INFORMATION SECURITY GOVERNANCE ASSESSMENT TOOL FOR HIGHER EDUCATION

Information security is a critical issue for institutions of higher education (IHE). IHE face issues of risk, liability, business continuity, costs, and national repercussions as they increasingly move their core activities to the Internet. Colleges and universities also play a unique role as the managers of some of the largest collections of computers on many of our fastest networks. In the end, an effective program for information security depends on an effective implementation of information security governance (ISG).

In April 2004, the Corporate Governance Task Force established as a result of the National Cyber Security Summit issued its report entitled "Information Security Governance: A Call to Action" (available at www.cyberpartnership.org). The report asserts that "America cannot solve its cyber security challenges by delegating them to government officials or CIOs. The best way to strengthen US information security is to treat it as a corporate governance issue that requires the attention of Boards and CEOs." A subcommittee of the task force that considered the ISG framework for educational institutions and nonprofit organizations concluded that the ISG framework and assessment tool originally developed for the corporate sector were valid in principle for the education and nonprofit sector and provide a good starting point.

Purpose of This Tool

The Information Security Governance (ISG) Assessment Tool for Higher Education is intended to help IHE determine the degree to which they have implemented an ISG framework at the strategic level within their institution. This tool is not intended to provide a complete and detailed list of information security policies or practices that must be followed. Rather, it is intended to help a president or institutional leadership identify general areas of concern as they relate to the ISG framework. If a particular question can't be answered affirmatively, then that question indicates an area the institution needs to examine to determine what risks may be associated with it and how the institution will address those risks.

This tool is designed to support the ISG framework recommended by the Corporate Governance Task Force and has been modified for IHE. The first section of this tool will help an institution assess its reliance on information technology. The remaining sections are intended to help IHE determine the maturity of information security governance at a strategic level. The overall rating (good, needs improvement, poor) will depend on the raw score and an institution's reliance on information technology.

This tool, in conjunction with the framework, can be used by institutions of varying sizes and types to gain a better understanding at a high level of the role information security governance has in their organization and how it can best be structured. Once an item in the assessment tool is noted for improvement, users are encouraged to take advantage of the many other tools and references already available that will offer more specific guidance in each area. For example, there are multiple references on conducting risk assessments, several references on incident response plans, commercial tools to help with vulnerability assessments, and so forth.

How to Use This Tool

This tool and the ISG framework were created to evaluate the *people*, *process*, and *technology* components of cybersecurity. This tool was intended for use by an institution as a whole, although a unit within an institution may also use it to help determine the maturity of its individual information security program. Unless otherwise noted, it should be completed by the president, chancellor, chief executive officer, or a designee.

Answer the questions in each section as best you can, and enter the total in the space provided at the end of each section. The total from each section should be entered into the chart on the last page to determine your total security assessment score. Your *overall security evaluation rating* is determined by factoring together your *total reliance on IT score* with your *total security assessment score* to correspond with an *overall assessment* of poor, needs improvement, or good.

Acknowledgements

The ISG Assessment Tool for Higher Education was developed by the Security Risk Assessment Working Group of the EDUCAUSE/Internet2 Computer and Network Security Task Force (www.educause.edu/security). The developers want to thank the Corporate Governance Task Force of the National Cyber Security Summit who developed the assessment tool from which the higher education version is derived. The creators of the ISG Assessment Tool in turn acknowledge TechNet, the creators of the TechNet Corporate Information Security Evaluation for CEOs, for their gracious contribution to the project. The TechNet Corporate Information Security Evaluation served as the starting point for the Corporate Governance Task Force ISG tool with the general format and many of the questions taken directly from it.

Questions or comments regarding the ISG Assessment Tool or application of the ISG framework for IHE should be addressed to Security-Task-Force@educause.edu.

Section I: Organizational Reliance on IT

This section is designed to help you determine your institution's reliance on information technology for business continuity. Your overall security evaluation rating will depend in part on your institution's reliance on information technology. It should be completed by the president, chancellor, chief executive officer, or a designee.

	Scoring: Very Low = 0; Low = 1; Medium = 2; High = 3; Very High = 4	**Score**
1	**Characteristics of Organization**	
1.1	Annual budget of the organization Less than $10 million = very low $10 million to $100 million = low $100 to $500 million = medium $500 million to $1 billion or more = high $1 billion or more = very high	
1.2	Number of employees Less than 500 employees = very low 500 to 1,000 employees = low 1,000 to 5,000 employees = medium 5,000 to 20,000 employees = high more than 20,000 employees = very high	
1.3	Number of students Less than 1,000 students = very low 1,000 to 5,000 students = low 5,000 to 10,000 students = medium 10,000 to 20,000 students = high more than 20,000 students = very high	
	Higher Education Characteristics	
1.4	Dependence on information technology systems and the Internet to conduct academic, research, and outreach programs and offer support services	
1.5	Value of organization's intellectual property stored or transmitted in electronic form	
1.6	Impact of major system downtime on operations	
1.7	Impact to your operations from an Internet outage	
1.8	Dependency on multinational and multisite operations	
1.9	Plans for multinational and multisite operations (outsourced business functions, multiple campus locations, new research collaborations, student enrollment overseas)	
1.10	Impact to national or critical infrastructure in case of outage or compromise to your systems	
1.11	The sensitivity of stakeholders (including but not limited to students, faculty, staff, alumni, governing boards, legislators, donors, and funding agencies) to privacy	
1.12	Stakeholders' sensitivity to security	
1.13	Level of regulation regarding security (FERPA, HIPAA, GLBA, other applicable international, federal, state, or local regulations)	
1.14	Potential impact on reputation of a security incident (student enrollment, faculty recruitment, ability to attract donors, negative press)	
1.15	Extent of operations dependent on third parties (business partners, contractors, suppliers)	
1.16	Does your organization have academic or research programs in a sensitive area that may make you a target of violent physical or cyber attack from any groups?	
	TOTAL RELIANCE ON IT SCORE	

	Section II: Risk Management This section assesses the risk management process as it relates to creating an information security strategy and program. Please note the change in scoring. This method of scoring applies throughout the remainder of this document. It should be completed by the president, chancellor, chief executive officer, or a designee.	
	Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4	**Score**
2	**Information Security Risk Assessment**	
2.1	Does your organization have a documented information security program?	
2.2	Has your organization conducted a risk assessment to identify the key objectives that need to be supported by your information security program?	
2.3	Has your organization identified critical assets and the functions that rely on them?	
2.4	Have the information security threats and vulnerabilities associated with each of the critical assets and functions been identified?	
2.5	Has a cost been assigned to the loss of each critical asset or function?	
2.6	Do you have a written information security strategy?	
2.7	Does your written information security strategy include plans that seek to cost-effectively reduce the risks to an acceptable level, with minimal disruptions to operations?	
2.8	Is the strategy reviewed and updated at least annually or more frequently when significant changes require it?	
2.9	Do you have a process in place to monitor federal, state, or international legislation or regulations and determine their applicability to your organization?	
	TOTAL RISK MANAGEMENT SCORE	

Section III: People

This section assesses the organizational aspects of your information security program. It should be completed by the president, chancellor, chief executive officer, or a designee.

	Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4	**Score**
3	**Information Security Function/Organization**	
3.1	Is there a person or organization that has information security as their primary duty, with responsibility for maintaining the security program and ensuring compliance?	
3.2	Do the leaders and staff of your information security organization have the necessary experience and qualifications?	
3.3	Does your information security function have the authority it needs to manage and ensure compliance with the information security program?	
3.4	Does your information security function have the resources it needs to manage and ensure compliance with the information security program?	
3.5	Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes and audits?	
3.6	Has specific responsibility been assigned for the execution of business continuity and disaster recovery plans (either within or outside the information security function)?	
3.7	Do you have an ongoing training program in place to build skills and competencies for information security for members of the information security function?	
3.8	Is someone in the information security function responsible for liaising with units to identify any new security requirements based on changes to operations?	
3.9	Does the information security function actively engage with other units (human resources, student affairs, legal counsel) to develop and enforce compliance with information security policies and practices?	
3.10	Does the information security function report regularly to institutional leaders and the governing board on the compliance of the institution to and the effectiveness of the information security program and policies?	
3.11	Are the senior officers of the institution ultimately responsible and accountable for the information security program, including approval of information security policies?	
3.12	Do the unit heads and senior managers have specific programs in place to comply with information security policies and standards with the goal of ensuring the security of the information and systems that support the operations and assets under their control?	
3.13	Have you implemented an information security education and awareness program such that all administrators, faculty, staff, contractors, external providers, students, guests, and others know the information security policies that apply to them and understand their responsibilities?	
	TOTAL PEOPLE SCORE	

	Section IV: Processes This section assesses the processes that should be part of an information security program. It should be completed by the president, chancellor, chief executive officer, or a designee.	
	Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4	**Score**
4	**Security Technology Strategy**	
4.1	Does your institution have an official information security architecture, based on your risk management analysis and information security strategy?	
4.2	Is the security architecture updated periodically to take into account new needs and strategies as well as changing security threats?	
4.3	As the architecture evolves, is there a process to review existing systems and applications for compliance and for addressing cases of noncompliance?	
4.4	Have you instituted processes and procedures for involving the security personnel in evaluating and addressing any security impacts before the purchase or introduction of new systems?	
4.5	If a deployed system is found to be in noncompliance with your official architecture, is there a process and defined timeframe to bring it into compliance or to remove it from service, applications or business processes?	
4.6	Do you have a process to appropriately evaluate and classify the information and information assets that support the operations and assets under your control, to indicate the appropriate levels of information security?	
4.7	Are there specific, documented, security-related configuration settings for all systems and applications?	
4.8	Do you have a patch management strategy, policy, and procedures in place and responsibilities assigned for monitoring and promptly responding to patch releases, security bulletins, and vulnerabilities reports?	
	Policy Development and Enforcement	
4.9	Are written information security policies consistent, easy to understand, and readily available to administrators, faculty, employees, students, contractors, and partners?	
4.10	Is there a method for communicating security policies to administrators, faculty, employees, students, contractors, and partners?	
4.11	Are consequences for noncompliance with corporate policies clearly communicated and enforced?	
4.12	Are there documented procedures for granting exceptions to policy?	
4.13	When policies are updated or new policies are developed, is an analysis conducted to determine the financial and resource implications of implementing the new policy?	
4.14	Do your security policies effectively address the risks identified in your risk analysis/risk assessments?	
4.15	Are relevant security policies included in all of your third-party contracts?	
4.16	Are information security issues considered in all important decisions within the organization?	

	Information Security Policies and Procedures	
	Based on your information security risk management strategy, do you have official written information security policies or procedures that address each of the following areas?	
4.17	Individual employee responsibilities for information security practices	
4.18	Acceptable use of computers, e-mail, Internet, and intranet	
4.19	Protection of organizational assets, including intellectual property	
4.20	Managing privacy issues, including breaches of personal information	
4.21	Identity management, including excursions or breaches of sensitive identity information	
4.22	Access control, authentication, and authorization practices and requirements	
4.23	Data classification, retention, and destruction	
4.24	Information sharing, including storing and transmitting institutional data on outside resources (ISPs, external networks, contractors' systems)	
4.25	Vulnerability management (patch management, antivirus software)	
4.26	Disaster recovery contingency planning (business continuity planning)	
4.27	Incident reporting and response	
4.28	Security compliance monitoring and enforcement	
4.29	Change management processes	
4.30	Physical security and personnel clearances or background checks	
4.31	Reporting security events to affected parties, including individuals, public, partners, law enforcement, and other security organizations as appropriate	
4.32	Prompt investigation and correction of the causes of security failures	
4.33	Data backups and secure off-site storage	
4.34	Secure disposal of data, old media, or printed materials that contains sensitive information	
	Physical Security	
	For your critical data centers, programming rooms, network operations centers, and other sensitive facilities or locations:	
4.35	Are multiple physical security measures in place to restrict forced or unauthorized entry?	
4.36	Is there a process for issuing keys, codes, and/or cards that require proper authorization and background checks for access to these sensitive facilities?	
4.37	Is your critical hardware and wiring protected from power loss, tampering, failure, and environmental threats?	

	Security Program Administration	
4.38	Do you maintain a current inventory of both the physical network elements (routers/switches, subnets, DNS, DHCP servers) and also the logical network assets (domain names, network addresses, access control lists)?	
4.39	Do you have a configuration-management process in place to ensure that changes to your critical systems are for valid business reasons and have received proper authorization?	
4.40	Does your organization periodically test and evaluate or audit your information security program, practices, controls, and techniques to ensure they are effectively implemented?	
4.41	Do you conduct a periodic independent evaluation or audit of your information security program and practices for each business unit?	
4.42	Does each periodic independent evaluation or audit test the effectiveness of information security policies, procedure, and practices of a representative subset of each business unit's information systems?	
4.43	Does each periodic independent evaluation or audit assess the compliance of each business unit with the requirements of a standard information security framework and related information security policies, standards, procedures, and guidelines?	
4.44	Are security-performance metrics instituted, evaluated, and reported?	
	TOTAL PROCESSES SCORE	

Section V: Technology

This section assesses the major technology topics related to information security. It should be completed by the president, chancellor, chief executive officer, or a designee with input from the chief security officer or chief information officer.

	Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4	**Score**
5	**Security Technology**	
5.1	Are Internet-accessible servers protected by more than one security layer (firewalls, network IDS, host IDS, application IDS)?	
5.2	Are there controls between the layers of end-tier systems?	
5.3	Are your networks, systems, and applications periodically scanned to check for vulnerabilities as well as integrity of configurations?	
5.4	Do you constantly monitor in real time your networks, systems and applications for unauthorized access and anomalous behavior such as viruses, malicious code insertion, or break-in attempts?	
5.5	Are security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments automatically logged?	
5.6	Is sensitive data encrypted and associated encryption keys properly protected?	
5.7	Are there effective and reliable mechanisms in place to manage digital identities (accounts, keys, tokens) throughout their life cycle, from registration through termination?	
5.8	Do all of your systems and applications support and enforce automatic password change management or automatic expiration of passwords, as well as password complexity and reuse rules?	
5.9	Do you have an authentication system in place that applies higher levels of authentication to protect resources with higher levels of sensitivity?	
5.10	Do you have an authorization system that enforces time limits and defaults to minimum privileges?	
5.11	Do your systems and applications enforce session/user management practices including automatic timeouts, lockout on login failure, and revocation?	
5.12	Do you employ specific measures to prevent and detect rogue access for all of your wireless LANs?	
5.13	Do you employ specific measures to secure the servers that manage your network domain names and addresses (DNS and DHCP servers)?	
5.14	Do you employ specific measures to secure your remote access services (VPN and dial-up) as well as to secure remote access client systems?	
5.15	Is every desktop workstation and server protected with antivirus software?	
5.16	Is there an audit trail to verify that virus definitions files are updated frequently and systematically?	
5.17	Is every desktop workstation and server updated regularly with the latest operating system patches?	
5.18	Taking into account severity and urgency, are there mechanisms in place to report and respond to a variety of anomalies and security events?	
	TOTAL TECHNOLOGY SCORE	

Scoring Tool

		Low	High	Dependency
TOTAL RELIANCE ON IT SCORE		**0**	**8**	**Very Low**
		9	**16**	**Low**
		17	**32**	**Medium**
		33	**48**	**High**
		49	**64**	**Very High**
TOTAL RISK MANAGEMENT SCORE				
TOTAL PEOPLE SCORE				
TOTAL PROCESSES SCORE				
TOTAL TECHNOLOGY SCORE				
TOTAL SECURITY ASSESSMENT SCORE (Risk Management, People, Process, & Technology)				

OVERALL SECURITY EVALUATION RATING:

Reliance on IT	Program Rating Ranges		Overall Assessment
Very High	**0**	**199**	Poor
	200	**274**	Needs Improvement
	275	**336**	Good
High	**0**	**174**	Poor
	175	**249**	Needs Improvement
	250	**336**	Good
Medium	**0**	**149**	Poor
	150	**224**	Needs Improvement
	225	**336**	Good
Low	**0**	**124**	Poor
	125	**199**	Needs Improvement
	200	**336**	Good
Very Low	**0**	**99**	Poor
	100	**174**	Needs Improvement
	175	**336**	Good