day, it's really about protecting information and mitigating risk," says Sanns. "And now that we have the best practices and methodology to optimize our institutional security, I can definitely say it's helping me sleep better at night."

Next Steps

With an IT security improvement strategy now firmly established, the UT Health Science Center plans to bring in Cisco Services for follow-up on the assessment in the near future. "Although we received an initial green light to move ahead with our research projects, we have to demonstrate our progress in security enhancement every few years," says Boettcher. "With Cisco, we know we'll have a trusted vendor to help us conduct an ongoing assessment throughout the project lifecycle."

For More Information

To learn more about Cisco's FISMA General Risk Assessment Service, visit: www.cisco.com/web/strategy/government/fisma.html.

Product List

- Cisco IP Telephony
- Cisco Routing and Switching

Services List

- Cisco FISMA General Risk Assessment

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.