INFORMATION SECURITY GOVERNANCE:

A CALL TO ACTION

The road to information security goes through corporate governance. 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.

The Corporate Governance Task Force was formed in December 2003 to develop and promote a coherent governance framework to drive implementation of effective information security programs. Although information security is often viewed as a technical issue, it is also a governance challenge that involves risk management, reporting and accountability. As such, it requires the active engagement of executive management.

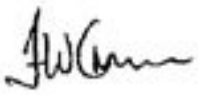
Today's economic environment demands that enterprises in both the public and private sectors reach beyond traditional boundaries. Citizens, customers, educators, suppliers, investors and other partners are all demanding more access to strategic resources. As enterprises reinvent themselves to meet this demand, traditional boundaries are disappearing and the premium on information security is rising. Heightened concerns about critical infrastructure protection and homeland security are accelerating this trend.

In this report we provide a framework and guidelines to help organizations assess their performance and put in place an information security governance program. By themselves, however, these tools are not enough. To succeed we need a private sector commitment to implement this framework and begin to integrate information security into its corporate governance program.

As we embrace information security governance, it is important to remember that, like quality, it is a journey that requires continuous improvement over time. We are still in the early stages of this journey. As we progress, we will not only reap the rewards of productivity growth, customer satisfaction and improved competitiveness, but also gain the larger reward of enhanced homeland security.

We encourage you to join us in this effort.

F. William Conner



Chairman, CEO and President
Entrust, Inc.

Arthur W. Coviello

CEO and President
RSA Security Inc.

TASK FORCE MEMBERS & PARTICIPANTS

TASK FORCE CO-CHAIRS

F. William Conner
Chairman, CEO and President
Entrust, Inc.

Arthur W. Coviello
CEO and President
RSA Security Inc.

TASK FORCE SUBCOMMITTEE CHAIRS

Michael Sullivan, Entrust, Inc.
Co-Chair, Framework Subcommittee

Howard Hantman, RSA Security Inc.
Co-Chair, Framework Subcommittee

Maureen Glynn, Intel Corporation
Chair, Corporate Implementation Subcommittee

Mark Luker, EDUCAUSE
Chair, Education and Non-Profit Implementation Subcommittee

John W. Lainhart, IBM
Co-Chair, Verification & Compliance Subcommittee

Dave Cullinane, Washington Mutual/ISSA
Co-Chair, Verification & Compliance Subcommittee

TASK FORCE MEMBERS

Michael Aisenberg ..... VeriSign, Inc.
Julia Allen ..... Carnegie Mellon University
Scott Bergs ..... Midwest Wireless Holdings
Mark Bohannon ..... Software & Information Industry Association
Dan Burton..... Entrust, Inc.
Susan Caldwell..... IT Governance Institute
Robert Dix..... U.S. House of Representatives
Mark Egan..... Symantec
Cristin Flynn ..... BellSouth
Kevin Gahan ..... MCI
Susan Getgood ..... SurfControl
Margie Gilbert..... U.S. House of Representatives
Ed Glover..... Sun Microsystems
Amy Goodman..... Gibson, Dunn & Crutcher, LLP

Matt Halbleib ..... Intel Corporation
Edward Hearst..... Sybase
Robert Higgins..... Motorola
Joy Hughes..... George Mason University
Shannon Kellogg..... RSA Security Inc.
Susan Kennedy..... University of Pennsylvania
William Levant ..... Deloitte
James Lewis..... CSIS
Mark Lindig ..... KPMG/ GSC
John McClurg..... Lucent Technologies/ Bell Labs
Charles Meister ..... University of Southern California, ICIIP
Rod Nydam ..... PCIS/ Morris, Manning & Martin, LLP
Will Ozier..... OPA, Inc.
Rodney Peterson ..... EDUCAUSE
Michael Rasmussen ..... Forrester Research/ISSA
Robyn Render ..... University of North Carolina
Mike Roberts..... Darwin Group
Douglas Sabo ..... Network Associates
Laney Settelmeyer ..... Intel Corporation
Marilyn Thornton..... ALLTEL
John Williams..... Preventsys
Morley Winograd ..... CTM
Gordon Wishon ..... University of Notre Dame

TASK FORCE SECRETARIAT

Gretchen Beyer ..... TechNet
Leslie Saul Garvin..... TechNet

CONTRACTOR SUPPORT

Joseph Butcher..... Booz Allen Hamilton
Audrey Plonk ..... Booz Allen Hamilton
Kristin Royster..... Booz Allen Hamilton
Demetria Scott ..... Booz Allen Hamilton

TABLE OF CONTENTS

EXECUTIVE SUMMARY

To better secure its information systems and strengthen America's homeland security, the private sector should incorporate information security into its corporate governance efforts. Although information security is not solely a technical issue, it is often treated that way. If businesses, educational institutions, and non-profit organizations are to make significant progress securing their information assets, executives must make information security an integral part of core business operations. There is no better way to accomplish this goal than to highlight it as part of the existing internal controls and policies that constitute corporate governance.

The Corporate Governance Task Force believes that information security governance (ISG) efforts will be most successful if conducted voluntarily, instead of mandated by government. With the appropriate tools and guidance, the private sector can effectively rise to the challenges set out in *The National Strategy to Secure Cyberspace*. The recommendations that follow are designed for broad application to private sector businesses across all sectors, non-profit organizations, and educational institutions.

Recommendation 1

Organizations should adopt the information security governance framework described in this report to embed cyber security into their corporate governance process.

The Corporate Governance Task Force has developed a comprehensive governance framework to guide implementation of effective information security programs. Drawing on the present body of work on information security governance, including International Organization for Standardizations/ International Electrotechnical Commission (ISO/IEC 17799) and the Federal Information Security Management Act (FISMA), the Task Force has developed an objective, standards-based, scaleable, and collaborative framework (Appendix A) to aid organizations in the creation of an ISG structure. The framework can be adapted to a wide variety of entities, including corporations of all sizes in different industry sectors, as well as education and non-profit institutions.

To facilitate use of the framework, the Task Force has developed several additional tools. The ISG Functions & Responsibilities Guide (Appendix B) provides guidance for mapping information security duties to key corporate functions and is applicable to organizations of various sizes. The IDEAL process (Appendix C) provides a model for organizations to use to adapt and implement the ISG framework and assessment tool within their organizations. The information security governance assessment tool (Appendix D) serves as a rapid evaluation tool for corporations and other business organizations to assess their current ISG practices, while the ISG Implementation Plan for Education and Non-profit Institutions (Appendix E) examines and adapts successful recommendations for implementing the ISG assessment tool outside the corporate model.

Recommendation 2

Organizations should signal their commitment to information security governance by stating on their Web site that they intend to use the tools developed by the Corporate Governance Task Force to assess their performance and report the results to their board of directors.

By stating on their Web site that they embrace information security governance, organizations can help drive a voluntary, private sector effort to strengthen America's cyber security. To ensure that public statements about information security governance are transparent and consistent, industry

associations should work with the relevant government agencies to develop standard language and create an ISG logo to accompany these statements.

Some organizations may want to incorporate this statement into the privacy policy statement that appears on their Web site. Others may choose to post a freestanding statement about information security governance. Still others may take a different approach because of concerns about heightened cyber security threats, which may result from a public statement. Regardless of form, the goal is for all organizations to adopt and signal a commitment to effective information security governance.

Because organizations have diverse needs and will vary their approaches to information security governance, the Task Force has identified a Core Set of Principles to help guide their efforts (see below). By reviewing these principles internally, organizations can develop a program that is best tailored to their needs.

- **CEOs should have an annual information security evaluation conducted, review the evaluation results with staff, and report on performance to the board of directors.**
- **Organizations should conduct periodic risk assessments of information assets as part of a risk management program.**
- **Organizations should implement policies and procedures based on risk assessments to secure information assets.**
- **Organizations should establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability.**
- **Organizations should develop plans and initiate actions to provide adequate information security for networks, facilities, systems and information.**
- **Organizations should treat information security as an integral part of the system lifecycle.**
- **Organizations should provide information security awareness, training and education to personnel.**
- **Organizations should conduct periodic testing and evaluation of the effectiveness of information security policies and procedures.**
- **Organizations should create and execute a plan for remedial action to address any information security deficiencies.**
- **Organizations should develop and implement incident response procedures.**
- **Organizations should establish plans, procedures and tests to provide continuity of operations.**
- **Organizations should use security best practices guidance, such as ISO 17799, to measure information security performance.**

Recommendation 3

All organizations represented on the Corporate Governance Task Force should signal their commitment to information security governance by voluntarily posting a statement on their Web site. In addition, TechNet, the Business Software Alliance, the Information Technology Association of America, the Chamber of Commerce and other leading trade associations and membership organizations should encourage their members to embrace information security governance and post statements on their Web sites. Furthermore, all Summit participants should embrace information security governance and post statements on their Web sites, and if applicable, encourage their members to do so as well.

To drive compliance with this voluntary effort, all organizations represented on the Corporate Governance Task Force should embrace and implement these recommendations as soon as possible. In doing so, these organizations will set an example for others to follow. Moreover, leading trade associations and membership organizations should publicly endorse information security governance, and encourage their members to do the same. In addition, all National Cyber Security Summit participants should embrace information security governance and post statements on their individual Web sites, and if applicable, encourage their members to do so as well. In order to encourage small and medium-sized organizations to embrace information security governance, large enterprises should work with their partners, suppliers and customers to facilitate adoption. By creating a critical mass of interest and commitment—and working with the Department of Homeland Security (DHS) to publicize it—Task Force participants will be able to accelerate adoption of information security governance throughout the private sector.

Recommendation 4

The Department of Homeland Security should endorse the information security governance framework and core set of principles outlined in this report, and encourage the private sector to make cyber security part of its corporate governance efforts.

DHS should launch a public campaign urging organizations to embrace information security governance and recognize those that do so. Such a campaign should take into account the following:

- It should consist of a broad-based recognition of effort and commitment, not an exclusive award that is difficult to apply for and evaluate. For example, DHS could recognize those organizations that put an ISG statement on their Web site.
- It should emphasize that information security governance is a way for the private sector to execute against *The National Strategy to Secure Cyberspace*.
- It should highlight the need for continuous improvement, not a one-time effort.
- It should be structured so that it protects against the threat that can accompany public recognition about cyber security. Because any public statements about cyber security also can make organizations a target for hackers, the DHS should be careful to recognize enterprises for their information security *governance* efforts, not their security performance.

Recommendation 5

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) should revise the Internal Controls-Integrated Framework so that it explicitly addresses information security governance.

In spite of all the discussion about corporate governance, more attention needs to be given to the role of information technology (IT) in the financial reporting process. In order to establish that internal controls are adequate, it is essential to take into account IT controls. Auditors are beginning to emphasize that information security be part of the corporate governance compliance process.

Accounting and audit references to "internal controls" are contained in COSO's Internal Controls-Integrated Framework, but as currently written it does not provide a roadmap for information security governance. By revising the COSO guidelines for internal controls so that they provide guidance for information security governance, we can lay the groundwork for the private sector to conduct self-assessments and for auditors to apply these rules consistently. In the absence of such specific guidance, Control Objectives for Information and Related Technology (COBIT) can serve as a reference, and along with ISO 17799, can provide additional detailed information security governance guidance.

Conclusion

Effective information security governance cannot be established overnight and requires continuous improvement. The Corporate Governance Task Force has developed recommendations and tools that will provide a strong start to organizations seeking to improve their information security governance. Adoption of these recommendations and tools, however, is not the end of the process. Rather, it is an essential first step to secure information systems and strengthen our nation's homeland security.

The Task Force calls on organizations to make information security governance a priority and to use these tools to launch internal information security governance processes and generate awareness of the need to treat information security as a governance issue. The important thing is to get started and systematically improve performance over time.

1.0 INTRODUCTION AND CHARGE

Information security is not only a technical issue, but also a business and governance challenge that involves risk management, reporting, and accountability. Effective security requires the active engagement of executive management to assess emerging threats and provide strong cyber security leadership. The term penned to describe executive management's engagement is *corporate governance*. Corporate governance consists of the set of policies and internal controls by which organizations, irrespective of size or form, are directed and managed. Information security governance is a subset of organizations' overall governance program. Risk management, reporting, and accountability are central features of these policies and internal controls.

During the December 2003 Cyber Security Summit, the Corporate Governance Task Force agreed on the importance of adopting a scalable governance framework to help organizations define the pathway from awareness about IS issues to implementation of solutions. With this goal in mind, the Task Force established four subcommittees to

- **Distill the current body of work on information security governance,**
- **Establish a preliminary framework for information security governance,**
- **Tailor implementation guidelines for different entities, and**
- **Propose processes for assessing compliance.**

The sections below outline the Task Force's suggestions for structuring the ISG framework, using the ISG assessment tool, and demonstrating compliance with the framework.

2.0 CORPORATE GOVERNANCE TASK FORCE RECOMMENDATIONS

2.1 Information Security Governance Framework

Recommendation 1

Organizations should adopt the information security governance framework described in this report to embed cyber security into their corporate governance process.

Information security governance (ISG) is an essential component of successful organizational management. The fragile state of information security demands that immediate steps be taken to ensure that data are not compromised and that information systems remain secure. The framework subcommittee of the Corporate Governance Task Force was charged with examining current private sector approaches to information security governance and identifying how organizations may improve ISG structures.

The framework subcommittee developed an ISG framework, matrix, and PowerPoint presentation (Appendix A and B) outlining various elements of an effective information security governance program. Use of the framework will guide a program of successful information security risk management and oversight. The framework recommends controls to help protect an organization's information and information systems. The ISG framework addresses the following areas of governance:

- **Authority and functions of the board of directors/trustees**
- **Authority and functions of the senior executive**
- **Authority and functions of the executive team members**
- **Authority and functions of senior managers**
- **Responsibilities of all employees and users**
- **Organizational unit security program**
- **Organizational unit reporting**
- **Information security program evaluation**

In addition to the framework, the subcommittee created a matrix (Appendix B) to map elements of the framework to different organizational structures. According to the framework, the Senior Executive has the responsibility to assign various information security functions to the appropriate individuals within an organization. The matrix provides examples for typical roles found in four large organizations, one medium organization, one small organization and one public agency. The framework and the matrix are designed to assist any entity in structuring an internal model for information security governance.

As security, and particularly information security, become a central concern across industry and government, it is essential that sound governance models exist to ensure proper infrastructure protection. The framework subcommittee examined organizational structures and governance to provide a framework for the future of information security. The program, when applied to all types of organizations, will allow for the protection of valuable information in the face of growing cyber security risks.

2.2 ISG Framework Implementation

Since many organizations have only begun to consider information security as part of their business model, a change in mindset is required to achieve the goal of integrating information security into corporate governance. The Task Force concluded that the IDEAL model, developed by Carnegie Mellon University's Software Engineering Institute, would be a beneficial model for organizations when adapting and implementing the framework and assessment tool for use within their own organizational structures. The model is an organizational improvement model that serves as a roadmap for initiating, planning and implementing improvement actions. The IDEAL model is named for the five phases it describes: Initiating, Diagnosing, Establishing, Acting and Learning, shown in Table 1.

Table 1.

I	**Initiating**	Lay the groundwork for a successful improvement effort.
D	**Diagnosing**	Determine where you are relative to where you want to be.
E	**Establishing**	Plan the specifics of how you will reach your destination.
A	**Acting**	Do the work according to the plan.
L	**Learning**	Learn from the experience and improve your ability to adopt new improvements in the future.

The ISG assessment tool, properly implemented by organizations, is the first step in incorporating information security into an organization's corporate governance structure. An increased focus on information security will add to an organization's overall reputation and strengthen its security posture.

The assessment tool (Appendix D) was developed to support the framework created by the Corporate Governance Task Force. The tool is intended to help organizations determine the degree to which they have implemented an ISG framework. Both the framework and the tool are designed to cover a broad base of information security areas that support and interact with business processes to manage risk within an organization.

This tool is not intended to provide a detailed list of information security policies or practices an organization must follow. A number of widely accepted methodologies were used to develop the tool and remain as acceptable options for organizations to identify areas of information security concern. The goal is simply for organizations to more completely examine information security as an integral part of their operation.

The ISG assessment tool is divided into four sections:

- **Business Dependency**—measuring an organization's reliance on information technology for business continuity as well as the degree of sector interdependency and regulation
- **Risk Management**—evaluating the risk management process as it relates to creating an information securing strategy and program
- **People**—evaluating the organizational aspects of your information security program
- **Processes**—identifying the processes that should be part of an information security program.

The ISG assessment tool, in conjunction with the framework, can be used by organizations of varying sizes and types, regardless of industry, 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.

Although the tool initially was developed for use by corporate organizations, a subgroup within the Task Force was created to examine applicability of both the framework and the tool in the non-profit and education sectors. The Education and Non-profit Implementation Subgroup issued a report (Appendix E) describing how best to translate both the framework and the tool to support

applicability in non-profit and education organizations. The report is intended for institutions that do not currently have an information security governance structure in place. It examines and adapts successful recommendations for implementing the ISG framework and tool to fit the culture and structure of education and non-profit organizations.

2.3 ISG Verification and Compliance

Information security has a lot in common with quality assurance. Recognizing the similarities, Task Force members have consciously modeled verification and compliance policy recommendations on lessons learned from national efforts to improve quality. Information security is not a one-time effort, but a journey that requires continuous improvement. An internationally recognized standard is critical to rallying an effective private sector response, and efforts are likely to be most successful if they are conducted voluntarily, rather than mandated by government.

The Corporate Governance Task Force understands that, as with the early quality assurance initiatives, many enterprises are concerned that the efforts to improve information security will increase business costs. Like quality assurance, however, information security holds the larger promise of increased productivity, heightened customer satisfaction, and ultimately, greater brand loyalty. The four recommendations that follow are designed to facilitate the verification and compliance of information security governance efforts.

2.3a Verification & Compliance Recommendations

Recommendation 2

Organizations should signal their commitment to information security governance by stating on their Web site that they intend to use the tools developed by the Corporate Governance Task Force to assess their performance and report the results to their board of directors.

The tool set for information security governance can be found in Appendices A, B, C, D and E of this report. In addition, the Task Force developed a set of principles to help guide adoption. The ISG Core Set of Principles (see Table 2) is derived from widely recognized information security and IT governance frameworks—International Organization for Standardization (ISO) 17799, Federal Information Security Management Act (FISMA), and Control Objectives for Information and Related Technology (COBIT). The ISG framework and implementation tools developed by the Corporate Governance Task Force will help organizations launch this process, as well as undertake more in-depth evaluations that will serve as the basis for future improvement. These principles can help guide efforts to incorporate information security into corporate governance programs.

Table 2.

- CEOs should have an annual information security evaluation conducted, review the evaluation results with staff, and report on performance to the board of directors.
- Organizations should conduct periodic risk assessments of information assets as part of a risk management program.
- Organizations should implement policies and procedures based on risk assessments to secure information assets.
- Organizations should establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability.
- Organizations should develop plans and initiate actions to provide adequate information security for networks, facilities, systems and information.
- Organizations should treat information security as an integral part of the system life-cycle.
- Organizations should provide information security awareness, training, and education to personnel.
- Organizations should conduct periodic testing and evaluation of the effectiveness of information security policies and procedures.
- Organizations should create and execute a plan for remedial action to address any information security deficiencies.
- Organizations should develop and implement incident response procedures.
- Organizations should establish plans, procedures, and tests to provide continuity of operations.
- Organizations should use security best practices guidance, such as ISO 17799, to measure information security performance.

By stating on their Web site that they embrace information security governance, organizations can help drive a voluntary, private sector effort to strengthen America's cyber security. To ensure that public statements about information security governance are transparent and consistent, industry associations should work with the relevant government agencies to develop standard language and create an ISG logo to accompany these statements.

Recommendation 3:

All organizations that are members of the Corporate Governance Task Force should signal their commitment to information security governance by voluntarily posting a statement on their Web site. In addition, TechNet, the Business Software Alliance, the Information Technology Association of America, the Chamber of Commerce and other leading trade associations and membership organizations should encourage their members to embrace information security governance and post statements on their Web sites. Furthermore, all Summit participants should embrace information security governance and post statements on their Web sites, and, if applicable, encourage their members to do so as well.

To drive compliance with this voluntary effort, all organizations represented on the Corporate Governance Task Force should embrace and implement these recommendations as soon as possible. In doing so, these organizations will set an example for others to follow. Moreover, leading trade associations and membership organizations should publicly endorse information security governance, and encourage their members to do the same. In addition, all National Cyber Security Summit participants should embrace information security governance and post statements on their individual Web sites, and, if applicable, encourage their members to do so as well. To encourage small and medium-sized organizations to embrace information security governance, large enterprises should work with their partners, suppliers and customers to facilitate adoption. By creating a critical mass of interest and commitment—and working with the Department of Homeland Security (DHS) to publicize it—Task Force participants will be able to accelerate adoption of information security governance throughout the private sector.

Recommendation 4:

DHS should endorse the information security governance framework and Core Set of Principles outlined in this report, and encourage the private sector to make cyber security part of its corporate governance efforts.

DHS should launch a public campaign urging organizations to embrace information security governance and recognize those that do so. Unless the DHS champions information security governance, it will be difficult to generate the momentum and enthusiasm necessary for success. To facilitate this effort, DHS should create a program to recognize those organizations that embrace information security governance and post the statement on their Web site. In doing so, DHS will stimulate efforts to make security a core part of the policies and internal controls which constitute an organization's governance efforts. To encourage extensive adoption, DHS should structure their program to reward the widespread information security governance efforts of numerous organizations across several different sectors. The DHS award should be designed to allow small, medium and large enterprises in different sectors to apply. DHS should move rapidly to establish criteria for this prize in order to promote widespread information security governance efforts.

The public recognition that accompanies such a cyber security award is a double-edged sword. Winners enjoy the acclaim associated with it, but they also may fear becoming a potential target for hackers. For this reason, the award should be given to organizations for their information security *governance* efforts—not as an indication of flawless cyber security. The award should be structured so that public recognition is at the discretion of the winner. To make the award attractive to organizations that are concerned about attracting cyber attacks, DHS also should develop non-public incentives. For example, winners could be invited to brief leading private sector and Federal CIOs on their efforts, could be publicly acclaimed for their efforts to protect homeland security without reference to cyber security, and so forth. Organizations that are overly concerned about the notoriety with hackers that may accompany this award can always choose not to apply.

Recommendation 5:

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) should revise the Internal Controls-Integrated Framework so that it explicitly addresses information security governance.

In spite of all the discussion about corporate governance, little attention has been given to the role of IT in the financial reporting process. To establish that internal controls are adequate, it is

essential to take into account IT controls. Auditors are beginning to emphasize that information security be part of the corporate governance compliance process.

Accounting and audit references to "internal controls" are contained in COSO's Internal Controls-Integrated Framework, but as currently written it does not provide a roadmap for information security governance. By revising the COSO guidelines for internal controls so that they provide guidance for information security governance, we can lay the groundwork for the private sector to conduct self-assessments and for auditors to apply these rules consistently. In the absence of such specific guidance, COBIT can serve as a reference, and along with ISO 17799, can provide additional detailed information security governance guidance.

3.0 CONCLUSIONS

The National Strategy to Secure Cyberspace released by the White House in February 2003 outlines the steps necessary for the effective protection of U.S. information assets. Priority III of the Strategy requires the development of a National Cyberspace Security Awareness and Training Program. Including information security in corporate governance programs is the first step for making organizations aware of the importance of sound information security governance.

The Corporate Governance Task Force was convened to "develop and promote a coherent governance framework to drive implementation of effective information security programs" in private sector organizations. In addition to the recommendations and tool set contained in this report, the Task Force plans to promote ISG implementation through an awareness and rollout campaign in the months to come. By using the ISG framework and assessment tools, organizations can integrate information security into their corporate governance programs, and thereby create a safer business community not only for themselves, but also for those enterprises that interact with them.

In this era of increased cyber attacks and information security breaches, it is essential that all organizations give information security the focus it requires. Addressing these cyber and information security concerns, the private sector will not only strengthen its own future security, but the nation's homeland security as well. The Task Force calls on organizations to make information security governance a priority and to use the tools described in this report to develop effective information security governance programs.

APPENDIX A: INFORMATION SECURITY GOVERNANCE FRAMEWORK

1. Introduction and Purpose

1.1. This document provides an overview of the various elements of an information security governance program. It is based on the October 2003 Business Software Alliance report, "Information Security Governance—Toward a Framework for Action." Information security governance is a subset of good organizational governance, which comprises the set of policies and internal controls by which organizations are directed and managed.

1.2. The purpose of this document is to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources; to provide effective management and oversight of the related information security risks; to provide for development and maintenance of minimum controls required to protect an organization's information and information systems; and to provide a mechanism for oversight of the information security program.

1.3. Recognizing that it is not practical to account for every organization type, size, and structure in a single framework, this document is offered in a general form that can be adapted to most organizational structures. The organization leaders must adapt the framework elements to their specific situation, assigning functions to those staff members most capable and appropriate. Additional guidance is offered to assist with this task in companion documents.

1.4. As used in this document, the term information security means protecting information and information systems from unauthorized use, disclosure, disruption, modification, or destruction to provide the following:

- Confidentiality, which means preserving an appropriate level of information secrecy
- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- Availability, which means ensuring timely and reliable access to and use of information.

2. Responsibilities of the Board of Directors/Trustees

The board of directors/trustees or similar governance entity should provide strategic oversight regarding information security, including

2.1. Understanding the criticality of information and information security to the organization.

2.2. Reviewing investment in information security for alignment with the organization strategy and risk profile.

2.3. Endorsing the development and implementation of a comprehensive information security program.

2.4. Requiring regular reports from management on the program's adequacy and effectiveness.

3. Responsibilities of the Senior Executive

The Senior Executive, typically a Chief Executive Officer accountable to the Board of Directors or like entity, should provide oversight of a comprehensive information security program for the entire organization, including

3.1. Assigning the responsibility, accountability and authority for each of the various functions described in this document to appropriate individuals within the organization.

3.2. Overseeing organizational compliance with the requirements of this document, including through any authorized action to enforce accountability for compliance with such requirements.

3.3. Reporting to the board of directors/trustees or similar governance entity on organization compliance with the requirements of this document, including

- A summary of the findings of evaluations, with an indication of the level of residual risk deemed acceptable
- Significant deficiencies in organization information security practices
- Planned remedial action to address such deficiencies.

3.4. Designating an individual to fulfill the role of senior information security officer, who should possess professional qualifications, including training and experience, required to administer the information security program as defined in this document, and head an office with the mission and resources to assist in pursuing organizational compliance with this document.

4. Responsibilities of the Executive Team Members

Specific members of the Executive Team, typically those managers reporting directly to the Senior Executive, should oversee the organization's security policies and practices, including

4.1. Overseeing the development and implementation of policies, principles, standards, and guidelines on information security, consistent with the guidance of accepted security practices such as ISO/IEC 17799, and in section 7 of this document.

4.2. Seeing that information security management processes are integrated with organization strategic and operational planning processes.

4.3. Coordinating information security policies and procedures with related information resources management policies and procedures.

4.4. Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized use, disclosure, disruption, modification, or destruction of information collected or maintained, or information systems used or operated by or on behalf of the organization.

4.5. Seeing that each independent organizational unit develops and maintains an information security program.

4.6. Seeing that the senior information security officer, in coordination with organizational unit heads, reports periodically to the Senior Executive on the effectiveness of their information security program, including the progress of remedial actions.

4.7. Seeing that the senior information security officer assists organizational unit managers concerning their information security responsibilities.

5. Responsibilities of Senior Managers

The head of each independent organizational unit should see that senior organizational unit managers provide information security for the information and information systems that support the operations and assets under their control, including through

5.1. Assessing the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of such information or information systems.

5.2. Implementing policies and procedures that are based on risk assessments and cost-effectively reduce information security risks to an acceptable level.

5.3. Determining the levels of information security appropriate to protect such information and information systems.

5.4. Periodically testing and evaluating information security controls and techniques to see that they are effectively implemented.

5.5. Seeing that the organization has trained personnel sufficient to assist the organization in complying with the requirements of this document and related policies, procedures, standards, and guidelines.

5.6 Seeing that all employees, contractors and other users of information systems are aware of their responsibility to comply with the information security policies, practices and relevant guidance appropriate to their role in the organization.

6. Responsibilities of All Employees and Users

All employees of an organization and, where relevant, third-party users share responsibilities for the security of information and information systems accessible to them, including

6.1. Awareness of the information security policies, practices and relevant guidance appropriate to their role in the organization.

6.2. Compliance with the security policies and procedures related to the information and information systems they use.

6.3. Reporting of vulnerabilities or incidents affecting security or security policy compliance to the appropriate management channels.

7. Organizational Unit Security Program

Each independent organizational unit should develop, document, and implement an information security program, consistent with the guidance of accepted security practices such as ISO/IEC 17799, to provide information security for the information and information systems that support the operations and assets of the organizational unit, including those provided or managed by another organizational unit, contractor, or other source, which includes

7.1. Periodic assessment of the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of such information or information systems.

7.2. Policies and procedures that are based on risk assessments and cost-effectively reduce information security risks to an acceptable level.

7.3. Seeing that information security is addressed throughout the life cycle of each information system.

7.4. Pursuing compliance with the requirements of this document, policies and procedures as may be prescribed by the Senior Executive, and any other applicable legal, regulatory, or contractual requirements.

7.5. Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate.

7.6. Security awareness training to inform personnel, including contractors and other users of information systems who support the operations and assets of the organizational unit, of

- Information security risks associated with their activities
- Their responsibilities in complying with organization policies and procedures designed to reduce these risks.

7.7. Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually.

7.8. A process for pursuing remedial action to address any deficiencies in the information security policies, procedures, and practices.

7.9. Procedures for detecting, reporting, and responding to security incidents, including

- Mitigating risks associated with such incidents before substantial damage is done
- Notifying and consulting with a federal or industry information security incident center
- Notifying and consulting with the corporate disclosure committee, law enforcement agencies, or other companies or organizations in accordance with law.

7.10. Plans and procedures to pursue continuity of operations for information systems that support the operations and assets of the organization.

8. Organizational Unit Reporting

Each independent organizational unit should:

8.1. Report periodically to the appropriate senior executive on the adequacy and effectiveness of the information security program, including compliance with the requirements of this document.

8.2. Address the adequacy and effectiveness of the information security program in the organizational unit's budget, investment, and performance plans and reports.

8.3. Report any significant deficiency in organizational information security practices, planned remedial actions to address such deficiencies, and an indication of the level of residual risk deemed acceptable.

8.4. In consultation with the appropriate senior executive, report as part of the performance plan a description of the time periods, and the resources, including budget, staffing, and training, that are necessary to implement the information security program elements required.

8.5. Provide customers and business partners with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with them.

9. Independent Information Security Program Evaluation

Although not practical for all organization types and sizes, each independent organizational unit should perform a regular evaluation to validate the effectiveness of its information security program.

9.1. Each evaluation by the organizational unit under this section could be performed by an internal auditor or an independent external auditor, and it should include

- Testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the organizational unit's information systems
- An assessment of compliance with the requirements of this document and related information security policies, procedures, standards, and guidelines.

9.2. The evaluation recommended by this section

- Should be performed in accordance with generally accepted auditing standards
- May be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable organizational unit.

9.3. Organizational units and evaluators should take appropriate steps to ensure the protection of related information, which, if disclosed, may adversely affect information security. Such protections should be commensurate with the risk and comply with all applicable laws and regulations.

9.4. The Senior Executive should summarize the results of the evaluations conducted under this section in a report to the Board of Directors/Trustees, or a similar governance entity in which such an entity exists.

Acknowledgements

The Corporate Governance Task Force would like to thank the Business Software Alliance Task Force on information security governance for its initial work in developing this framework. The Task Force owes a special thanks to Mike Sullivan, CIO of Entrust, Inc., for his pioneering efforts to develop the ISG framework. We would also like to thank those on the framework subcommittee who helped in many different ways to develop this framework.

Appendix B ISG FUNCTIONS AND RESPONSIBILITIES

Functional Group	Responsibilities	GENERAL FRAMEWORK				LARGE ENTERPRISE EXAMPLE A								LARGE ENTERPRIS		
		TIER 1 EXEC	TIER 2 EXEC	MID-LVL MANAGER	STAFF/ EMPL	SR EXEC CEO	COO	CIO	EXEC CSO	CRO	DEPT HD	MID-LVL MANAGER	EMPL	SE EXEC CEO	COO	EXEC CIO
SENIOR EXECUTIVE Oversight / Tone The Senior Executive, typically a Chief Executive Officer accountable to the Board of Directors or like entity, should provide oversight of a comprehensive information security program for the entire organization, including:	3.1. assigning the responsibility, accountability and authority for each of the various functions described in this document to appropriate individuals within the organization	●				●								●		
	3.2. overseeing organizational compliance with the requirements of this document, including through any authorized action to enforce accountability for compliance with such requirements	●				●								●		
	"3.3. reporting to the Board of Directors/Trustees, or similar governance entity where such an entity exists, on organization compliance with the requirements of this document, including: · a summary of the findings of evaluations, with an indication of the level of residual risk deemed acceptable; · significant deficiencies in organization information security practices; and · planned remedial action to address such deficiencies."	●				●								●		
	3.4. designating an individual to fulfill the role of senior information security officer, who should possess professional qualifications, including training and experience, required to administer the information security program as defined in this document; and head an office with the mission and resources to assist in ensuring organizational compliance with this document	●				●								●		
EXECUTIVE Program Administration and Policies Specific members of the Executive Team, typically those managers reporting directly to the Senior Executive, should oversee the organization's security policies and practices, including:	4.1. overseeing the development and implementation of policies, principles, standards, and guidelines on information security, consistent with the guidance of accepted security practices, such as ISO/IEC 17799, and in section 7 of this framework document		●						●							●
	4.2. ensuring that information security management processes are integrated with organization strategic and operational planning processes		●						●							●
	4.3. coordinating information security policies and procedures with related information resources management policies and procedures		●						●							●
	4.4. providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized use, disclosure, disruption, modification, or destruction of information collected or maintained, or information systems used or operated by or on behalf of the organization		●				●			●					●	
	4.5. ensure that each independent organizational unit develops and maintains an information security program		●						●							●
	4.6. ensure that the senior information security officer, in coordination with organizational unit heads, report periodically to the Senior Executive on the effectiveness of their information security program, including progress of remedial actions		●						●							●
	4.7. ensure the senior information security officer assist organizational unit managers concerning their information security responsibilities		●						●							●
	5.1. assessing the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of such information or information systems		●	●						●						
	5.2. implementing policies and procedures that are based on risk assessments and cost-effectively reduce information security risks to an acceptable level		●	●						●						
	5.3. determining the levels of information security appropriate to protect such information and information systems;		●	●						●		●				
MID-LEVEL MANAGER Policy Implementation and Execution The head of each independent organizational unit should ensure that senior organizational unit managers provide information security for the information and information systems that support the operations and assets under their control, including through:	5.4. periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented			●								●				
	5.5. ensure that the organization has trained personnel sufficient to assist the organization in complying with the requirements of this document and related policies, procedures, standards, and guidelines			●								●				
	5.6. ensure that all employees, contractors and other users of information systems are aware of their responsibility to comply with the information security policies, practices and relevant guidance appropriate to their role in the organizatio			●					●							●
ALL EMPLOYEES AND USERS Policy Understanding, Compliance, Enforcement All employees of an organization and, where relevant, third party users, share responsibilities for the security of information and information systems accessible to them, including:	6.1. awareness of the information security policies, practices and relevant guidance appropriate to their role in the organization	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	6.2. compliance with the security policies and procedures related to the information and information systems they use	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	6.3. reporting vulnerabilities or incidents affecting security or security policy compliance to the appropriate management channels	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

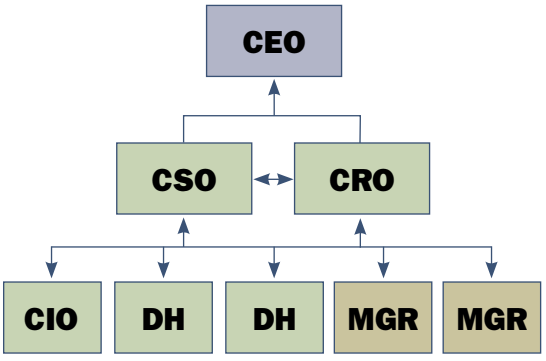
SE EXAMPLE B			LARGE ENTERPRISE EXAMPLE C						LARGE ENTERPRISE EXAMPLE D						MEDIUM ENTERPRISE EXAMPLE						SMALL ENTERPRISE EXAMPLE			PUBLIC AGENCY EXAMPLE				
DEPT HD	MID-LVL MANAGER	EMPL	SE EXEC CEO	COO	EXEC CIO	DEPT HD	MID-LVL MANAGER	EMPL	SE EXEC CEO	COO	EXEC CIO	DEPT HD	MID-LVL MANAGER	EMPL	SE EXEC CEO	COO	EXEC CIO	DEPT HD	MID-LVL MANAGER	EMPL	EXEC	MANAGER	EMPL	DIR	AGENCY HEAD	CIO	SENIOR MGR	STAFF
			●						●						●						●			●				
			●						●						●						●			●				
			●						●						●						●			●				
			●						●						●						●					●		
					●					●						●					●			●				
					●					●						●					●				●			
					●					●					●		●				●			●				
				●						●	●						●				●				●			
					●					●						●						●				●		
					●					●						●	●				●					●		
					●					●						●						●				●		
	●				●						●						●					●				●		
	●				●						●						●					●				●		
	●						●						●						●			●				●		
	●						●						●						●			●				●		
	●						●						●						●			●				●		
													●			●						●					●	
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Information Security Governance

Responsibilities	Functional Role Examples
• Oversee overall "Corporate Security Posture" (Accountable to Board) • Brief board, customers, public	• Chief Executive Officer
• Set security policy, procedures, program, training for Company • Respond to security breeches (investigate, mitigate, litigate) • Responsible for independent annual audit coordination	• Chief Security Officer • Chief Information Officer • Chief Risk Officer • Department/Agency Head
• Implement/audit/enforce/assess compliance • Communicate policies, program (training)	• Mid-Level Manager
• Implement Policy, Report security vulnerabilities and breeches	• Enterprise Staff/Employees

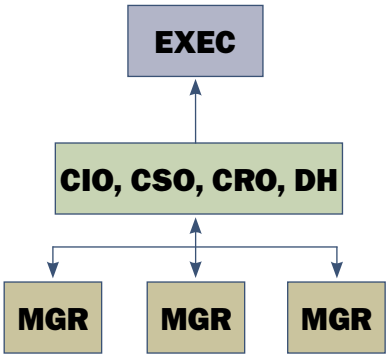
Organizational Function Examples

Larger Enterprise



(Segregation of Duties Maintained)

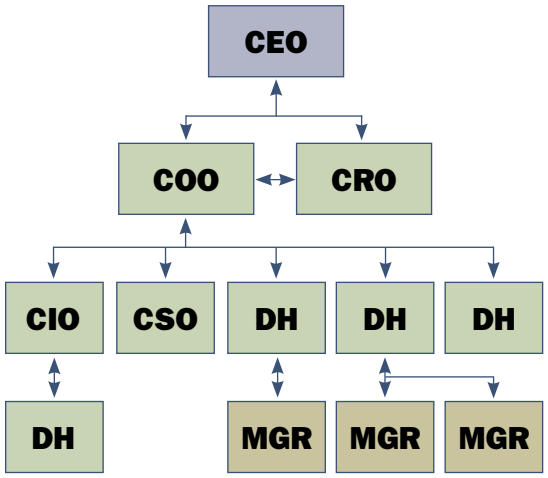
Smaller Enterprise



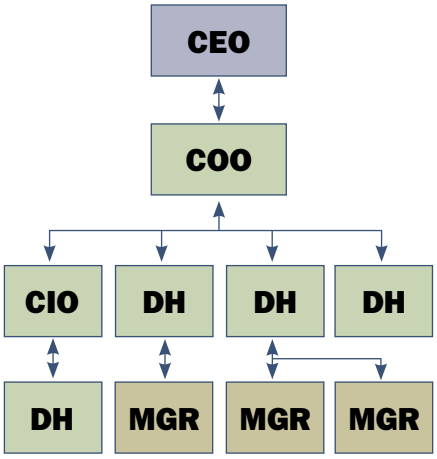
(Segregation of Duties Not Honored)

Additional Organizational Function Examples

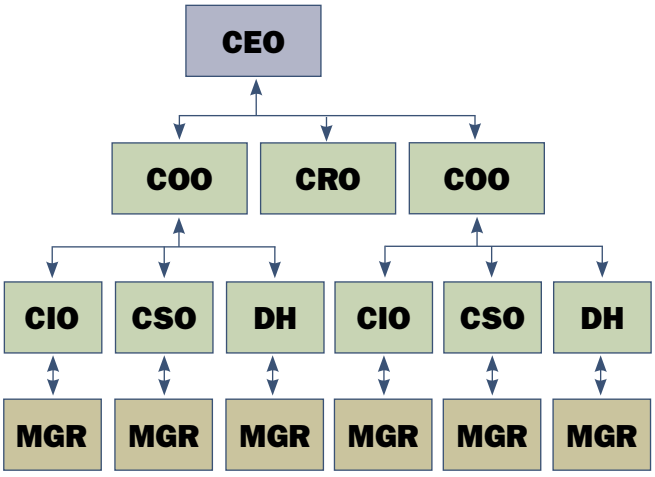
Larger Enterprise Example 1A



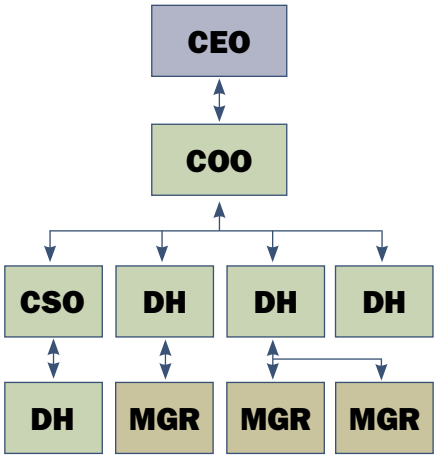
Large Enterprise Example B



Large Enterprise Example 2A

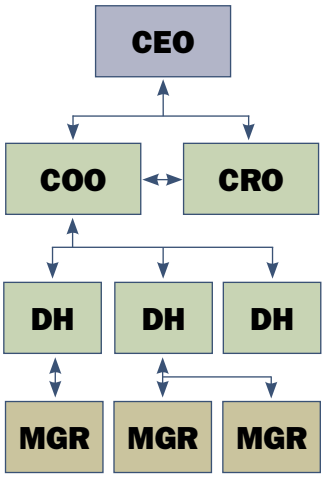


Large Enterprise Example C

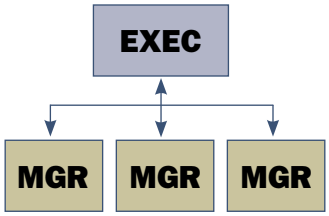


Additional Organizational Function Examples

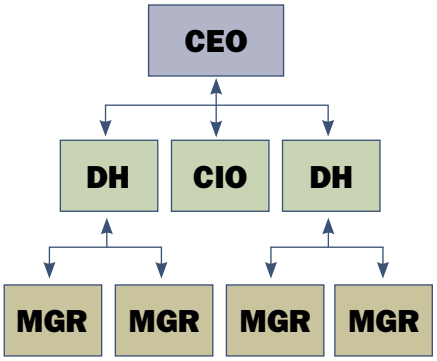
Larger Enterprise Example D



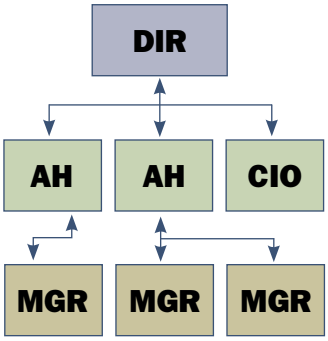
Small Enterprise Example



Medium Enterprise Example



Public Agency Example



APPENDIX C: ORGANIZATION/PROCESS FOR IMPLEMENTATION

Premise

Use an existing model that has been proven in some improvement contexts and could be applied to or tailored for cyber security.

Goals

- Make it stick, that is achieve and sustain selected improvements
- Each organization can see itself in the process
- It could be applied to industry, government, and academia
- It is scaleable

Background on IDEAL Model (or the process for improving the cyber security of an enterprise)

The IDEAL Model v. 1.1, developed by Carnegie Mellon University's Software Engineering Institute, describes an improvement adoption life cycle consisting of five major phases (Initiating, Diagnosing, Establishing, Acting, and Learning). These phases are further divided into 15 activities. Originally developed for software process improvement, IDEAL has been adapted to facilitate any improvement effort, including cyber security. Details may be found at http://www.sei.cmu.edu/ideal/.

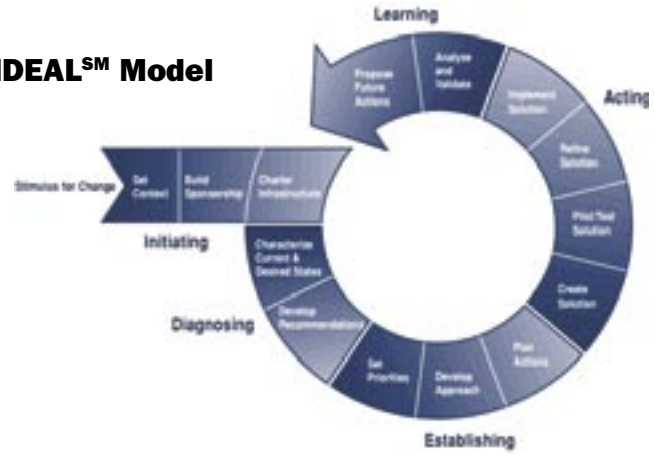
Initiating, Diagnosing, Establishing, Acting, and Learning

The IDEAL[SM1] model is an organizational improvement model that serves as a roadmap for initiating, planning, and implementing improvement actions. The IDEAL model is named for the five phases it describes: initiating, diagnosing, establishing, acting, and learning as follows:

I	**Initiating**	Lay the groundwork for a successful improvement effort.
D	**Diagnosing**	Determine where you are relative to where you want to be.
E	**Establishing**	Plan the specifics of how you will reach your destination.
A	**Acting**	Do the work according to the plan.
L	**Learning**	Learn from the experience and improve your ability to adopt new improvements in the future.

1 IDEAL is a service mark of Carnegie Mellon University. The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

The IDEAL℠ Model



Following are key activities for cyber security process improvements within an organization.

Initiating Phase

Stimulus for Change

The stimulus for change is not technically a part of any activity, but rather it is the condition, event, or direction that indicates that some sort of change is needed. It therefore initiates an IDEAL cycle. In this case, the enterprise CEO or Board of Directors must perceive a need to improve its cyber security posture within the company, for example, an Internet virus infects the company network and it loses production for a period of time. Stimulus also could come from a public campaign to promote cyber security.

Establish Context

This activity involves ensuring that the change under consideration is tied to a key business driver or critical success factor, such as market drivers. This is part of the risk management process to determine what level of risk is acceptable to the organization, knowing who it affects and what mission is affected if the risk is realized. The organization may want a quick evaluation to help justify committing resources and build sponsorship before the more intense risk assessment work.

Build Sponsorship

The information security governance defines who (job function) must be involved for cyber security, for example CEO, or business unit. This is a process of convincing all of these groups that cyber security change is necessary and obtaining their agreement to become active, visible sponsors of the change initiative.

Charter Infrastructure

This activity identifies exactly who will be taking action, including the coordinator for this effort.

Diagnosing Phase

Characterize Current and Desired State

Although the stimulus for change activity, listed above, may have identified one or more problems, the outcome from this activity is a more thorough assessment of the organization's security posture. This is where the assessment tool may be used.

Develop Recommendations

Based on links and resources provided by the tool for specific areas of improvement, the assessment team develops recommendations, that is, the ways and means employed to get from the current state to a desired state.

Establishing Phase

Set Priorities

Prioritization criteria are developed based on business drivers, business area impact, and perhaps a recent risk assessment or audit. Each recommendation is evaluated against the criteria. Priorities could include funding, timely completion, and operational impact. Note that priorities are not always derived from recommendations, for example, employee safety may be a priority but not a recommendation.

Develop Approach

Up to this point, the recommendations are based only upon the results of the Establish Context and Characterize Current and Desired State activities. The approach accounts for recommendations but *expands or alters them as necessary to meet the priorities that have been set for the effort*. Expansion may include requirements for new skills and knowledge to adopt a particular improvement (awareness/training) or aspects of the organization's culture such as sources of resistance and market forces.

Plan Actions

The plan for an improvement effort differs from both the recommendations and the approach both in degree and in substance. First, it *takes the level of detail down* to the point of "brass tacks." Everyone is told what to do, when to do it, how to do it, and so on. Second, it *translates an approach* that exists outside of time and space into a scheduled event that is tied *to specific days and hours*. The execution of the plan is structured and managed like any project with schedules, tasks, assigned responsibilities, committed resources, milestones, decision points, reviews, measurement, status tracking, and risk management.

Acting Phase

Create Solution

This is the procedure or act required to take action and execute the implementation project plan.

Test/Pilot Solution

This activity involves implementing and observing the candidate solution in one or more pilot situations in which the risk can be contained. Notice that this activity should be one of "verification" rather than of "validation." That is, the problems with the proposed solution are identified, but the wider issue of whether the solution itself is the right one is not addressed. In practice, the two often blend and one cannot continually ask the first question without also asking the second. The "Analyze and Validate" activity described below provides a formal opportunity for comparing the solution as implemented against the initial goals.

Refine Solution

Any problems found in the Test/Pilot Solution activity may or may not be corrected; this is a decision made by the project manager/coordinator based on risk, resources, and other business and rollout considerations.

Install Solution

This activity can be repeated more than once; multiple revisions of the solution can occur. But there is a difference between errors in the solution (which were identified and corrected in the past two activities) and errors in implementation.

Learning Phase

Analyze and Validate

The purpose of this activity in any effort is to compare the results of the improvement effort with its goals and requirements, in other words, to determine whether the original objective of the exercise had been met. One purpose of this IDEAL process is to collect and analyze the lessons learned from an effort and apply these to subsequent interactions.

Propose Future Actions

This activity identifies what additional actions need to be planned in the future.

APPENDIX D: ISG ASSESSMENT TOOL

The information security governance (ISG) assessment tool is intended to directly support the ISG framework developed by the Corporate Governance Task Force. It is intended to help a company determine the degree to which it has implemented an information security governance framework at the strategic level within the company. Other tools address the operational and tactical levels of information security. We encourage organizations to examine the available operational and tactical tools to choose the one that works best for their organization. These include International Organization for Standardization-International Electrotechnical Commission 17799-1:200, Control Objectives for Information and Related Technology, FISCAM, and so forth.

This tool is not intended to provide a complete and detailed list of information security policies or practices. Rather, it is intended to help a company identify general areas of concern as they relate to the framework. The tool can assist companies and organizations to identify areas that may be at risk so that they can begin to address those risks.

Purpose of This Tool

This tool is designed to support the ISG framework. The first section of this tool will help a company assess their reliance on information technology. The remaining sections are intended to help a company determine the maturity of information security governance within its organization at a strategic level. The overall rating (Good, Needs Improvement, Poor) will depend on the raw score and a company's dependence on information technology.

The assessment tool, in conjunction with the framework, can be used by organizations of varying sizes and types to gain a better understanding at a high level of the role that information security governance has in the company and how it can best be structured.

Once an item in the assessment tool is noted for improvement we would encourage users 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, there are several references on incident response plans, and there are commercial tools to help with vulnerability assessments.

How To Use This Tool

This tool and the framework were created to evaluate the "people" and "process" components of cyber security and not the "technology" component directly. The tool was intended for use by an organization as a whole although a business unit within an organization could use the tool to help determine the maturity of its individual information security program.

Answer the questions in each section and the total for each section will be automatically provided at the end of each section and following completion of the tool. An overall rating will also be automatically calculated and indicated in the "Overall Security Evaluation Rating" field at the end of the tool.

Acknowledgements

The Corporate Governance Task Force would like to thank TechNet, the creators of the TechNet Corporate Information Security Evaluation for CEOs, for their gracious contribution to this project. The TechNet Corporate Information Security Evaluation served as the starting point for the ISG assessment tool, with the concept, format and many of the questions taken directly from it. The Task Force owes a special thanks to Matt Halbleib of Intel Corporation, Laney Settelmeyer of Intel Corporation and Marilyn Thornton of ALLTEL. Additionally, we would also like to thank those on the Subcommittee who helped in many different ways to develop this tool.

Section I: Business Dependency Evaluation

This section is designed to help you determine whether your company has a high, medium or low reliance on information technology for business continuity. It also considers your degree of sector interdependency and regulation. Your overall security evaluation rating will depend in part on your business dependency.

Scoring: very low = 0; low = 1; medium = 2; high = 3; very high = 4		
1	**Company Characteristics**	
1.1	Gross revenue of the entire company Less than $10 million = very low $10 million to $100 million = low $100 million to $1 billion = medium $1 billion to $10 billion = high More than $10 billion = 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	Dependence upon information technology systems and the Internet to offer products and services to customer	
1.4	Value of company's intellectual property stored or transmitted in electronic form	
1.5	Impact of major system downtime on revenues	
1.6	Degree of change within company (expansions, mergers, acquisitions, divestitures, new markets, etc.)	
1.7	Impact to your business from an Internet outage	
1.8	Dependency on multinational operations for current revenue stream	
1.9	Plans for multinational operations (e.g. outsourced business functions to offshore locations, growing into areas representing increased portions of overall revenue)	
	Industry Characteristics	
1.10	Potential impact to national or critical infrastructure in case of outage or interruption to your systems	
1.11	Customer sensitivity to security and privacy	
1.12	Level of industry regulation regarding security (e.g. GLBA, HIPAA, Sarbanes Oxley, other applicable international or local regulations)	
1.13	Potential brand impact of a security incident	
1.14	Extent of business operations dependent upon third parties (business partners, contractors, suppliers)	

Continue on next page.

Scoring: very low = 0; low = 1; medium = 2; high = 3; very high = 4		
1.15	Customers ability to quickly switch to a competitor, based upon competitor's ability to offer more secure/reliable services	
1.16	Does your company do business in a politically sensitive area? (Would your business be a target of violent physical or cyber attack from any groups?)	
	Total Business Dependency Score	

Section II: Risk Management

This section evaluates 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.

Scoring: 0 = not implemented; 1 = planning stages; 2 = partially implemented; 3 = close to completion; 4 = fully implemented		
2	**Corporate Information Security Risk Assessment**	
2.1	Does your company have an Information Security Program Charter?	
2.2	Has your company conducted a risk assessment to identify the key business objectives that need to be supported by your corporate information security program?	
2.3	Has your company identified critical corporate assets and the business 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 quantifiable cost been assigned to the loss of each critical asset or function?	
2.6	Do you have a written information security strategy that seeks to cost-effectively measure risk and specify actions to manage risk at an acceptable level, with minimal business disruptions?	
2.7	Do you have a written information security strategy that seeks to cost-effectively reduce the risks to an acceptable level, with minimal business disruptions?	
2.8	Is the strategy reviewed and updated at least annually, or more frequently when significant business 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 business?	
	Total Risk Management Score	

Section III: People

This section evaluates the organizational aspects of your information security program.

Scoring: 0 = not implemented; 1 = planning stages; 2 = partially implemented; 3 = close to completion; 4 = fully implemented		
3	**Corporate Information Security Function/Organization**	
3.1	Is there a person or organization that has information security as its 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? *(e.g. CISSP, CISM, CISA certification)*	
3.3	Does your information security function have the authority and resources it needs to manage and ensure compliance with the information security program?	
3.4	Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes, and audits?	
3.5	Has specific responsibility been assigned for the execution of business continuity and disaster recovery plans (either within or outside of the Information Security Department)?	
3.6	Do you have an ongoing training program in place for information security staff?	
3.7	Is someone in the information security organization function responsible for liaising with business units to identify any new security requirements based on changes to the business?	
3.8	Does the information security function actively engage with other critical functions, such as Human Resources and Legal, to develop and enforce compliance with information security policies and practices?	
3.9	Does the information security function report regularly to the executive staff and Board of Directors on the compliance of the business to and the effectiveness of the information security program and policies?	
3.10	Is the executive staff ultimately responsible and accountable for the information security program, including approval of information security policies?	
3.11	Do the business 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?	
3.12	Have you implemented an information security education and awareness program such that all employees, contractors, and external providers know the information security policies that apply to them and understand their responsibilities?	
	Total People Score	

Section IV: Processes

This section identifies the processes that should be part of an information security program.

Scoring: 0 = not implemented; 1 = planning stages; 2 = partially implemented; 3 = close to completion; 4 = fully implemented		
4	**Security Technology Strategy**	
4.1	Does your company 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 business 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 non-compliance?	
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 non-compliance with your official architecture, is there a process and defined time frame 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?	
	Corporate Information Security Policies	
	Based on your information security risk management strategy, do you have written corporate information security policies that address each of the following areas?	
4.8	Individual employee responsibilities for information security practices	
4.9	Acceptable use of computers, e- mail, Internet, and intranet	
4.10	Protection of corporate assets, including intellectual property	
4.11	Managing privacy issues, including excursions or breaches of privacy-related information	
4.12	Identity management, including excursions or breaches of sensitive identity information	
4.13	Access control, authentication, and authorization practices and requirements	
4.14	Data classification, retention, and destruction	
4.15	Information sharing,; including storing and transmitting company data on outside resources (Internet Service Providers, external networks, contractors' systems)	
4.16	Vulnerability management (e.g., patch management, antivirus software)	

Continue on next page.

Scoring: 0 = not implemented; 1 = planning stages; 2 = partially implemented; 3 = close to completion; 4 = fully implemented		
4.17	Disaster recovery and contingency planning (business continuity planning)	
4.18	Incident reporting and response	
4.19	Security compliance monitoring and enforcement	
4.20	Change management processes	
4.21	Physical security and personnel security	
4.22	Are written information security policies consistent, non-technical, easy to understand and readily available to employees, contractors, and partners?	
4.23	Is there a method for communicating security policies to all employees?	
4.24	Are there documented procedures for implementing a policy?	
4.25	Are there documented procedures for granting exceptions to policy?	
4.26	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?	
4.27	Do your security policies effectively address the risks identified in your risk analysis/risk assessments?	
4.28	Are relevant security policies included in all of your third-party contracts?	
4.29	Are consequences for non-compliance with corporate policies clearly communicated and enforced?	
4.30	Are information security issues considered in all the important business decisions within the company (product development, vendor selection, purchasing, etc.)?	
Security Program Administration		
4.31	Does your company periodically test and evaluate/audit your information security program, practices, controls, and techniques to ensure they are effectively implemented?	
4.32	Do you conduct a periodic independent evaluation/audit of your information security program and practices for each business unit?	
4.33	Does each periodic independent evaluation/audit test the effectiveness of information security policies, procedures, and practices of a representative subset of each business unit's information systems?	
4.34	Does each periodic independent evaluation/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?	
	Total Processes Score	

Scoring

Section	Total Score
I Business Dependency	
II Risk Management	
III People	
IV Process	

Results

Low	High	Dependency
0	15	Very low
16	31	Low
32	47	Medium
48	63	High
64	80	Very high

Business Dependency	Program Rating Ranges	Overall Assessment
Very high	0 - 139	Poor
	140 - 179	Needs improvement
	180 - 220	Good
High	0 - 119	Poor
	120 - 164	Needs improvement
	165 - 220	Good
Medium	0 - 99	Poor
	100 - 149	Needs improvement
	150 - 220	Good
Low	0 - 84	Poor
	85 - 134	Needs improvement
	135 - 220	Good
Very low	0 - 69	Poor
	70 - 119	Needs improvement
	120 - 220	Good

APPENDIX E: EDUCATION AND NON-PROFIT IMPLEMENTATION PLAN

The Critical Need for Information Security Governance in Education and Non-profit Institutions.

Information security is a critical issue in education and non-profit (E&NP) institutions as well as in the corporate and government sectors. Though organized on different models and driven by different goals than the corporate sector, the E&NP organizations face similar 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. (They also produce much of the research on information security and educate the security professionals of the future.) In the end, an effective program for information security depends, in the E&NP sector as in the others, on an effective implementation of information security governance.

A number of E&NP institutions have already implemented effective ISG programs and can serve as examples for others. Others are now doing so under the mandates and guidelines of their state governments. This section is intended for institutions that have not yet established a governance structure at the executive level for information and cyber security. It examines and adapts successful recommendations for implementing ISG in the corporate sector to fit the culture and structure of the E&NP organizations. It is intended to provide a good starting point for the successful adoption of ISG, one that can be followed in subsequent steps to support the implementation of appropriate and effective security practices throughout the organization.

Adapting the ISG Recommendations for E&NP Institutions

The ISG framework, tool, process, and verification recommendations for the corporate sector are valid in principle for the E&NP sector, but they cannot be used to best effect without adaptation of the language and some of the recommendations to better fit the structures and operations of the E&NP world. Members of the ISG Subcommittee for the education and non-profit organizations of the Summit will work with major stakeholder organizations such as the EDUCAUSE/Internet2 Task Force on Computer and Network Security to write and vet tailored versions of these documents to achieve a more successful and widespread implementation of ISG in the E&NP sector. The revised documents will be tested in pilot implementations as a next step. The remainder of this section illustrates the changes that must be made for their successful use in E&NP institutions.

Why Consider a Separate Case for Education and Non-profit Institutions?

Most guidelines and standards for information security refer to either government agencies (the Federal Information Security Management Act of 2002) or large corporations (the Business Software Alliance's "Information Security Governance: Toward a Framework for Action," TechNet's "Corporate Information Security Evaluation for CEOs"). These guidelines provide a very useful starting point for E&NP institutions, but may be difficult to introduce because of issues of language and emphasis. The ISG assessment tool of Appendix D, for example, emphasizes phrases such as "impact of downtime on revenues" and "expansions, mergers and acquisitions, new markets" that are not the central focus for risk assessment in the E&NP world. Additional ques-

tions of fit related to the very large degree of decentralization in many large E&NP institutions. In addition, all of these guidelines would be much more effective in E&NP institutions if presented with some additional motivation specific to the sector.

Using the ISG Framework in Education and Non-profit Institutions

The ISG framework recommendations of Appendix A require only minor translations throughout to be effective in E&NP institutions. Although not affecting the underlying content or effect of the framework, these translations would improve the "take-up rate" and simplify implementation by speaking more directly to the intended audience. Following are some examples of such translations:

- **Use E&NP terms such as "dean," or "director," instead of "senior company manager" throughout the document**
- **Use "Board of Regents," "Trustees," "Board of Directors," and so forth as Governance Committee throughout.**
- **Broaden the specific references to the ISO/IEC 17799 standards to a more general phrase such as ""consistent with accepted security practices such as ISO/IEC 17799." Institutions that do not use the ISO/IEC 17799 code of practice directly should be advised to consult it as a guide to the topics covered.**

The thrust of these suggestions is to produce an essentially equivalent framework that speaks the language and invokes the core concerns of the institutional executive in the E&NP world. Successful first-time implementation (in an institution that has not yet implemented an ISG plan) would require considerably more definition, examples, discussion, and motivation. Implementations will vary considerably according to the degree of centralization/decentralization of campus information technology (IT) services and management, but each can be expected to contain the elements of the framework in some form.

Using the ISG Assessment Tool in Education and Non-profit Institutions

The checklist of Appendix D provides a very useful snapshot of specific actions that are required for an effective security program. As with the framework, the checklist would require some translations to be successful in E&NP institutions. Again, these translations would not affect the underlying content or effect of the checklist, but would improve the "take-up rate" and simplify implementation by speaking more directly to the intended audience. The most important changes are on the first page of the checklist, in the Business Dependency Evaluation which seeks to determine how much an institution depends on information security for business, continuity. It also rates the degree of dependence on external regulations and on information exchange with other institutions. Following are several examples:

- **The central concept "Impact of major system downtime on revenues" must become "Impact of downtime on critical company functions such as research, instruction, and constituent service" for the E&NP sector**
- **Other impacts such as liability for lawsuits may prove to be more important as business drivers for ISG in E&NP**

- FERPA regulations can be added to GLBA and HIPAA as an important regulation affecting education. It is important to explain how these requirements affect the top leadership of the institution
- "Potential impact to national or critical infrastructure in case of outage or interruption to your systems" must be expanded to include the launching of denial of service by third parties from compromised systems
- The degree of change within company (expansions, mergers, acquisitions, divestitures, new markets, etc.) becomes (new programs and methods of instruction and research, reaching new student populations, etc.) for the education sector
- We must reword "customers" to "students, patrons, constituents, etc." to resonate with E&NP executives.

As with the framework, the thrust of these suggestions is to produce an essentially equivalent checklist that speaks the language and invokes the core concerns of the institutional executive in the E&NP world. Successful first-time implementation (in an institution that has not yet implemented an ISG plan) would require considerably more definition, discussion, and motivation based on E&NP examples.

Using the Verification and Compliance Recommendations in E&NP

The recommendations for verification and compliance, including the 12-part checklist, are quite appropriate for the E&NP community. Successful introduction would require only minor translations of terminology.

Initial Process for Implementing Information Security Governance in E&NP

It is recognized that some colleges, universities, and non-profit organizations already have an effective governance structure for information security and that some others are well on their way. These recommendations, therefore, are focused on the many institutions that need to start at the beginning. What is needed for the executive leadership of these institutions is not a detailed plan for a full-scale implementation of all aspects of information security. What is needed for executives is a short, "beginner's guide" on how to introduce an ISG program in a step-by-step manner that yields early success while building support and understanding. It must speak the language of executives and focus on their concerns. It can use the good experiences of those who have gone before for motivation and examples, as well as the painful experiences of peer institutions where ISG was too little or too late.

We can learn much about the process from the experience of the U.S. Government in implementing information security in response to federal legislation.

Some keys to successful implementation:

- Do simple, subjective risk assessments, and put your effort into improving security (OMB A-130 Appendix III)
- Express risk in words to make it easier for non-security people to understand, using the formula:

  [vulnerability] could **[threat]** that could **[impact]**.

- **Use a simple High-Moderate-Low (Red-Yellow-Green) ranking (FIPS 199)**
- **Identify your key information systems and business owners (NIST SP800-19)**
- **Use an iterative process, with progressive detail (GAO/AIMD 00-33)**
- **Use a transparent process with summary reporting (GAO/AIMD 98-68).**

This pragmatic, keep-it-simple approach to the initial implementation of ISG is especially apt for the E&NP sector.

The *Effective Security Practices Guide* recently published by EDUCAUSE and Internet2 includes a good overview that shows the sequence of steps to implement an effective security program as well as the relationships between the various parts. See http://www.educause.edu/security/guide/. It contains strongly motivating examples of recent security failures at specific colleges and universities as well as the experiences of successful ISG implementations at peer institutions. The top levels of this guide, only a few pages long, are required reading for E&NP executives who need to implement ISG. (The lower levels of the guide are intended for security professionals, not executives.) The "Preliminary Risk Assessment" section explains why a risk assessment is so important and can serve as motivation for conducting the very rapid, subjective approach of the ISG checklist tool. As in the following example, a URL points to more complete documentation of a particular example:

Arguably, those responsible for information security in colleges and universities are abundantly aware of the risks because they are faced with security breaches regularly. However, this argument actually emphasizes the need for a risk assessment—to help you manage the risks. Many universities are straining to address immediate information security problems and have not had an opportunity to prioritize the risks and develop an overall security strategy. Individuals who are responsible for computer security in higher education instituitions need a method for identifying the most important problems that require the most attention, specifically because they are faced with such a large number of problems. Also, simply addressing immediate problems does not necessarily improve the security of the university in the long term. Without a solid security strategy, it is likely that solutions will be driven by technology rather than by the needs of the university. A preliminary risk assessment can help form an institutional security strategy, potentially leading to the creation of an information security department, the redesign of IT infrastructure, and other major changes to improve security.

Effective Security Practice: UC Berkeley (http://www.educause.edu), improving computer and network security—the progression from raising security awareness, to developing an information security group, to implementing IT security policy (1994–2003).

By highlighting problems that pose the greatest risk to the operation of the institution, a preliminary risk assessment can help drive more a detailed risk analysis of critical systems or processes, and it can help you obtain resources for solutions to the most pressing security problems. In short, a preliminary risk assessment forms the foundation of an effective security program.

The preliminary risk assessment, in turn, can generate the allies and cooperation required for more extensive risk analyses. This on-line Effective Practices Guide can be used again at successive levels to expand the new security implementation beyond ISG and risk assessment to the entire range of effective security practices. After it has completed the initial steps successfully, a large institution may wish to consider a formal methodology for institutional improvement (e.g., the IDEAL process recommended for the corporate sector) to better organize the process. However, such formalized management methods may never be adopted in some E&NP institutions, because of size and culture. This need not preclude the successful implementation of ISG and information security itself.

Finally, there is a recent history of "peer pressure" on college and university presidents to implement ISG and an effective security plan. The following letter was sent from the president of the American Council on Education.

American Council on Education

Letter to Presidents Regarding Cyber security

February 28, 2003

Dear Colleague:

Campus computers and networks are now essential to your education, research, and business operations. As you know, security failures in those computers and networks can disrupt your entire enterprise and create legal or other liabilities. We've all seen the headlines: grades and salary records altered; medical information and social security numbers exposed to the public; major commercial web sites attacked by hackers using campus computers as a launching point; and massive invasions by Internet worms.

Although maintaining Cyber security is a complex problem, only a small part of the solution comes from hardware and software. As with any major institutional initiative, success depends on education, resources, people, management, policies, and, above all, leadership. As the President of your institution, you have an essential role to play in the effective deployment of computer and network security on your campus. I urge you to start with these steps:

Set the tone: ensure that all campus stakeholders know that you take Cyber security seriously. Insist on community-wide awareness and accountability.

Establish responsibility for campus-wide Cyber security at the cabinet level. At a large university, this responsibility might be assigned to the Chief Information Officer. At a small college, this person may have responsibility for many areas, including the institutional computing environment.

Ask for a periodic Cyber security risk assessment that identifies the most important risks to your institution. Manage these risks in the context of institutional planning and budgeting.

Request updates to your Cyber security plans on a regular basis in response to the rapid evolution of the technologies, vulnerabilities, threats, and risks.

The National Strategy to Secure Cyberspace was released on February 14, 2003, and is available at http://www.securecyberspace.gov. For the past year, EDUCAUSE and Internet2 have been working with the President's Critical Infrastructure Protection Board and White House staff to develop Cyber security recommendations and effective practices for the nation's higher education sector in the context of the National Strategy. Faculty, administrators, and security professionals from a wide variety of colleges and universities met in four NSF-funded workshops during the past six months to explore solutions that minimize security problems without compromising academic values. The Task Force also commissioned a Washington, D.C. law firm to develop a legal memo regarding Legal Issues for IT Security at Colleges and Universities. Final versions of the workshop reports, details of the recommendations, and the legal memo will be available shortly at the Task Force Web site at http://www.educause.edu/security.

It is my hope that our community, by working together, can become part of the solution to this national security risk while better serving our own institutions' goals.

Sincerely,

David Ward, President

Recommended Outline of a Guide for Implementing ISG in E&NP

1. Overview of guide

2. Critical need for action

a. Real examples of significant damage to institutions from failures in E&NP (from Effective Practices Guide)

b. Rising tide of intrusions, worms, and viruses

c. Risks and costs of losing business continuity

d. Threat of financial and even criminal liability for the institution and its leaders (white paper on legal issues of higher education IT security, http://www.educause.edu/ir/library/pdf/CSD2746.pdf)

e. Threats to the national security (National Strategy to Secure Cyberspace)

f. Analogy to health insurance

3. Why ISG is essential at the executive level

a. Requires institutional commitment

b. Framework document

c. Letter from David Ward to college presidents

4. What to do first

a. Form initial executive-level team of major stakeholders for executive awareness and education. Include CIO and CSO if they exist or those with most similar responsibilities. (Effective Practices Guide)

b. Review executive-level EDUCAUSE book, "*Computer and Network Security in Higher Education*," and example implementations

c. Review regulations and other mandates (e.g., state security standards, HIPAA, GLB, FERPA)

d. Assign responsibility for initial risk assessment (framework)

e. Conduct a quick, subjective, top-level risk assessment (ISG tool)

f. Report process and status to the Board

g. Build team of those leaders required to implement the next level

5. Then iterate

a. Address most serious problems from completed risk assessment—ISG, policy, responsibility, budget, education and awareness, technology. This will lead to further definition of ISG roles and responsibilities. (framework, Effective Practices Guide)

b. Retake the checklist (ISG tool)

c. Report to the Board and the community

d. Extend the risk assessment to the next level (Effective Practices Guide)

6. Formalize process as required (consultants, models)

The ISG Subcommittee for the Education and Non-profit Organizations of the Summit will work with major stakeholder organizations such as the EDUCAUSE/Internet2 Task Force on Computer and Network Security to write and vet tailored versions of these documents to achieve a more successful and widespread implementation of ISG in the E&NP sector. The revised documents will be tested in pilot implementations as a next step.

APPENDIX F: INFORMATION SECURITY GOVERNANCE BIBLIOGRAPHY

–American Institute of Certified Public Accountants, Inc. and the Canadian Institute of Chartered Accountants. "Trust Services—WebTrust and SysTrust".

–Business Industry Advisory Council/International Chamber of Commerce, "Information Security Assurance for Executives: An International Business Commentary on the 2002 OECD Guidelines for the 'Security of Networks and Information Systems: Towards a Culture of Security'," April 22, 2003.

–Business Roundtable, "Building Security in the Digital Resource: An Executive Resource," November 2002.

–Business Roundtable, "Information Security Addendum to Principles of Corporate Governance," announced April 2003.

–General Accounting Office, "Federal Information System Controls Audit Manual," January 1999.

–Heinman, Don, "Public Sector Information Security: A Call to Action for Public-Sector CIOs. IBM Endowment for the Business of Government," October 2002.

–Information Security Forum, "The Standard of Good Practice for Information Security," Version 4, March 2003.

–Information Systems Security Association (ISSA), "The Generally Accepted Information Security Principles (GAISP)", in preparation.

–Information Technology Committee of the International Federation of Accountants, "International Information Technology Guidelines – Managing Security of Information," January 1998.

–Information Technology Governance Institute, "COBIT Management Guidelines" July 2000.

–Information Technology Governance Institute and the Information Systems Audit and Control Association, "COBIT Quickstart," September 2003.

–Information Technology Governance Institute, "Control Objectives for Information and related Technology (COBIT)," 3rd edition, July 2000.

–Information Technology Governance Institute, "Information Security Governance: Guidance for Boards of Directors and Executive Management," 2001.

–Information Technology Governance Institute, "Board Briefing on IT Governance," 2nd edition, 2003.

–Institute of Internal Auditors, "Information Security Management and Assurance: A Call to Action for Corporate Governance," 2000.

–Institute of Internal Auditors "Information Security Governance: What Directors Need to Know," 2001.

–Information Technology Governance Institute and the Information Systems Audit and Control Association, "IT Control Objectives for Sarbanes Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Disclosure and Financial Reporting (Discussion Document)," 2003.

–Information Technology Governance Institute and the Information Systems Audit and Control Association, "IT Governance Implementation Guide," September 2003.

–International Chamber of Commerce, "ICC Handbook on Information Security Policy for Small to Medium Enterprises," April 11, 2003.

–International Information Security Foundation, "Generally Accepted System Security Principles," Fall 2000.

–International Standards Organization (ISO) and the International Electrotechnical Commission (IEC), "Code of Practice for Information Security," (ISO/IEC 17799) May 5, 2003 (final coordination draft).

–Internet Security Alliance, "Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices," 1st edition, July 2002.

–National Association of Corporate Directors, "Information Security Oversight: Essential Board Practices," December 2001.

–National Institute of Standards and Technology, "Automated Information Security Program Review Areas," July 27, 2002.

–National Institute of Standards and Technology, "Generally Accepted Principles and Practices for Security Information Technology Systems," September 1996.

–Organization of Economic Cooperation and Development, "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security," adopted 25 July 2002.

–The Technology Network (TechNet), "TechNet Corporate Information Security Evaluation for CEOs," www.technet.org/cybersecurity.

–U.S. Congress, "Federal Information Security Management Act of 2002 (FISMA)", 2002.

–The World Bank, (Thomas Glaessner, Tom Kellermann, and Valerie McNevin), "Electronic Security: Risk Mitigation in Financial IT Transactions," June 2002.