Information Security Governance:
Standardizing the Practice of Information Security

Tammy L. Clark, Georgia State University
Toby D. Sitko, EDUCAUSE Center for Applied Research
By now, colleges and universities understand that the security of their information assets is among their highest priorities in terms of risk and liabilities, business continuity, and protection of their reputations as responsible stewards of private and public information. Information assets include, and are not limited to, student and personnel records, health and financial information, research data, teaching and learning materials, and all restricted and unrestricted electronic library materials. If keeping information secure has such high stakes, then the policies and practices of information security must be carefully governed. Given the complexities of building and maintaining secure systems that make the right information available to the right people at the right times while keeping the same information off-limits to others, it is no wonder that the governance of this domain has become an important discipline of its own.

In the world of financial accounting, Generally Accepted Accounting Principles (GAAP) serves as the standard framework of guidelines. In contrast, the information security field has not yet adopted a consistent set of guidelines. Practitioners are free to pick and choose from a selection of frameworks based on information technology (IT) process improvement, controls, risk management, and common criteria and recommended best practices to ensure “CIA” (confidentiality, integrity, and availability).

This research bulletin discusses the trend to use a variety of risk management and process improvement frameworks and standards to create an information security program that is sufficiently comprehensive and effective for colleges and universities. Prevalent standards in use at this time include the Control Objectives for Information and related Technology (CobiT) IT control framework, the Information Technology Infrastructure Library (ITIL) v.3 service management framework, National Institute of Standards and Technology (NIST) Special Publications 800 Series, and the set of information control objectives commonly referred to as ISO 27000.

Specifically, the process of implementing the ISO 27000 framework at Georgia State University (GSU) is discussed. In addition, this bulletin provides a rationale for an information security governance framework that enables executives to better assess the degree to which their information security programs are effective in handling risks and perceived threats to confidential data, aligning information security goals with institutional academic and business objectives, and ensuring these programs are continuously improving over time.
In 2004, the Corporate Governance Task Force of the National Cyber Security Partnership issued a report called “Information Security Governance: A Call to Action.”1 A subcommittee of this task force was established to evaluate the information security governance framework for educational institutions and nonprofit organizations. The subcommittee concluded that the framework and accompanying Information Security Governance Assessment Tool2 originally developed for the corporate sector were valid and provided a good starting point for education and the nonprofit sector. The assessment tool is intended to help institutions of higher education determine the extent to which they have implemented a governance framework for information security. It is also designed to identify information security concerns under the broad areas of risk assessment, people, processes, and technology.3

Many higher education information security programs are currently embedded within IT departments rather than having reporting relationships similar to that of the comptroller, internal auditors, legal affairs, or risk or emergency management directors, all of which typically align with or report to the chief institutional executive.

University information security programs are charged with protecting institutional assets and data subject to a myriad of regulatory controls and increasing levels of risk. This responsibility carries the additional burden of handling the repercussions and public scrutiny stemming from breaches, compromises, or unauthorized access to financial data (credit card numbers, bank accounts) or student/faculty/staff personally identifiable information (Social Security numbers). As if that were not enough, information security programs must also cope with the fallout from disruptions in services provided (online registration, self-service websites, online courseware, or e-commerce sites).

How do college and university leaders become involved with these programs? How do they evaluate the effectiveness and efficiency of processes and controls in place, given that the practice of information security is not yet uniformly standardized and performance measurements are not clearly defined?

Information Security Challenges

The probability and impact of realized threats and damage to the confidentiality, integrity, and availability of data repositories and IT assets have never been higher. The costs of suffering a breach are also escalating, as institutions are required to expend large amounts for notification and credit-protection coverage for those affected by breaches and to pay fines and litigation costs/penalties. Despite all the publicity about high-profile data breaches, claims of copyright infringements, and insidious viruses and malware, amazingly, there is still a perception that information security is an IT problem rather than everyone’s business. Until we understand the critical role that the institution’s
executive leaders play in positioning information security programs for success or failure, little will be done to overcome these challenges.

For many reasons, implementing an information security governance framework can significantly enhance an institution’s ability to operate an effective and robust information security program. Information security governance frameworks integrate well with ITIL and other IT governance models used to improve business processes; provide a means for executives to define and control the costs of providing services; and in so doing, markedly increase customer satisfaction.

Key points to consider:

- Information security frameworks, such as the ISO 27000 series of standards, promote a cost-effective, risk-management-based approach that assists top management in evaluating costs and prioritizing the implementation of necessary controls.

- A top-down approach that includes the active involvement of university executive leaders, as well as the oversight of auditors and attorneys, is critical to the success of information security governance programs.

- A focus on improving business processes; inserting controls; analyzing gaps related to measuring, prioritizing, and handling risks and compliance requirements; and developing corrective and preventive action plans will yield an effective approach to demonstrating due diligence in protecting confidential and sensitive data.

- Implementing an information security governance model involves taking a proactive, strategic, and measured approach that is more effective in the long run than the reactive, threat-based approach currently used by many colleges and universities.

- Information security has traditionally been viewed as a function of IT rather than an integral part of the core business functions of the institution, and business and IT executives alike will benefit from greater understanding and involvement in their information security programs.

- Many university executives are in the position of having to do more with less in terms of funding and staffing IT and information security functions. An advantage of most information security governance models is that an institution, regardless of size or budgets, can implement controls and improvements to its information security posture incrementally over time, using available resources.

- Compliance with legislative, fiduciary, and institutional policy requirements is always a challenge for university presidents. An information security governance framework assists with managing the complex regulatory landscape and builds a cooperative and mutually beneficial partnership between information security staffs and key stakeholders such as IT auditors and attorneys.
Standards and Terms Defined

The world of information security is complex, not solely because of governance and technology considerations, but also because information security practitioners must understand how to select relevant controls and requirements from a diverse set of information security standards and guidelines. To help keep track of these standards and guidelines, following is a set of definitions that will be used within this research bulletin:

**COBIT:** Created by the Information Systems Audit and Control Association (ISACA), Control Objectives for Information and related Technology (COBIT) is a major information security governance model that provides a set of generally accepted measures, indicators, processes, and best practices for the use, governance, and control of information technology. See [http://www.isaca.org/Template.cfm?Section=COBIT6](http://www.isaca.org/Template.cfm?Section=COBIT6).

**COSO:** The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a major information security governance model that was established in 1985 to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems. See [http://www.coso.org/](http://www.coso.org/).

**FISMA:** The Federal Information Security Management Act (FISMA) implementation project of NIST (see below) is a major information security governance model. FISMA imposes mandatory processes that must be followed for all information systems used or operated by a U.S. federal agency or by a contractor or other organization on behalf of a U.S. government agency. See [http://csrc.nist.gov/groups/SMA/fisma/index.html](http://csrc.nist.gov/groups/SMA/fisma/index.html).

**ISMS:** An Information Security Management System (ISMS) is a system of management concerned with information security. It includes mechanisms to design, implement, review, measure, and maintain processes and systems that ensure the confidentiality, integrity, and availability of information assets while striving to minimize information security risks. See [http://en.wikipedia.org/wiki/Information_security_management_system](http://en.wikipedia.org/wiki/Information_security_management_system).

**ISO 27001:** Published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the ISO 27001 standard is a major information security governance model that outlines the requirements to design and implement an ISMS. The full name is ISO/IEC 27001:2005–Information technology–Security techniques–Information security management systems–Requirements. ISO 27001, which describes “shall do’s,” is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. Organizations can become certified against this standard by accredited ISO 27001 registrars. Modeling an information security governance program using this standard will provide organizations with an auditable, measurable, and comprehensive framework that promotes strategic planning and continuous improvements. See [http://www.iso.org/iso/catalogue_detail?csnumber=42103](http://www.iso.org/iso/catalogue_detail?csnumber=42103).
ISO 27002: An ISO standard last modified in October 2005 by the ISO and the IEC, ISO 27002 is the common name for a comprehensive set of best practices used in establishing and managing an ISMS. Renumbered as ISO 27002 in July 2007, the full name is ISO/IEC 27002:2005–Information technology–Security techniques–Code of practice for information security management. ISO 27002, which describes “should do’s,” establishes guidelines and general principles for initiating, planning, implementing, maintaining, and improving information security management in an organization. The 36 control objectives and 133 controls outlined provide general guidance on the commonly accepted goals of information security management. Organizations can become compliant with this standard, but certification requires that they incorporate the requirements outlined in ISO 27001. See http://www.iso.org/iso/catalogue_detail?csnumber=50297.

ITIL: The Information Technology Infrastructure Library (ITIL) is a set of concepts and techniques for managing information technology infrastructure, development, and operations. See http://www.itil-officialsite.com/.

NIST: The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The mission of NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life. See http://www.nist.gov/.

Information Security at Georgia State University

Georgia State University (GSU), located in the heart of downtown Atlanta, is the second largest university in Georgia, with a population of approximately 27,000 students. The university’s IT environment is a federated model in which the central IT organization provides key products and services to the university community, while individual colleges and departments manage their own IT resources and projects. The information security program is a unit within the central IT organization and reports to the CIO.

In the early stages of the GSU information security program (2000–2004), a myriad of initiatives, technologies, security-awareness endeavors, risk-management methods, and incident-response measures were introduced to the institution. The program evolved from reactive mode—chasing the threats and problems—to a proactive program of managing information security, reducing large-scale incidents, and taking preventive and corrective actions. In September 2004, GSU began aligning its security plan with ISO 27002 (formerly ISO 17799), the Code of Practice for Information Security Management, which lists 36 control objectives and recommends a comprehensive range of specific security controls (133 separate controls).

By assessing the control objectives against the information security measures currently in place, and by ensuring that GSU was continuously evaluating and handling risks and threats, GSU raised the overall awareness and participation of central IT and departmental staffs in implementing effective threat countermeasures and devoted substantial effort toward improving the university’s information security posture.
During this period, the GSU president approved a security review policy, and the CIO implemented an IT Procurement Review (ITPR) process that requires security reviews on IT projects that cost $5,000 or more. This process enables the information security team to recommend controls and reengineer business processes in the early stages of IT projects, to ensure that unacceptable risks are effectively eliminated. Over time, the business and academic executives at GSU have begun to realize the value of these security reviews and the increased ability of the institution to protect confidential data. As a result, the information security program is increasingly viewed as a key business partner/enabler, and security reviews and awareness training are routinely requested by departments at GSU.

In 2007, GSU’s CIO championed an initiative to get two areas of GSU certified under the ISO 27001 standard. The university became one of the first in the nation to achieve this international designation when both the information security program and a financial business unit at the university were certified by registrar BSI Management Systems in March 2008.5

Strategic planning ensures that GSU information security program objectives are met in a consistent, measurable, and cost-effective manner. It provides an umbrella framework that allows for prioritization, gap analysis, metrics, and effective integration of security processes and solutions into the university’s infrastructure.

At the tactical level, there is a consistent push each year to prioritize action items based on the results of targeted risk assessments, regulatory and policy implications and/or guidance, and institution-wide strategic academic and business goals. This all works behind the scenes to keep the information security program poised to take advantage of opportunities to improve key business processes, integrate controls to protect the university’s network infrastructure from attacks and intrusions, influence decisions of top management about future directions of IT, and build the perception that information security adds value to the enterprise.

ISO 27000 as a Framework

ISO 27000 is designed to provide a process or model for establishing, operating, maintaining, and improving an ISMS. As such, it can be tailored to each institution’s information security needs. In addition to being compatible with other standards and guidelines appropriate to information security, ISO 27000 favors an incremental deployment of controls. It employs the Plan-Do-Check-Act (PDCA) structure to facilitate orderly creation, testing, and implementation of the ISMS and emphasizes development and improvement of policies, objectives, processes and procedures, routine reviews and audits, and continuous improvements.

A number of accredited certification bodies are available worldwide to provide certification with ISO 27001 and its international variants. Certifications are typically conducted by ISO/IEC lead auditors, and they involve three stages:

- A “table top” review of the existence and completeness of key documentation such as the institution’s ISMS policy, statement of applicability (SoA), a
summary of the controls that have been planned and implemented to address identified risks, and a risk analysis report/risk treatment plan (RTP) for all assets within the ISMS

- An in-depth audit involving testing the existence and effectiveness of the information security controls stated in the SoA and RTP, as well as their supporting documentation

- A follow-up reassessment audit to confirm that a previously certified institution remains in compliance with the standard and is able to demonstrate continuous improvements in the information security posture through further evaluation and refinement of risks, business processes, and controls

The ISO 27001 certification is a three-year process during which the certified institution’s ISMS is further evaluated to demonstrate increased effectiveness and compliance with ISO 27001. Among the guiding principles of certification is that certification is not something that an institution achieves and then ignores. Rather, in order to maintain certification, the institution must both review and monitor its ISMS on an ongoing basis.

What It Means to Higher Education

Standards are always out of date. That's what makes them standards.

—Alan Bennett

Many of us remember decades of airplane travel that didn’t involve what the U.S. has come to accept as airport security. When we think about what it takes to make a cultural shift among a large population, we might do well to remember that in the space of only a few years, air travelers went from freely boarding airplanes to baggage scanning to full-body X-rays. If we think that instilling a culture of information security on our campuses is difficult, imagine what would happen if we required people to remove their shoes before they came to campus!

Information security governance frameworks work seamlessly with other IT governance models. Like broader governance models, they emphasize a continual improvement in business processes, alignment of information security strategies with academic and business objectives, and managing risk in ways that mitigate risk to the institution at large—with the overarching purposes of ensuring that confidential data is protected from unauthorized access; university policies and regulatory/legislative statutes are complied with; and the integrity and availability of university IT systems, services, and data repositories are effectively maintained.

To recap, in order to be successful, an information security governance framework must have the active commitment, support, and involvement of the institution’s top management executives. Implementation of these frameworks requires a top-down approach to ensure that all ships are steering in the same direction. Policies, objectives, and activities of the information security program must speak to the academic and business objectives of the institution. Consistent, repeatable, and auditable methods for measuring and mitigating risk to information and technology assets must be included in
the framework. Members of the campus community will typically understand and cooperate with efforts to keep information secure if they have access to

- training for managers and employees about the relationships between effective information security controls and improved business processes;
- information security awareness training responsive to their needs, roles, and responsibilities; and
- adequate funding and staffing for information security activities.

Ultimately, the campus will begin to focus efforts around the implementation of business processes and controls commensurate with acceptable levels of risk. At the same time, experienced information security personnel who are trained in governance, risk management, and auditing can effectively work with business and academic departments, as well as with IT, to illustrate how to reengineer business processes and include controls that allow for transparency while ensuring protection of valuable information resources and compliance with regulatory requirements. Julia Allen, senior researcher within the CERT Program at the Software Engineering Institute at Carnegie Mellon University, sums up the overall rationale for information security governance:

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization’s management—including boards of directors, senior executives, and all managers—does not establish and reinforce the business need for effective enterprise security, the organization’s desired state of security will not be articulated, achieved, or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.6

Key Questions to Ask

- How can selecting and implementing information security governance frameworks assist us in determining whether our information security programs are efficient and cost-effective?
- What investment in staff and resources would we have to make to develop and implement an information security governance framework?
- How can information security governance frameworks provide assurances to key institution stakeholders that confidential data is protected with due diligence and/or that our information security objectives are being met?

Where to Learn More

- Boes, Richard, Tom Cramer, Vicky Dean, Roger Hanson, and Nan McKenna. “Campus IT Security: Governance, Strategy, Policy, and Enforcement”
Endnotes


4. The names ITIL and IT Infrastructure Library are registered trademarks of the United Kingdom’s Office of Government Commerce (OGC).


About the Authors

Tammy L. Clark (tlclark@gsu.edu) is Chief Information Security Officer at Georgia State University. Toby D. Sitko (tsitko@educause.edu) is a Fellow at the EDUCAUSE Center for Applied Research.