Building ISO 27001 Certified Information Security Programs

Last reviewed: August 2017

Case Study

Designing and maintaining an ISO/IEC 27001 certified Information Security Management System (ISMS)

Background

The University of Tampa achieved its first-ever ISO/IEC 27001:2013 certification in 2015. The current organizations participating—known as the *scope* of the information security management system—are Information Technology & Security, Human Resources, and the academic Cyber-Security lab infrastructure. There are future plans to incrementally increase the scope to include additional university organizations. Companies like Workday, Cisco, Microsoft, and others (especially cloud providers) also certify their information security programs against the ISO 27001 and new 27018 standards to demonstrate their commitment to data security and effective information security practices and controls.

The University of Tampa must undergo annual surveillance audits and re-certify their ***ISO 27001*** information security management system (ISMS) every three years. ITS is also currently preparing for the first ***ISO 22301*** certification of the university's business continuity management system (BCMS) in 2018-2019, as well as in the early stages of designing a certifiable ***ISO 20000*** service management system (SMS). ISO 22301 and ISO 20000 are compatible standards to ISO 27001 that assist enterprise technology and security organizations in developing effective and mature business processes, with well-defined strategic and tactical goals and operations.

- ***ISO 27001*** provides the requirements for building a robust and effective information security management system (ISMS) and is compatible with other major standards and requirements, such as NIST, the federal Cybersecurity Framework, PCI, and HIPAA.
- ***ISO 22301*** provides a framework to plan, establish, implement, operate, monitor, review, maintain, and continually improve a business continuity management system (BCMS). It is expected to help organizations protect against, prepare for, respond to, and recover when disruptive incidents may occur.
- ***ISO 20000*** specifies requirements for technology and security service providers to plan, establish, implement, operate, monitor, review, maintain, and improve an SMS. The requirements include the design, transition, delivery, and improvement of services to fulfill agreed-upon service requirements.

Description

The University of Tampa is a medium-sized, private liberal arts and business oriented institution that has been in a pronounced period of growth in enrollments, facilities construction, addition of key majors and degrees in cybersecurity and other business areas, automating business and academic processes, and improving data protection. Dr. Ronald Vaughn has served as President of UT since the mid 1990's and is very involved in promoting excellent data security practices, as are the rest of the senior staff at UT. This has led to a large amount of progress in a very short time period.

Tammy Clark serves as the university's chief information officer and chief information security officer, is a member of the president's senior staff group, and reports directly to Dr. Vaughn. She developed the university's information security program from the ground floor starting in mid-2012. Throughout 2016, she re-engineered and combined various technical organizations at the university into the Information Technology & Security organization, with four key areas underneath it: Enterprise Solutions, Information Security, Information Technology Operations, and the Project Management Office. This also involved realigning staff roles and responsibilities, as well as including data security accountabilities in every ITS staff members' job description and annual evaluations.

UT's information security program was standardized from the start around ISO/IEC 27000, a series of popular international information security standards that provide recommended practices and requirements for establishing effective information security programs, since 2012. These standards are compatible with NIST, HIPAA, PCI DSS, and many other industry guidelines and requirements. Organizations are certified ISO/IEC 27001:2013 compliant. This standard provides requirements for developing and improving an ISMS. ISO/IEC 27002:2013, a standard that provides recommendations pertaining to security controls that reduce information security risks, was applied across the university to assist with elevating security awareness, promoting data protection, and prioritizing information security risks and controls.

A few examples of how university executives support and assist with maintaining an effective ISMS:

- Annual risk management and data protection assessments are conducted with every administrative department on campus, including multiple academic areas.
- Contracts and procurements for technology related solutions or equipment are not processed by the CFO's area unless they have undergone security and vendor reviews that are satisfactory (i.e., don't introduce unacceptable risks or vulnerabilities).
- The use of multifactor authentication is being incrementally embraced (e.g., MFA is required for off campus use of key enterprise applications or privileged access).
- Security awareness education is required at UT. All staff and faculty members, including third-party service providers situated at UT, are required to complete SANS Securing the Human online training modules pertaining to their particular roles and responsibilities; they must also read and acknowledge UT's Acceptable Use Policy.
- Student security awareness ambassadors staff a program for students, SpartanSecure, and Residence Life staff involve information security team members in all student orientations and meetings with student leaders on campus.

Preparation for ISO 27001 Certification: The Information Security team works extensively with organizations in the ISMS scope in conducting controls gap assessments (ISO/IEC 27002), educational sessions on ISO 27001 requirements, and over 12 audit preparation sessions. Each audit participant receives an "ISO 27001 Prep Kit" that identifies key information about the information security management system and certification audits.

An extensive ISMS electronic manual was prepared that outlines how all ISO 27001 requirements (including 114 appendix A controls) are (effectively) met. The manual also contains required documentation such as:

- Strategic and tactical security plans
- Descriptions of risk management and risk treatment planning and methodologies
- Management reviews of the ISMS that included UT's president
- Risk assessment and risk treatment reports

- Status on corrective actions resulting from risks assessments and internal audits of the ISMS
- Descriptions of continuous improvements that will be made to ensure the effectiveness of the ISMS going forward

Benefits

Standardizing management of UT's information security program around the ISO 27000 family of standards ensures that decisions are made in a strategic and measured fashion and are closely aligned with business and academic goals, as well as the university's objectives.

ISO 27000 is a business-centric standard that provides guidance in developing key initiatives that resonate with university business and academic leaders, rather than taking an IT-centric approach that minimizes their participation. The approach is also holistic and comprehensive, taking into account people, process, and technology issues and considerations.

Human resources and ITS made numerous improvements in documenting and implementing controls and key processes. Staff became more intentional about ensuring their practices were targeted at safeguarding data. Many of the changes they made were practical (e.g., to customize applications of recommended controls in the ISO standards), where previously decisions were more ad hoc or based on convenience.

Why did we decide to become ISO/IEC 27001:2013 certified, and what will happen in the future?

UT's president fully supports this endeavor and promotes it campus-wide and to the board of trustees, as evidence of due diligence and the strong commitment to manage a comprehensive, cost-effective, risk management based information security program. UT's information security program integrates business and academic goals and objectives that matter to key university stakeholders. Business and academic leaders appreciate collaborative efforts to make data security improvements that often result in more efficient processes in business areas, as well. Many university departments are retaining the services of cloud software-as-a-service (SaaS) providers, and information security policies require that all university organizations work with ITS in evaluating their proposed vendor contracts, SLAs, security controls, audits, PCI compliance, etc.

Shortcomings

- This effort can be time-consuming—undertaking the compliance effort can be university-wide, but the initial certification scope needs to be carefully considered.
- If information security organizations take a "do it yourself" approach or try to "bite off more than they can chew" upfront, they may not be successful.
- The ISO standards are not free of charge and have licensing restrictions. There are also costs associated with becoming ISO 27001 certified.
- Institutions that have research areas requiring compliance with federal regulations (e.g., NIST, FISMA) will need to align both sets of requirements (ISO 27000/NIST and/or FISMA). Many areas of these standards map against each other but also have distinct variances in their approach to risk management and data security.

Implementation Challenges

At the beginning, it was a somewhat daunting journey, as the information security program was under development and the legacy IT organization did not have much in the way of documentation or a comprehensive approach to security controls. Information security partnered with a newly-created project management office to provide a structured approach, which allowed ITS leaders to integrate ISO 27001 documentation and controls requirements within their areas during predefined time periods spread out over two years.

Future Plans

As mentioned earlier in this case study, there are plans to certify against two additional ISO standards, and an ongoing commitment to retaining the ISO 27001 certification. President Vaughn feels that in addition to obvious benefits that can be gained, retaining this certification also provides UT with a competitive edge in an era of numerous information security and technology related disruptions, problems, and uncertainties across every sector in our society.

References

- Security Program Development
- Developing a Risk-Based Information Security Program (2007 PowerPoint presentation)

Return on Investment

Since the information security program's humble beginnings in late 2012, many improvements have been made across the university, resulting in a security-aware culture. Additionally, the IT organization has closed many security gaps that were present between 2012 and 2014. UT's president has provided his full support behind the information security program to expand and continue with ISO/IEC 27001 certification in the future. The university’s data protection capabilities have risen exponentially. And additional information security solutions put in place to protect the university's community against key threats – such as phishing – have been very successful in lowering the amount of incidents experienced at UT.

Replicable

5 (on a scale of 1 to 5, where 5 is Highly Replicable)

Effectiveness

5 (on a scale of 1 to 5, where 5 is Highly Effective)

Category

- Security Program Development

Submitted By

Tammy Clark, Chief Information Officer, University of Tampa

❓ Questions or comments? ℹ Contact us.

⚠ *Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).*