United States General Accounting Office

GAO

Accounting and Information Management Division

May 1998

Executive Guide

Information Security Management

Learning From Leading Organizations

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	5/1/1998	Report 5/1/1998

4. TITLE AND SUBTITLE
Executive Guide: Information Security Management, Learning from Leading Organizations

5. FUNDING NUMBERS

6. AUTHOR(S)
GAO

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

United States General
Accounting Office

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

Increased computer interconnectivity and the popularity of the Internet are offering organizations of all types unprecedented opportunities to improve operations by reducing paper processing, cutting costs, and sharing information. However, the success of many of these efforts depends, in part, on an organization's ability to protect the integrity, confidentiality, and availability of the data and systems it relies on.

14. SUBJECT TERMS
IATAC Collection, information security

15. NUMBER OF PAGES
69

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Preface

Increased computer interconnectivity and the popularity of the Internet are offering organizations of all types unprecedented opportunities to improve operations by reducing paper processing, cutting costs, and sharing information. However, the success of many of these efforts depends, in part, on an organization's ability to protect the integrity, confidentiality, and availability of the data and systems it relies on.

Deficiencies in federal information security are a growing concern. In a February 1997 series of reports to the Congress, GAO designated information security as a governmentwide high-risk area. In October 1997, the President's Commission on Critical Infrastructure Protection described the potentially devastating implications of poor information security from a broader perspective in its report entitled Critical Foundations: Protecting America's Infrastructures. Since then, audit reports have continued to identify widespread information security weaknesses that place critical federal operations and assets at risk.

Although many factors contribute to these weaknesses, audits by GAO and Inspectors General have found that an underlying cause is poor security program management. To help identify solutions to this problem, Senators Fred Thompson and John Glenn, Chairman and Ranking Minority Member, respectively, of the Senate Committee on Governmental Affairs, requested that we study organizations with superior security programs to identify management practices that could benefit federal agencies. This guide outlines the results of that study. It is intended to assist federal officials in strengthening their security programs, and we are pleased that it has been endorsed by the federal Chief Information Officers Council.

This guide is one of a series of GAO publications, listed in appendix I, that are intended to define actions federal officials can take to better manage their information resources. It was prepared under the direction of Jack L. Brock, Director, Governmentwide and Defense Information Systems, who can be reached at 202-512-6240 or *brockj.aimd@gao.gov*.

Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division

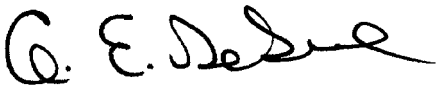
A Message From the Federal Chief Information Officers Council

Washington
April 7, 1998

A high priority of the CIO Council is to ensure the implementation of security practices within the Federal government that gain public confidence and protect government services, privacy, and sensitive and national security information. This Executive Guide, "Information Security Management, Learning From Leading Organizations," clearly illustrates how leading organizations are successfully addressing the challenges of fulfilling that goal. These organizations establish a central management focal point, promote awareness, link policies to business risks, and develop practical risk assessment procedures that link security to business needs. This latter point--the need to link security to business requirements--is particularly important, and is illustrated in a statement of a security manager quoted in the guide: "Because every control has some cost associated with it, every control needs a business reason to be put in place."

The CIO Council is pleased to endorse the principles and best practices embodied in this guide. Its findings underscore the policies articulated in Appendix III to OMB Circular A-130, "Security of Federal Automated Information Resources." We expect that it will be a valuable resource for all agency CIOs and program managers who execute those policies, and will complement the other activities of the Council to improve Federal information systems security.

We look forward to working with the General Accounting Office in the future as we implement these best practices to further enhance agency security practices and programs.



G. Edward DeSeve
Acting Deputy Director for Management
U.S. Office of Management and Budget
and Chair, CIO Council

James J. Flyzik
Chief Information Officer
U.S. Department of the Treasury
and Vice Chair, CIO Council

Contents

Abbreviations

CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISSP	Certified Information Systems Security Professional
GAO	General Accounting Office
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

Federal Information Security Is A Growing Concern

Electronic information and automated systems are essential to virtually all major federal operations. If agencies cannot protect the availability, integrity, and, in some cases, the confidentiality, of this information, their ability to carry out their missions will be severely impaired. However, despite the enormous dependence on electronic information and systems, audits continue to disclose serious information security weaknesses. As a result, billions of dollars in federal assets are at risk of loss, vast amounts of sensitive data are at risk of inappropriate disclosure, and critical computer-based operations are vulnerable to serious disruptions.

This guide is designed to promote senior executives' awareness of information security issues and to provide information they can use to establish a management framework for more effective information security programs. Most senior federal executives, like many of their private sector counterparts, are just beginning to recognize the significance of these risks and to fully appreciate the importance of protecting their information resources. The opening segments describe the problem of weak information security at federal agencies, identify existing federal guidance, and describe the issue of information security management in the context of other information technology management issues. The remainder of the guide describes 16 practices, organized under five management principles, that GAO identified during a study of nonfederal organizations with reputations for having good information security programs. Each of these practices contains specific examples of the techniques used by these organizations to increase their security program's effectiveness.

Potential Risks Are Significant

Although they have relied on computers for years, federal agencies, like businesses and other organizations throughout the world, are experiencing an explosion in the use of electronic data and networked computer systems. As a result, agencies have become enormously dependent on these systems and data to support their operations.

The Department of Defense, alone, has a vast information infrastructure that includes 2.1 million computers and over 10,000 networks that are used to

exchange electronic messages, obtain data from remote computer sites, and maintain critical records. Civilian agencies also are increasingly reliant on automated, often interconnected, systems, including the Internet, to support their operations. For example,

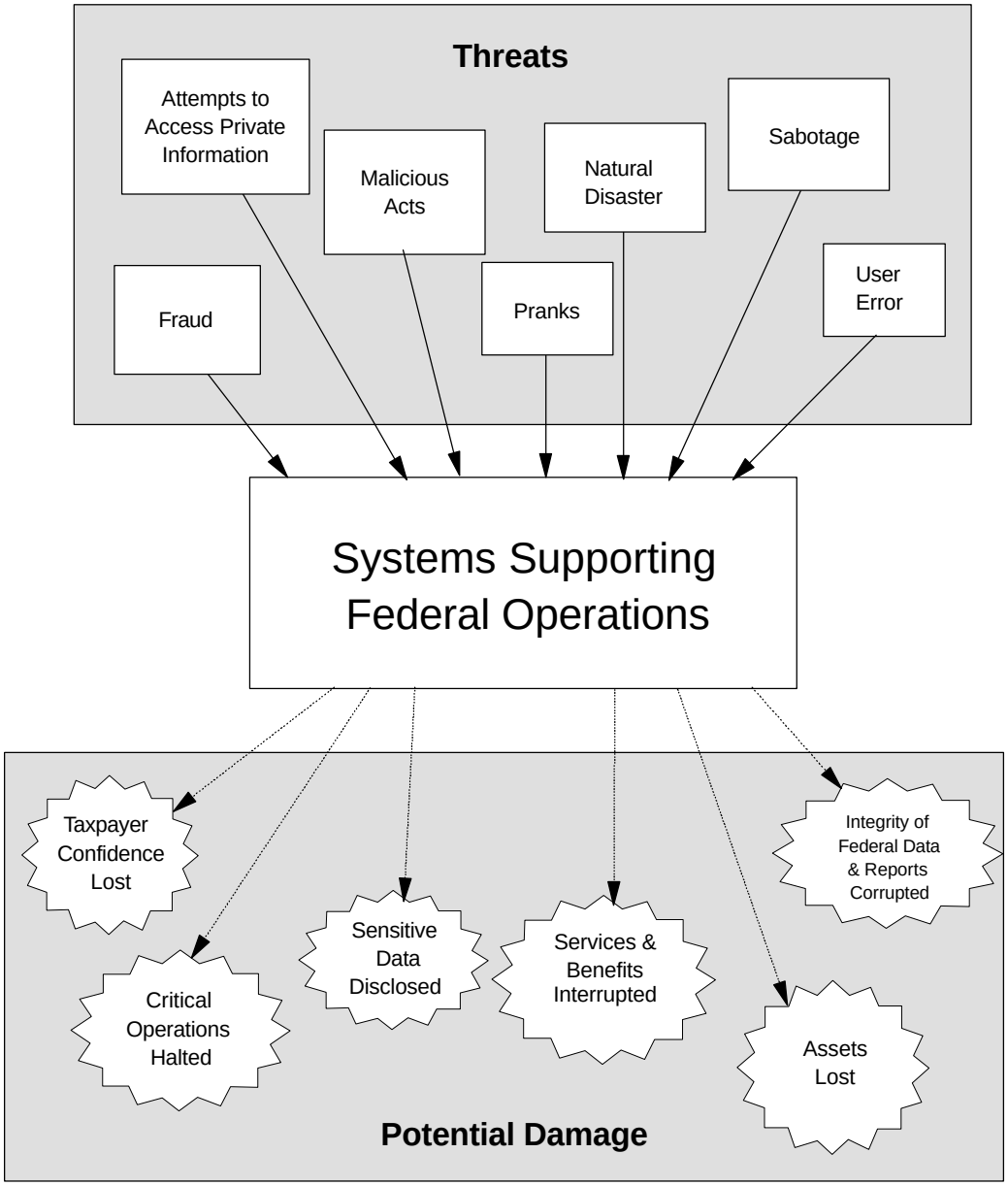
- law enforcement officials throughout the United States and Canada rely on the Federal Bureau of Investigation's National Crime Information Center computerized database for access to sensitive criminal justice records on individual offenders;
- the Internal Revenue Service relies on computers to process and store hundreds of millions of confidential taxpayer records;
- the Customs Service relies on automated systems to support its processing and inspection of hundreds of billions of dollars worth of imported goods; and
- many federal agencies, such as the Social Security Administration, the Department of Agriculture, and the Department of Health and Human Services, rely on automated systems to manage and distribute hundreds of billions of dollars worth of payments to individuals and businesses, such as medicare, social security, and food stamp benefits.

Although these advances promise to streamline federal operations and improve the delivery of federal services, they also expose these activities to greater risks. This is because automated systems and records are fast replacing manual procedures and paper documents, which in many cases are no longer available as "backup" if automated systems should fail.

This risk is exacerbated because, when systems are interconnected to form networks or are accessible through public telecommunication systems, they are much more vulnerable to anonymous intrusions from remote locations. Also, much of the information maintained by federal agencies, although unclassified, is extremely sensitive, and many automated operations are attractive targets for individuals or organizations with malicious intentions, such as committing fraud for personal gain or sabotaging federal operations. Several agencies have experienced intrusions into their systems, and there are indications, such as tests at the Department of Defense, that the number of attacks is growing and that many attacks are not detected.

Additional risks stem from agency efforts to examine and adjust their computer systems to ensure that they properly recognize the Year 2000. These Year 2000 conversion efforts are often conducted under severe time constraints that, without adequate management attention, could result in a weakening of controls over the integrity of data and programs and over the confidentiality of sensitive data.

Information Security Risks



Weaknesses Abound, but Management Attention Has Been Lacking

> *"Just as in the private sector, many federal agencies are reluctant to make the investments required in this area [of computer security] because of limited budgets, lack of direction and prioritization from senior officials, and general ignorance of the threat."*
>
> -- Statement of Gary R. Bachula, Acting Under Secretary for Technology, Department of Commerce, before House Science Subcommittee on Technology, June 19, 1997

Unfortunately, federal agencies are not adequately protecting their systems and data. In September 1996, we reported that audit reports and agency self-assessments issued during the previous 2 years showed that weak information security was a widespread problem.[1] Specifically, weaknesses such as poor controls over access to data and inadequate disaster recovery plans increased the risk of losses, inappropriate disclosures, and disruptions in service associated with the enormous amounts of electronically maintained information essential for delivering federal services and assessing the success of federal programs. Due to these previously reported weaknesses and findings resulting from our ongoing work, in February 1997, we designated information security as a new governmentwide high-risk issue.[2]

In our September 1996 report, we stated that an underlying cause of federal information security weaknesses was that agencies had not implemented information security programs that (1) established appropriate policies and controls and (2) routinely monitored their effectiveness. Despite repeated reports of serious problems, senior agency officials had not provided the management attention needed to ensure that their information security programs were effective.

Also, in that report, we made a number of recommendations intended to improve the Office of Management and Budget's (OMB) oversight of agency information security practices and strengthen its leadership role in this area. Specifically, we recommended that OMB promote the federal Chief Information Officers Council's adoption of information security as one of its top priorities and encourage the council to develop a strategic plan for increasing awareness of the importance of information security, especially among senior agency executives, and improving information security program management

---

[1] Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996).

[2] High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

governmentwide. Initiatives that we suggested for the CIO Council to consider incorporating in its strategic plan included

- developing information on the existing security risks associated with nonclassified systems currently in use,
- developing information on the risks associated with evolving practices, such as Internet use,
- identifying best practices regarding information security programs so that they can be adopted by federal agencies,
- establishing a program for reviewing the adequacy of individual agency information security programs using interagency teams of reviewers,
- ensuring adequate review coverage of agency information security practices by considering the scope of various types of audits and reviews performed and acting to address any identified gaps in coverage,
- developing or identifying training and certification programs that could be shared among agencies, and
- identifying proven security tools and techniques.

Since September 1996, the CIO Council, under OMB's leadership, has taken some significant actions, which include designating information security as one of six priority areas and establishing a Security Committee. The Security Committee, in turn, has developed a preliminary plan for addressing various aspects of the problem, established links with other federal entities involved in security issues, held a security awareness day for federal officials, and begun exploring ways to improve federal incident response capabilities.

Although there is more that OMB and the CIO Council can do, information security is primarily the responsibility of individual agencies. This is because agency managers are in the best position to assess the risks associated with their programs and to develop and implement appropriate policies and controls to mitigate these risks. Accordingly, in our reports over the last several years, we have made dozens of specific recommendations to individual agencies. Although many of these recommendations have been implemented, similar weaknesses continue to surface because agencies have not implemented a management framework for overseeing information security on an agencywide and ongoing basis. A list of our previous reports and testimonies on information security is provided at the end of this guide.

Requirements Are Outlined in Laws and Guidance

The need for federal agencies to protect sensitive and critical, but unclassified, federal data has been recognized for years in various laws, including the Privacy Act of 1974, the Paperwork Reduction Act of 1995, and the Computer

Security Act of 1987. Further, since enactment of the original Paperwork Reduction Act in 1980, OMB has been responsible for developing information security guidance and overseeing agency practices, and the Computer Security Act assigns the National Institute of Standards and Technology (NIST) primary responsibility for developing technical standards and providing related guidance. OMB, NIST, and agency responsibilities regarding information security were recently reemphasized in the Clinger-Cohen Act of 1996, formerly named the Information Technology Management Reform Act of 1996. The adequacy of controls over computerized data is also addressed indirectly by the Federal Managers' Financial Integrity Act of 1982 and the Chief Financial Officers Act of 1990. The Federal Managers' Financial Integrity Act requires agency managers to annually evaluate their internal control systems and report to the President and the Congress any material weaknesses that could lead to fraud, waste, and abuse in government operations. The Chief Financial Officers Act requires agencies to develop and maintain financial management systems that provide complete, reliable, consistent, and timely information.

In addition, a considerable body of federal guidance on information security has been developed. OMB has provided guidance since 1985 in its Circular A-130, Appendix III, Security of Federal Automated Information Resources, which was updated in February 1996. Further, NIST has issued numerous Federal Information Processing Standards, as well as a comprehensive description of basic concepts and techniques entitled An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, December 1995, and Generally Accepted Principles and Practices for Securing Information Technology Systems,[3] published in September 1996.

Additional federal requirements have been established for the protection of information that has been classified for national security purposes. However, these requirements are not discussed here because this guide pertains to the protection of sensitive but unclassified data, which constitute the bulk of data supporting most federal operations.

Exploring Practices of Leading Organizations

To supplement our ongoing audit work at federal agencies and gain a broader understanding of how information security programs can be successfully implemented, we studied the management practices of eight nonfederal

[3]Appendix II lists the principles identified in NIST's Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996.

organizations recognized as having strong information security programs. The specific objective of our review was to determine how such organizations have designed and implemented their programs in order to identify practices that could be applied at federal agencies.

We focused primarily on the management framework that these organizations had established rather than on the specific controls that they had chosen, because previous audit work had identified security management as an underlying problem at federal agencies. Although powerful technical controls, such as those involving encryption, are becoming increasingly available to facilitate information security, effective implementation requires that these techniques be thoughtfully selected and that their use be monitored and managed on an ongoing basis. In addition, there are many aspects of information security, such as risk assessment, policy development, and disaster recovery planning, that require coordinated management attention.

To identify leading organizations, we reviewed professional literature and research information and solicited suggestions from experts in professional organizations, nationally known public accounting firms, and federal agencies. In selecting organizations to include in our study, we relied primarily on recommendations from the Computer Security Institute and public accounting firms because they were in a position to evaluate and compare information security programs at numerous organizations. In addition, we attempted to select organizations from a variety of business sectors to gain a broad perspective on the information security practices being employed. After initial conversations with a number of organizations, we narrowed our focus to eight organizations that had implemented fairly comprehensive organizationwide information security programs. All were prominent nationally known organizations. They included a financial services corporation, a regional electric utility, a state university, a retailer, a state agency, a nonbank financial institution, a computer vendor, and an equipment manufacturer. The number of computer users at these organizations ranged from 3,500 to 100,000, and four had significant international operations. Because most of the organizations considered discussions of their security programs to be sensitive and they wanted to avoid undue public attention on this aspect of their operations, we agreed not to identify the organizations by name.

We obtained information primarily through interviews with senior security managers and document analysis conducted during and after visits to the organizations we studied. In a few cases, we toured the organizations' facilities and observed practices in operation. We supplemented these findings, to a very limited extent, with information obtained from others. For example, at the state agency, we also met with a statewide security program official and with state auditors. In addition, we asked the Computer Security Institute to

query its members about their efforts to measure the effectiveness of their security programs in order to gain a broader perspective of practices in this area.

To determine the applicability of the leading organization's practices to federal agencies, we discussed our findings with numerous federal officials, including officials in OMB's Information Policy and Technology Branch, the Computer Security Division of NIST's Information Technology Laboratory, CIO Council members, the chairman of the Chief Financial Officers Council's systems subcommittee, information security officers from 15 federal agencies, and members of the President's Commission on Critical Infrastructure Protection. Further, we discussed our findings with our Executive Council on Information Management and Technology, a group of executives with extensive experience in information technology management who advise us on major information management issues affecting federal agencies.

Throughout the guide, we make several observations on federal information security practices in order to contrast them with the practices of the non-federal organizations we studied. These observations are based on the body of work we have developed over the last several years and on our recent discussions with federal information security officers and other federal officials who are knowledgeable about federal information security practices.

Although we attempted to be as thorough as possible within the scope of our study, we recognize that more work in this area remains to be done, including a more in-depth study of individual practices. We also recognize that the practices require customized application at individual organizations depending on factors such as existing organizational strengths and weaknesses.

Security as an Element of a Broader Information Management Strategy

Although this guide focuses on information security program management, this is only one aspect of an organization's overall information management strategy. As such, an organization's success in managing security-related efforts is likely to hinge on its overall ability to manage its use of information technology. Unfortunately, federal performance in this broader area has been largely inadequate. Over the past 6 years, federal agencies have spent a reported $145 billion on information technology with generally disappointing mission-related results.

Recognizing the need for improved information management, the Congress has enacted legislation that is prompting landmark reforms in this area. In

particular, the Paperwork Reduction Act of 1995 emphasized the need for agencies to acquire and apply information resources to effectively support the accomplishment of agency missions and the delivery of services to the public. The Clinger-Cohen Act of 1996 repeated this theme and provided more detailed requirements. These laws emphasize involving senior executives in information management decisions, appointing senior-level chief information officers, and using performance measures to assess the contribution of technology in achieving mission results. Although their primary focus is much broader, both of these laws specify security as one of the aspects of information management that must be addressed. This environment of reform is conducive to agencies rethinking their security programs, as part of broader information management changes, and considering the implementation of the practices that have been adopted by nonfederal organizations.

Other Issues Affecting Federal Information Security

Security program management and the related implementation of controls over access to data, systems, and software programs, as well as service continuity planning, are central factors affecting an organization's ability to protect its information resources and the program operations that these resources support. However, there are numerous policy, technical, legal, and human resource issues that are not fully within the control of officials at individual agencies. These issues are currently being debated and, in many cases, addressed by private-sector and federal efforts. They include, but are not limited to, matters concerning (1) the use of encryption to protect the confidentiality of information and other cryptographic capabilities, including digital signatures and integrity checks, (2) personal privacy, (3) the adequacy of laws protecting intellectual property and permitting investigations into computer-related crimes, and (4) the availability of adequate technical expertise and security software tools.

These topics are beyond the scope of this guide and, thus, are not discussed herein. However, it is important to recognize that strengthening information security requires a multifaceted approach and sometimes involves issues that are beyond the control of individual businesses and agencies. Although the management practices described in this guide are fundamental to improving an organization's information security posture, they should be considered in the context of this broader spectrum of issues.

Leading Organizations Apply Fundamental Risk Management Principles

The organizations we studied were striving to manage the same types of risks that face federal agencies. To do so, they had responded to these risks by reorienting their security programs from relatively low-profile operations focused primarily on mainframe security to visible, integral components of their organizations' business operations. Because of the similarities in the challenges they face, we believe that federal entities can learn from these organizations to develop their own more effective security programs.

Federal and Nonfederal Entities Face Similar Risks and Rely on Similar Technologies

Like federal agencies, the organizations we studied must protect the integrity, confidentiality, and availability of the information resources they rely on. Although most of the organizations were private enterprises motivated by the desire to earn profits, their information security concerns focused on providing high-quality reliable service to their customers and business partners, avoiding fraud and disclosures of sensitive information, promoting efficient operations, and complying with applicable laws and regulations. These are the same types of concerns facing federal agencies.

Also, like federal agencies, the organizations relied, to varying degrees, on a mix of mainframe and client-server systems and made heavy use of interconnected networks. In addition, all were either using or exploring the possibilities of using the Internet to support their business operations.

Information Security Objectives Common to Federal and Nonfederal Entities

- Maintain customer, constituent, stockholder, or taxpayer confidence in the organization's products, services, efficiency, and trustworthiness
- Protect the confidentiality of sensitive personal and financial data on employees, clients, customers, and beneficiaries
- Protect sensitive operational data from inappropriate disclosure
- Avoid third-party liability for illegal or malicious acts committed with the organization's computer or network resources
- Ensure that organizational computer, network, and data resources are not misused or wasted
- Avoid fraud
- Avoid expensive and disruptive incidents
- Comply with pertinent laws and regulations
- Avoid a hostile workplace atmosphere that may impair employee performance

Risk Management Principles Provide A Framework for an Effective Information Security Program

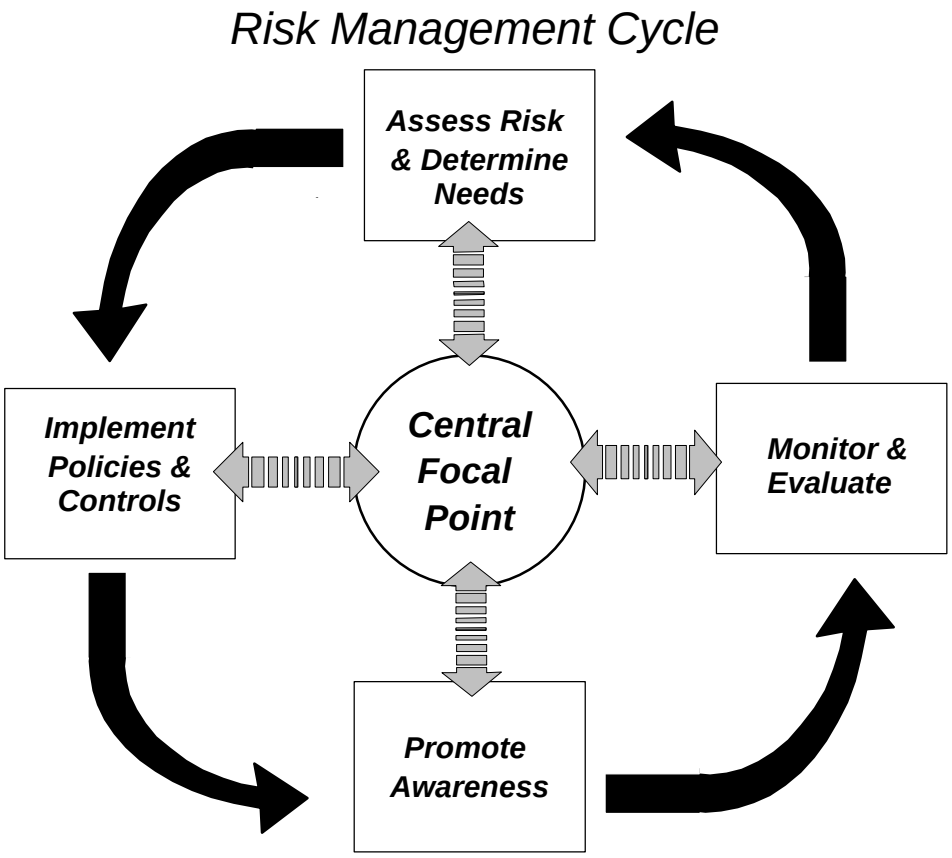
Although the nature of their operations differed, the organizations all had embraced five risk management principles, which are listed in the box below. These principles guided the organizations' efforts to manage the risk associated with the increasingly automated and interconnected environment in which they functioned.

Risk Management Principles Implemented by Leading Organizations

- **Assess risk and determine needs**
- **Establish a central management focal point**
- **Implement appropriate policies and related controls**
- **Promote awareness**
- **Monitor and evaluate policy and control effectiveness**

An important factor in effectively implementing these principles was linking them in a cycle of activity that helped ensure that information security policies addressed current risks on an ongoing basis. The single most important factor in prompting the establishment of an effective security program was a general recognition and understanding among the organization's most senior executives of the enormous risks to business operations associated with relying on automated and highly interconnected systems. However, risk assessments of individual business applications provided the basis for establishing policies and selecting related controls. Steps were then taken to increase the awareness of users concerning these risks and related policies. The effectiveness of controls and awareness activities was then monitored through various analyses, evaluations, and audits, and the results provided input to subsequent risk assessments, which determined if existing policies and controls needed to be modified. All of these activities were coordinated through a central security management office or group the staff of which served as consultants and

facilitators to individual business units and senior management. This risk management cycle is illustrated in the diagram below.

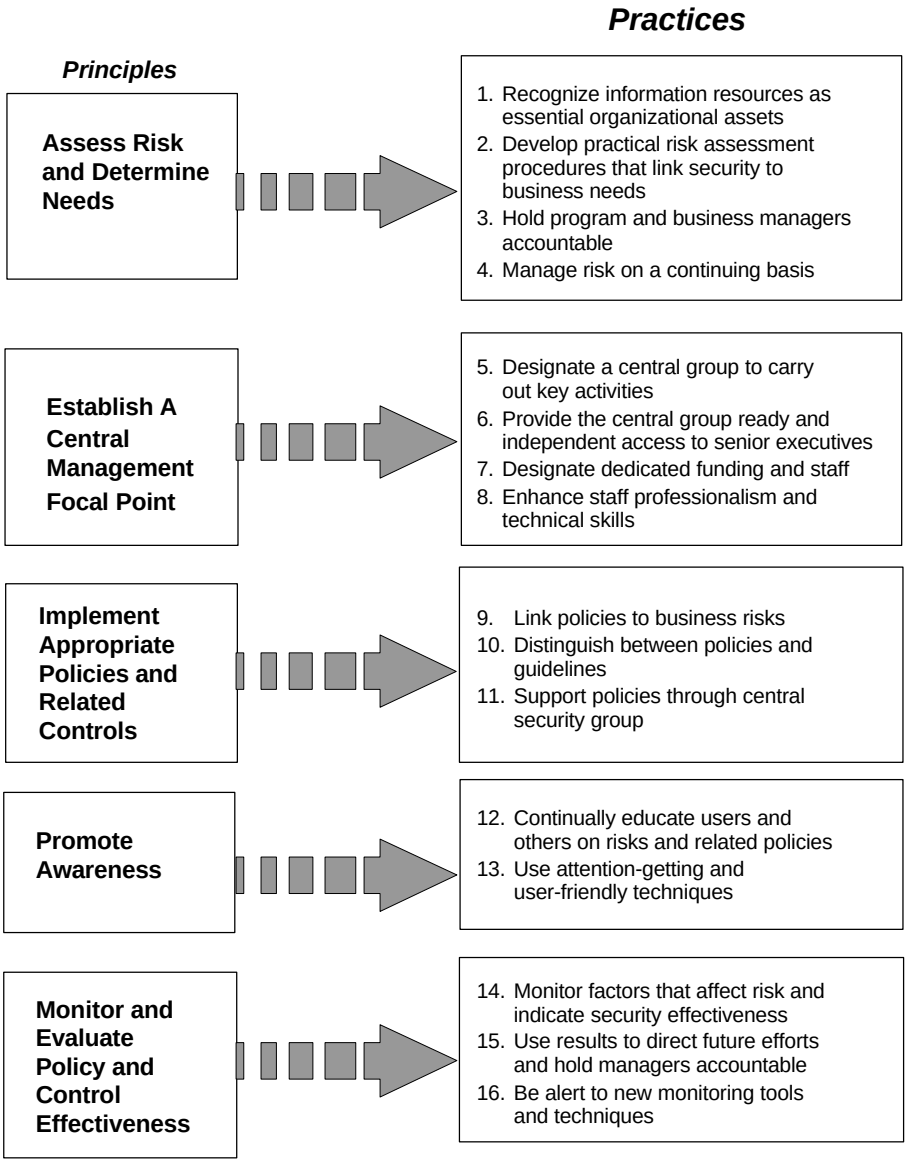


This continuing cycle of monitoring business risks, maintaining policies and controls, and monitoring operations parallels the process associated with managing the controls associated with any type of program. In addition, these principles should be familiar to federal agency officials since they have been emphasized in much of the recent guidance pertaining to federal information security. Most notably, they incorporate many of the concepts included in NIST's September 1996 publication, Generally Accepted Principles and Practices for Securing Information Technology Systems, and in OMB's February 1996 revision of Circular A-130, Appendix III, Security of Federal Automated Information Resources.

Principles Were Implemented Though Similar Practices

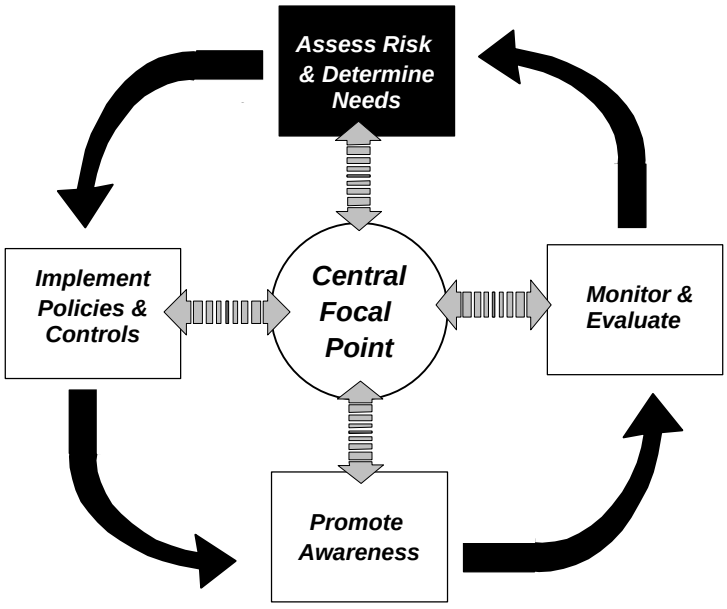
The organizations had developed similar sets of practices to implement the five risk management principles, although the techniques they employed varied depending on each organization's size and culture. Some programs were less mature than others and had not fully implemented all of the practices. However, security managers at each organization agreed that the 16 practices outlined in the following illustration, which relate to the five risk management principles, were key to the effectiveness of their programs.

Sixteen Practices Employed by Leading Organizations To Implement the Risk Management Cycle



The following pages provide a more detailed discussion of these practices and illustrative examples of the techniques used to implement them by the organizations we studied. The discussion follows the order of the practices as outlined above. Individual agency priorities for adopting the practices will vary depending on their existing security programs.

Assess Risk and Determine Needs



"We are not in the business of protecting information. We only protect information insofar as it supports the business needs and requirements of our company."

-- Senior security manager at a major electric utility

All of the organizations said that risk considerations and related cost-benefit trade-offs were a primary focus of their security programs. Security was not viewed as an end in itself, but as a set of policies and related controls designed to support business operations, much like other types of internal controls.[4]

Controls were identified and implemented to address specific business risks. As one organization's security manager said, "Because every control has some cost associated with it, every control needs a business reason to be put in place." Regardless of whether they were analyzing existing or proposed operations, security managers told us that identifying and assessing information security risks in terms of the impact on business operations was an essential step in determining what controls were needed and what level of resources could be expended on controls. In this regard, understanding the business risks associated with information security was the starting point of the risk management cycle.

---

[4]In GAO's recently revised Standards for Internal Control in the Federal Government, Exposure Draft (GAO/AIMD-98-21.3.1, December 1997), controls over computerized information and information processing are discussed in the context of the larger body of an agency's internal control activities.

Practice 1: Recognize Information Resources as Essential Organizational Assets That Must Be Protected

"Information technology is an integral and critical ingredient for the successful functioning of major U.S. companies."

-- Deloitte & Touche LLP Survey of American Business Leaders, November 1996

The organizations we studied recognized that information and information systems were critical assets essential to supporting their operations that must be protected. As a result, they viewed information protection as an integral part of their business operations and of their strategic planning.

Senior Executive Support Is Crucial

In particular, senior executive recognition of information security risks and interest in taking steps to understand and manage these risks were the most important factors in prompting development of more formal information security programs. Such high-level interest helped ensure that information security was taken seriously at lower organizational levels and that security specialists had the resources needed to implement an effective program.

This contrasts with the view expressed to us by numerous federal managers and security experts that many top federal officials have not recognized the indispensable nature of electronic data and automated systems to their program operations. As a result, security-related activities intended to protect these resources do not receive the resources and attention that they merit.

In some cases, senior management's interest had been generated by an incident that starkly illustrated the organization's information security vulnerabilities, even though no damage may have actually occurred. In other cases, incidents at other organizations had served as a "wake-up call." Two organizations noted that significant interest on the part of the board of directors was an important factor in their organizations' attention to information security. However, security managers at many of the organizations told us that their chief executive officers or other very senior executives had an ongoing interest in information technology and security, which translated into an organizationwide emphasis on these areas.

Although the emphasis on security generally emanated from top officials, security specialists at lower levels nurtured this emphasis by keeping them

abreast of emerging security issues, educating managers at all levels, and by emphasizing the related business risks to their own organizations.

Security Seen As An Enabler

In addition, most of the organizations were aggressively exploring ways to improve operational efficiency and service to customers through new or expanded applications of information technology, which usually prompted new security considerations. Officials at one organization viewed their ability to exploit information technology as giving them a significant competitive advantage. In this regard, several organizations told us that security was increasingly being viewed as an enabler--a necessary step in mitigating the risks associated with new applications involving Internet use and broadened access to the organization's computerized data. As a result, security was seen as an important component in improving business operations by creating opportunities to use information technology in ways that would not otherwise be feasible.

Practice 2: Develop Practical Risk Assessment Procedures That Link Security to Business Needs

The organizations we studied had tried or were exploring various risk assessment methodologies, ranging from very informal discussions of risk to fairly complex methods involving the use of specialized software tools. However, the organizations that were the most satisfied with their risk assessment procedures were those that had defined a relatively simple process that could be adapted to various organizational units and involved a mix of individuals with knowledge of business operations and technical aspects of the organization's systems and security controls.

The manufacturing company had developed an automated checklist that asked business managers and relevant staff in individual units a series of questions that prompted them to consider the impact of security controls, or a lack thereof, on their unit's operations. The results of the analysis were reported in a letter to senior management that stated the business unit's compliance with the security policy, planned actions to become compliant, or willingness to accept the risk. The results were also reported to the internal auditors, who used them as a basis for reviewing the business unit's success in implementing the controls that the unit's managers had determined were needed. Through the reporting procedure, the business managers took responsibility for either tolerating or mitigating security risks associated with their operations.

Such procedures provided a relatively quick and consistent means of exploring risk with business managers, selecting cost-effective controls, and documenting conclusions and business managers' acceptance of final determinations regarding what controls were needed and what risks could be tolerated. With similar objectives in mind, the utility company had developed a streamlined risk assessment process that brought together business managers and technical experts to discuss risk factors and mitigating controls. (This process is described in detail as a case example on page 28.)

Other organizations had developed less formal and comprehensive techniques for ensuring that risks were considered prior to changes in operations.

- The retailer had established standard procedures for requesting and granting new network connections. Under these procedures, documentation about the business need for the proposed connection and the risks associated with the proposed connection had to be submitted in writing prior to consideration by the central security group. Then, a meeting between the technical group, which implemented new connections, the requester, and the central security group was held to further explore the issue. The documentation and meeting helped

ensure that the requester's business needs were clearly understood and the best solution was adopted without compromising the network's security.

- The financial services corporation had implemented procedures for documenting business managers' decisions to deviate from organizationwide policies and standards. In order to deviate from a "mandatory policy," the business unit prepared a letter explaining the reason for the deviation and recognizing the related risk. Both the business unit executive and the central security group manager signed the letter to acknowledge their agreement to the necessity of the policy deviation. Deviations from less rigid "standards" were handled similarly, although the letter could be signed by the business unit executive, alone, and did not require the central security group's approval, though it was generally received. In all cases, the central security group discussed the information security implications of the deviation with the appropriate executive and signed-off only when it was satisfied that the executives fully understood the risk associated with the deviation. However, the ultimate decision on whether a deviation from policies or standards was appropriate was usually left to the business unit.

Organizations Saw Benefits Despite Lack of Precision

"*Actual losses are not necessarily good indications of risk.*"
-- Security manager at a prominent financial institution

Although all of the organizations placed emphasis on understanding risks, none attempted to precisely quantify them, noting that few quantified data are available on the likelihood of an incident occurring or on the amount of damage that is likely to result from a particular type of incident. Such data are not available because many losses are never discovered and others are never reported, even within the organizations where they occurred. In addition, there are limited data on the full costs of damage caused by security weaknesses and on the operational costs of specific control techniques. Further, due to fast-paced changes in technology and factors such as the tools available to would-be intruders, the value of applying data collected in past years to the current environment is questionable. As a result, it is difficult, if not impossible, to precisely compare the cost of controls with the risk of loss in order to determine which controls are the most cost-effective. Ultimately, business managers and security specialists must rely on the best information available and their best judgment in determining what controls are needed.

Despite their inability to precisely compare the costs of controls with reductions in risk, the organizations said that risk assessments still served their primary purpose of ensuring that the risk implications of new and existing applications were explored. In particular, the security managers believed that adequate information was available to identify the most significant risks. For example, in addition to their own organization's experience, they noted that information on threats, specific software vulnerabilities, and potential damage was widely available in technical literature, security bulletins from organizations such as the Carnegie-Mellon Computer Emergency Response Team (CERT), surveys done by professional associations and audit firms, and discussion groups. Although much of this information was anecdotal, the security managers thought that it was sufficient to give them a good understanding of the threats of concern to their organizations and of the potential for damage.

In addition, the lack of quantified results did not diminish the value of risk assessments as a tool for educating business managers. By increasing the understanding of risks, risk assessments (1) improved business managers' ability to make decisions on controls needed, in the absence of quantified risk assessment results, and (2) engendered support for policies and controls adopted, thus helping to ensure that policies and controls would operate as intended.

Practice 3: Hold Program and Business Managers Accountable

"Holding business managers accountable and changing the security staff's role from enforcement to service has been a major paradigm shift for the entire company."

-- Security manager at a major equipment manufacturer

The organizations we studied were unanimous in their conviction that business managers must bear the primary responsibility for determining the level of protection needed for information resources that support business operations. In this regard, most held the view that business managers should be held accountable for managing the information security risks associated with their operations, much as they would for any other type of business risk. However, security specialists played a strong educational and advisory role and had the ability to elevate discussions to higher management levels when they believed that risks were not being adequately addressed.

Business managers, usually referred to as program managers in federal agencies, are generally in the best position to determine which of their information resources are the most sensitive and what the business impact of a loss of integrity, confidentiality, or availability would be. Business or program managers are also in the best position to determine how security controls may impair their operations. For this reason, involving them in selecting controls can help ensure that controls are practical and will be implemented.

Accordingly, security specialists had assumed the role of educators, advisors, and facilitators who helped ensure that business managers were aware of risks and of control techniques that had been or could be implemented to mitigate the risks. For several of the organizations, these roles represented a dramatic reversal from past years, when security personnel were viewed as rigid, sometimes overly protective enforcers who often did not adequately consider the effect of security controls on business operations.

Some of the organizations had instituted mechanisms for documenting and reporting business managers' risk determinations. These generally required some type of sign-off on memoranda that either (1) reported deviations from predetermined control requirements, as was the case at the financial services corporation and the manufacturing company discussed previously or (2) provided the results of risk assessments, as was the case of the utility company described in the following case example. According to the security managers, such sign-off requirements helped ensure that business managers carefully considered their decisions before finalizing them.

Case Example: A Practical Method for Involving Business Managers in Risk Assessment

A major electric utility company has developed an efficient and disciplined process for ensuring that information security-related risks to business operations are considered and documented. The process involves analyzing one system or segment of business operation at a time and convening a team of individuals that includes business managers who are familiar with business information needs and technical staff who have a detailed understanding of potential system vulnerabilities and related controls. The sessions, which follow a standard agenda, are facilitated by a member of the central security group who helps ensure that business managers and technical staff communicate effectively and adhere to the agenda.

During the session, the group brainstorms to identify potential threats, vulnerabilities, and resultant negative impacts on data integrity, confidentiality, and availability. Then, they analyze the effects of such impacts on business operations and broadly categorize the risks as major or minor. The group does not usually attempt to obtain or develop specific numbers for threat likelihood or annual loss estimates unless the data for determining such factors are readily available. Instead, they rely on their general knowledge of threats and vulnerabilities obtained from national incident response centers, professional associations and literature, and their own experience. They believe that additional efforts to develop precisely quantified risks are not cost-effective because (1) such estimates take an inordinate amount of time and effort to identify and verify or develop, (2) the risk documentation becomes too voluminous to be of practical use, and (3) specific loss estimates are generally not needed to determine if a control is needed.

After identifying and categorizing risks, the group identifies controls that could be implemented to reduce the risk, focusing on the most cost-effective controls. As a starting point, they use a list of about 25 common controls designed to address various types of risk. Ultimately, the decision as to what controls are needed lies with the business managers, who take into account the nature of the information assets and their importance to business operations and the cost of controls.

The team's conclusions as to what risks exist and what controls are needed are documented along with a related action plan for control implementation. This document is then signed by the senior business manager and technical expert participating and copies are made available to all participant groups and to the internal auditors, who may later audit the effectiveness of the agreed upon controls.

Each risk analysis session takes approximately 4 hours and includes 7 to 15 people, though sessions with as many as 50 and as few as 4 people have occurred. Additional time is usually needed to develop the action plan. The information security group conducts between 8 and 12 sessions a month. According to the utility's central information security group, this process increases security awareness among business managers, develops support for needed controls, and helps integrate information security considerations into the organization's business operations.

Practice 4: Manage Risk on a Continuing Basis

> *"Information security is definitely a journey, not a destination--there are always new challenges to meet."*
>
> -- Chief information security officer at a major financial services corporation

The organizations emphasized the importance of continuous attention to security to ensure that controls were appropriate and effective. They stressed that constant vigilance was needed to ensure that controls remained appropriate--addressing current risks and not unnecessarily hindering operations--and that individuals who used and maintained information systems complied with organizational policies.

Such attention is important for all types of internal controls, but it is especially important for security over computerized information, because, as mentioned previously, the factors that affect computer security are constantly changing in today's dynamic environment. Such changing factors include threats, systems technologies and configurations, known vulnerabilities in existing software, the level of reliance on automated systems and electronic data, and the sensitivity of such operations and data.

Existing Federal Guidance Provides a Framework for Implementing Risk Management Practices

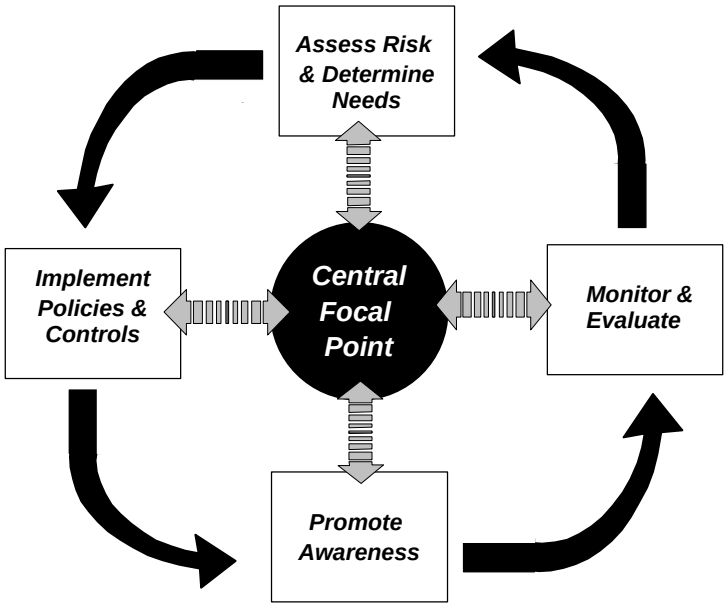
OMB's 1996 revision of Circular A-130, Appendix III, recognizes that federal agencies have had difficulty in performing effective risk assessments--expending resources on complex assessments of specific risks with limited tangible benefits in terms of improved security. For this reason, the revised circular eliminates a long-standing federal requirement for formal risk assessments. Instead, it promotes a risk-based approach and suggests that, rather than trying to precisely measure risk, agencies focus on generally assessing and managing risks. This approach is similar to that used by the organizations we studied.

Similarly, the concept of holding program managers accountable underlies the existing federal process for accrediting systems for use. Accreditation is detailed in NIST's Federal Information Processing Standards Publication 102, Guideline for Computer Security Certification and Accreditation, which was published in 1983. According to NIST, accreditation is "the formal authorization by the management official for system operation and an explicit acceptance of risk." OMB's 1996 update to Circular A-130, Appendix III, provides similar guidance, specifying that a management official should authorize in writing the use of each system before beginning or significantly changing use of the system. "By authorizing processing in a system, a manager accepts the risks associated with it."

Getting Started--Assessing Risk and Determining Needs

Senior Program Officials	Gain an understanding of the criticality and sensitivity of the information and systems that support key agency programs. Recognize that information security risks to program operations are potentially significant and support efforts to further explore and understand these risks as they relate to your agency's operations. Review discussions made by subordinate managers regarding the levels of information protection needed and take responsibility for making final determinations. Monitor implementation of the risk assessment process to ensure that it is providing benefits and does not evolve into a "paperwork exercise."
CIOs	Define risk assessment processes that involve senior program officials and require them to make final determinations regarding the level of information protection needed. Ensure that security specialists and other technical experts are available to educate and advise program officials regarding potential vulnerabilities and related controls.
Senior Security Officers	Promote and facilitate the risk assessment process by (1) developing practical risk assessment procedures and tools, (2) arranging for risk assessment sessions, (3) ensuring the involvement of key program and technical personnel, and (4) providing mechanisms for documenting final decisions. In promoting the adoption of policies and other controls, focus on the specific business reasons for the controls rather than on generic requirements.

Establish a Central Management Focal Point



"A central focal point is essential to spotting trends, identifying problem areas, and seeing that policies and administrative actions are handled in a consistent manner."

-- Senior information security officer for a major university

"Information security has become too important to handle on an ad hoc basis."

-- Security specialist at a major retailing company

Managing the increased risks associated with a highly interconnected computing environment demands increased central coordination to ensure that weaknesses in one organizational unit's systems do not place the entire organization's information assets at undue risk. Each of the organizations we studied had adopted this view and, within the last few years, primarily since 1993, had established a central security management group or reoriented an existing central security group to facilitate and oversee the organization's information security activities. As such, the central group served as the focal point for coordinating activities associated with the four segments of the risk management cycle.

As discussed in the previous section on risk analysis, the central security groups served primarily as advisers or consultants to the business units, and, thus, they generally did not have the ability to independently dictate information security practices. However, most possessed considerable "clout" across their organizations due largely to the support they received from their organization's senior management. In this regard, their views were

sought and respected by the organizations' business managers. The following case example describes how one organization strengthened its central security group and reoriented its focus.

Case Example: Transforming an Organization's Central Security Focal Point

In 1995, realizing that security was an essential element of its efforts to innovatively use information technology, a major manufacturer significantly reorganized and strengthened its central information security function. Prior to the reorganization, a central security group of about four individuals concentrated on mainframe security administration and had little interaction with the rest of the company. Since then, the central group has grown to include 12 individuals who manage the security of the company's (1) main network, (2) decentralized computer operations, and (3) Internet use. In addition, the group participates in the company's strategic planning efforts and in the early stages of software development projects to ensure that security implications of these efforts are addressed. In this regard, it serves as a communications conduit between management and the information systems staff who design, build, and implement new applications.

Members of the central group possess a variety of technical skills and have specific information security responsibilities, such as developing policy, maintaining the firewall that protects the organization's network from unauthorized intrusions, or supporting security staff assigned to individual business units. According to the group's manager, because of the shift in the central group's responsibilities, "the members of the group had to change their mind-set from a staff organization to a service organization. They had to be willing to work with business managers to enable rather than to control business operations."

Practice 5: Designate a Central Group to Carry Out Key Activities

Overall, the central security groups served as (1) catalysts for ensuring that information security risks were considered in both planned and ongoing operations, (2) central resources for advice and expertise to units throughout their organizations, and (3) a conduit for keeping top management informed about security-related issues and activities affecting the organization. In addition, these central groups were able to achieve some efficiencies and increase consistency in the implementation of the organization's security program by performing tasks centrally that might otherwise be performed by multiple individual business units.

Specific activities performed by central groups differed somewhat, primarily because they relied to a varying extent on security managers and administrators in subordinate units and on other organizationally separate groups, such as disaster recovery or emergency response teams. Examples of the most common activities carried out by central groups are described below.

- Developing and adjusting organizationwide policies and guidance, thus reducing redundant policy-related activities across the organization's units. For example, the manufacturer's central security group recently revamped the company's entire information security manual and dedicated one staff member to maintaining it.

- Educating employees and other users about current information security risks and helping to ensure consistent understanding and administration of policies through help-line telephone numbers, presentations to business units, and written information communicated electronically or through paper memos.

- Initiating discussions on information security risks with business managers and conducting defined risk assessment procedures.

- Meeting periodically with senior managers to discuss the security implications of new information technology uses being considered.

- Researching potential threats, vulnerabilities, and control techniques and communicating this information to others in the organization. Many of the organizations supplemented knowledge gained from their own experiences by frequently perusing professional publications, alerts, and other information available in print and through the Internet. Several mentioned the importance of networking with outside organizations, such as the International Information Integrity Institute, the European Security Forum, and the Forum of Incident Response and Security

Teams, to broaden their knowledge. One senior security officer noted, "Sharing information and solutions is important. Many organizations are becoming more willing to talk with outsiders about security because they realize that, despite differing missions and cultures, they all use similar technology and face many of the same threats."

- Monitoring various aspects of the organization's security-related activities by testing controls, accounting for the number and types of security incidents, and evaluating compliance with policies. The central groups often characterized these evaluative activities as services to the business units.

- Establishing a computer incident response capability, and, in some cases, serving as members of the emergency response team.

- Assessing risks and identifying needed policies and controls for general support systems, such as organizationwide networks or central data processing centers, that supported multiple business units. For example, some central groups controlled all new connections to the organization's main network, ensuring that the connecting network met minimum security requirements. Similarly, one organization's central group was instrumental in acquiring a strong user authentication system to help ensure that network use could be reliably traced to the individual users. Further, most central groups oversaw Internet use.

- Creating standard data classifications and related definitions to facilitate protection of data shared among two or more business units.

- Reviewing and testing the security features in both commercially developed software that was being considered for use and internally developed software prior to its being moved into production. For example, the manufacturing company's central group reviewed all new Internet related applications and had the authority to stop such applications from going into production if minimum security standards were not met. Similarly, the central information protection group at the utility was required to approve all new applications to indicate that risks had been adequately considered.

- Providing self-assessment tools to business units so that they could monitor their own security posture. For example, the financial services corporation provided business units with software tools and checklists so that they would assume responsibility for identifying and correcting weaknesses rather than depending on auditors to identify problems.

Practice 6: Provide the Central Group Ready and Independent Access to Senior Executives

Senior information security managers emphasized the importance of being able to discuss security issues with senior executives. Several noted that, to be effective, these senior executives had to be in a position to act and effect change across organizational divisions. The ability to independently voice security concerns to senior executives was viewed as important because such concerns could often be at odds with business managers' and system developers' desires to implement new computer applications quickly and avoid controls that would impede efficiency, user friendliness, and convenience. This ability to elevate significant security concerns to higher management levels helped ensure that risks were thoroughly understood and that decisions as to whether such risks should be tolerated were carefully considered before final decisions were made.

The organizational positions of the central groups varied. Most were located two levels below the Chief Information Officer (CIO). However, the groups reporting directly to the CIO or to an even more senior official viewed this as an advantage because it provided them greater independence. Several others said that, despite their lower organizational position, they felt free to contact their CIOs and other senior executives when important security issues arose, and they were relatively unrestrained by the need to "go through the chain of command." Some noted that senior managers frequently called them to discuss security issues. For example, at the nonbank financial institution, the senior security manager was organizationally placed two levels below the CIO, but she met independently with the CIO once every quarter. Also, during the first three months of 1997, she had met twice with the organization's chief executive officer, at his request, to discuss the security implications of new applications.

In contrast, several federal information security officials told us that they felt that their organizations were placed too low in the organizational structure to be effective and that they had little or no opportunity to discuss information security issues with their CIOs and other senior agency officials.

Rather than depend on the personal interest of individual senior managers, two of the organizations we studied had established senior-level committees to ensure that information technology issues, including information security, received appropriate attention. For example, the university's central group had created a committee of respected university technical and policy experts to discuss and build consensus about the importance of certain information security issues reported to senior management, thus lending weight and credibility to concerns raised by the central security office.

Practice 7: Designate Dedicated Funding and Staff

Unlike many federal agencies, the central groups we studied had defined budgets, which gave them the ability to plan and set goals for their organization's information security program. At a minimum, these budgets covered central staff salaries and training and security hardware and software. At one organization, business units could supplement the central group's resources in order to increase the central group's participation in high priority projects. While all of the central groups had staffs ranging from 3 to 17 people permanently assigned to the group, comparing the size of these groups is of limited value because of wide variations in the (1) sizes of the organizations we studied, (2) inherent riskiness of their operations, and (3) the additional support the groups received from other organizational components and from numerous subordinate security managers and administrators.

In particular, no two groups were alike regarding the extent of support they received from other organizational units. For example, the computer vendor relied on a security manager in each of the organization's four regional business units, while the utility's nine-member central group relied on 48 part-time information security coordinators at various levels within the company. Some central groups relied heavily on technical assistance located in another organizational unit, while others had significant technical expertise among their own staff, and, thus, were much more involved in directly implementing and testing controls.

Despite these differences, two key characteristics were common to each of the organizations: (1) information security responsibilities had been clearly defined for the groups involved and (2) dedicated staff resources had been provided to carry out these responsibilities. The following table summarizes the details on the size and structure of the organizations' information security staffs.

Placement and Staffing of Eight Central Information Security Management Groups

Organization	**Approximate number of system users**	**Placement of central group**	**Number of dedicated central staff**	**Other staff resources relied on** (some numbers are approximate)
Financial services corporation	70,000	Two levels below CEO	17	▪ 35 security officers in business units
Electric utility	5,000	One level below CIO	9	▪ 48 security coordinators at three levels throughout the organization ▪ Virus response team ▪ Administrators
State university	100,000	One level below CIO	3	▪ 170 LAN administrators ▪ Technical committee ▪ Policy committee ▪ Incident handling team
Retailer	65,000	Two levels below CIO	12	▪ 2,000 distributed security administrators ▪ Internal audit staff ▪ Technical services group ▪ Loss prevention staff
State agency	8,000	Two levels below CIO	8	▪ 25 district managers ▪ Security administrators in 31 units ▪ Individuals with specialized expertise in the information systems group
Nonbank financial institution	3,500	Two levels below CIO	7	▪ Central security administration group
Computer vendor	15,000	Three levels below CIO	4	▪ 27 regional security specialists
Equipment manufacturer	35,000	Several levels below CIO	12	▪ 70 site security administrators

Practice 8: Enhance Staff Professionalism and Technical Skills

The organizations had taken steps to ensure that personnel involved in various aspects of their information security programs had the skills and knowledge they needed. In addition, they recognized that staff expertise had to be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools. Further, most of the organizations were striving to increase the professional stature of their staff in order to gain respect from others in their organizations and attract competent individuals to security-related positions.

Update Skills and Knowledge of Security Managers and Specialists

The training emphasis for staff in the central security management groups, many of whom came to their groups with significant technical expertise, was on keeping staff skills and knowledge current. This was accomplished primarily through attendance at technical conferences and specialized courses on topics such as the security features of new software, as well as networking with other security professionals and reviewing the latest technical literature and bulletins. To maximize the value of expenditures on external training and events, one central group required staff members who attended these events to brief others in the central group on what they had learned.

In an effort to significantly upgrade the expertise of information security officers in its various business units, the central group at the financial services corporation had recently arranged for an outside firm to provide 5 weeks of training for these individuals. The training, which is planned to take place in 1-week increments throughout the year, is expected to entail a broad range of security-related topics, including general information security, encryption, access control, and how to build a better working relationship with the corporation's technical information systems group.

Citing an emerging trend, the senior information security managers had also started to create information security career paths and stress professional certification for security specialists. In particular, many organizations were encouraging their staff to become Certified Information Systems Security Professionals (CISSP).[5] One security manager noted that security specialists

[5]The CISSP certification was established by the International Information Systems Security Certification Consortium. The consortium was established as a joint effort of several information security-related organizations, including the Information Systems Security Association and the Computer Security Institute, to develop a certification program for information security professionals.

also needed excellent communication skills if they were to effectively fulfill their roles as consultants and facilitators for business managers who were less technically expert regarding computers and telecommunications.

Educate System Administrators

Increasing the expertise of system administrators presented different challenges. System administrators are important because they generally perform day-to-day security functions, such as creating new system user accounts, issuing new passwords, and implementing new software. These tasks must be completed properly and promptly or controls, such as passwords and related access restrictions, will not provide the level of protection intended. In addition, system administrators are the first line of defense against security intrusions and are generally in the best position to notice unusual activity that may indicate an intrusion or other security incident. However, at the organizations we studied, as at federal agencies, security is often a collateral duty, rather than a full-time job, and the individuals assigned frequently have limited technical expertise. As a result, the effectiveness of individual system administrators in maintaining security controls and spotting incidents is likely to vary.

To enhance the technical skills of their security administrators and help ensure that all of them had the minimal skills needed, most of the groups had established special training sessions for them. For example,

- the manufacturer required new security administrators to spend 2 to 5 days in training with the central security group, depending on their technical skills, before they were granted authority to perform specific functions on the network, such as controlling the users' access rights;

- the central security group at the university held annual technical conferences for the university's systems administrators and engaged professional training organizations to offer on-campus training at very reduced rates; and

- the state agency held a biannual conference for systems administrators that included sessions related to their information security responsibilities.

Attract and Keep Individuals with Technical Skills

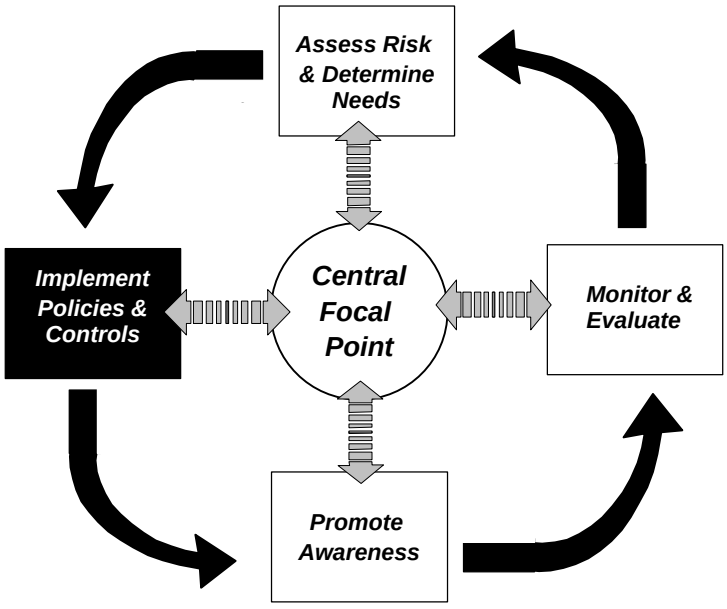
Most of the groups cited maintaining or increasing the technical expertise among their security staff as a major challenge, largely due to the high demand

for information technology experts in the job market. In response, several said they offered higher salaries and special benefits to attract and keep expert staff. For example, the financial services corporation provided competitive pay based on surveys of industry pay levels, attempted to maintain a challenging work environment, and provided flexible work schedules and telecommuting opportunities that allowed most of the staff to work at home 1 day a week. In addition, provisions were made for staff to do the type of work they preferred, such as software testing versus giving presentations.

Organizations relied on both internally and externally developed and presented training courses, sometimes engaging contractors or others to assist. For example, the state information security office above the state agency worked with an information security professional organization to provide a relatively low-cost statewide training conference. The state organization provided meeting rooms and administrative support while the professional organization used its professional contacts to obtain knowledgeable speakers.

Getting Started--Establishing a Central Focal Point	
Senior Program Officials	Involve agency security specialists in the early planning stages of projects involving computer and/or network support. Be accessible to agency security experts and open to considering the information security implications of any operations.
CIOs	Establish a central group to serve as a center of knowledge and expertise on information security and to coordinate agencywide security-related activities. Provide the central group adequate funding for staff resources, training, and security software tools. Be accessible to agency security specialists. Involve agency security experts in the early planning stages of system development or enhancement projects. Support efforts to attract and retain individuals with needed technical skills.
Senior Security Officers	Develop training plans for increasing the expertise of security specialists and security administrators. Explore mechanisms for leveraging resources by drawing on the expertise of others within or outside of the agency. Develop methods for attracting and retaining individuals with needed technical skills.

Implement Appropriate Policies and Related Controls



The organizations viewed information security policies as the foundation of their information security programs and the basis for adopting specific procedures and technical controls. As with any area of operations, written policies are the primary mechanism by which management communicates its views and requirements to its employees, clients, and business partners. For information security, as with other types of internal controls, these views and requirements generally flow directly from risk considerations, as illustrated in the management cycle depicted above.

As discussed earlier, our discussions with the eight organizations focused on their methods for developing and supporting policies and guidelines. We did not discuss the specific controls they had implemented due to the proprietary and often highly technical nature of this information.

Practice 9: Link Policies to Business Risks

The organizations stressed the importance of up-to-date policies that made sense to users and others who were expected to understand them. Many senior security managers told us that prior to the recent strengthening of their security programs, their organization's information security policies had been neglected and out-of-date, thus failing to address significant risks associated with their current interconnected computing environment. As a result, developing a comprehensive set of policies was one of their first steps in establishing an effective corporatewide security program. In addition, they emphasized the importance of adjusting policies continually to respond to newly identified risks or areas of misunderstanding. For example,

- At the financial services corporation, the central security group routinely analyzed the causes of security weaknesses identified by management and by auditors in order to identify policy and related control deficiencies.

- The university had recently developed more explicit policies on system administrator responsibilities in recognition of the critical role of system administration in a distributed environment.

- The manufacturing company had recently drafted policies on security incident response after an incident had exposed shortfalls in the company's guidance in this area.

A relatively new risk area receiving particular attention in organizational policies was user behavior. Many policies are implemented and, to some extent, enforced by technical controls, such as logical access controls that prevent individuals from reading or altering data in an unauthorized manner. However, many information security risks cannot be adequately mitigated with technical controls because they are a function of user behavior. In a networked environment, these risks are magnified because a problem on one computer can affect an entire network of computers within minutes and because users are likely to have easier access to larger amounts of data and the ability to communicate quickly with thousands of others. For example, users may accidentally disclose sensitive information to a large audience through electronic mail or introduce damaging viruses that are subsequently transmitted to the organizations entire network of computers. In addition, some users may feel no compunction against browsing sensitive organizational computer files or inappropriate Internet sites if there is no clear guidance on what types of user behavior are acceptable.

To address these risks, many of which did not exist prior to extensive use of networks, electronic mail, and the Internet, the organizations had begun placing

more emphasis on user behavior in their policies and guidelines. For example, the university's policies went beyond the traditional warnings against password disclosure by including prohibitions against a variety of possible user actions. These included misrepresenting their identity in electronic communications and conducting and promoting personal commercial enterprises on the network. The senior security officer at this organization noted that, when rules such as this are aimed at users, it is especially important that they be stated in clearly understandable, relatively nontechnical language. The security officers at the computer vendor said that because the company's information security policies emphasized user behavior, they were included in the organization's employee code of conduct.

Practice 10: Distinguish Between Policies and Guidelines

"Detailed guidelines are an important supplement to the official policies because they educate users and serve as an awareness tool."

-- Security manager at a prominent financial institution

A common technique for making organizational information security policies more useful was to divide them into two broad segments: concise high-level policies and more detailed information referred to as guidelines or standards. Policies generally outlined fundamental requirements that top management considered to be imperative, while guidelines provided more detailed rules for implementing the broader policies. Guidelines, while encouraged, were not considered to be mandatory for all business units.

Distinguishing between organizational policies and guidelines provided several benefits. It allowed senior management to emphasize the most important elements of information security policy, provided some flexibility to unit managers, made policies easier for employees to understand, and, in some cases, reduced the amount of formal review needed to finalize updated policies.

Guidelines Can Serve As An Educational Tool

Several security managers said that short policies that emphasized the most important aspects of the organizations security concerns were more likely to be read and understood than voluminous and detailed policies. However, they noted that more detailed guidelines often provided answers to employees' questions and served as a tool for educating subordinate security managers and others who wanted a more thorough understanding of good security practices.

For example, the utility company had distilled the fundamental components of its information protection policies into less than one page of text. This narrative (1) stated that *"Information is a corporate asset . . . . Information must be protected according to its sensitivity, criticality and value, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed,"* (2) outlined the responsibilities of information owners, custodians, and users, (3) defined the organization's three data classification categories, and (4) stated that each business unit should develop an information protection program to implement these policies. The policy

statement then referred the reader to a 73-page reference guide that provided definitions, recommended guidelines and procedures, explanatory discussions, and self-assessment questionnaires designed to assist business units in understanding the need for the policies and how they could be implemented.

Guidelines Provide for Flexibility

Although the latitude granted to business units varied, providing both policies and guidelines allowed business units to tailor the guidelines to their own individual unit's information protection needs. It also reinforced the business managers' sense of ownership of their information assets.

For example, the large financial services corporation had divided its information security rules into "policies" and "standards." Policies were mandatory, high-level requirements that, with rare exception, had to be followed. An example of a policy was that units were required to use commercially developed software rather than developing unique software in-house. An example of a standard at the same institution was a prescribed minimum password length. At this organization, deviations from policies had to be documented in a letter signed by both the executive of the business group requesting the deviation and the central information security group's manager. However, deviations from standards required only approval from the group's executive. Such deviations were required to be documented in a letter and, though not required, were usually approved by the central security group. All deviations had to be renewed annually.

Practice 11: Support Policies Through the Central Security Group

Generally, the central security management groups were responsible for developing written corporatewide policies in partnership with business managers, internal auditors, and attorneys. In addition, the central groups provided related explanations, guidance, and support to business units. Several security managers noted that business managers are much more likely to support centrally developed policies if they clearly address organizational needs and are practical to implement. For this reason, these organizations had developed mechanisms for involving other organizational components in policy documentation.

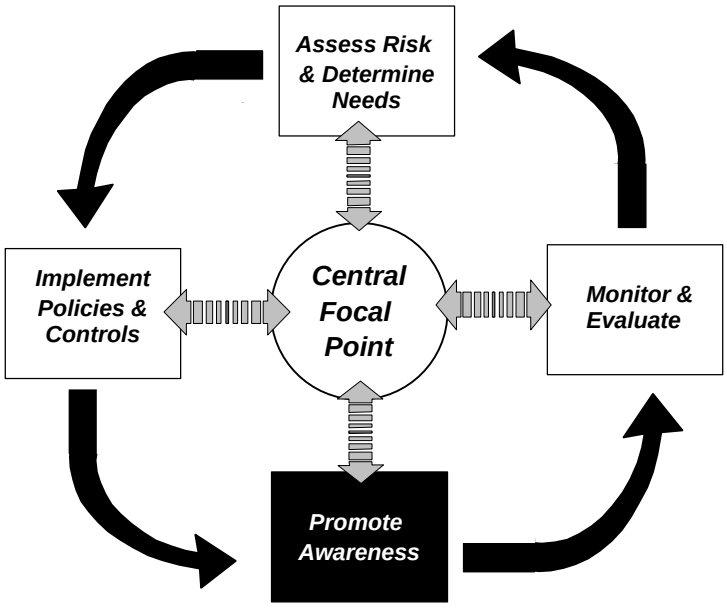
Most often this involvement was in the form of reviews of policy drafts. However, the university had established an information security policy committee that included top university officials, legal counsel, and representatives from student affairs, faculty affairs, and internal audit to assist in the development and review of policies.

The central security management groups played an important role in ensuring that policies were consistently implemented by serving as focal points for user questions. By serving as a readily available resource for organization employees, they helped clear up misunderstandings and provided guidance on topics that were not specifically addressed in written guidance.

Most organizations had also made their policies available through their computer networks so that users could readily access the most up-to-date version whenever they needed to refer to them. In addition, many organizations required users to sign a statement that they had read and understood the organization's information security policies. Generally, such statements were required from new users at the time access to information resources was first provided and from all users periodically, usually once a year. One security manager thought that requiring such signed statements served as a useful technique for impressing on the users the importance of understanding organizational policies. In addition, if the user was later involved in a security violation, the statement served as evidence that he or she had been informed of organizational policies. Additional techniques for communicating information security policies are discussed in the next section on promoting awareness.

Getting Started--Implementing Appropriate Policies and Related Controls	
Senior Program Officials	Review existing policies and assist in developing new policies to ensure that they address current business risks and related information protection needs.
CIOs	Assign responsibility to the central security group for coordinating the development of written policies that address current risks. Institute procedures for periodically updating policies.
Senior Security Officers	Document policies clearly so that they can be readily understood by managers and users. Review existing policies to identify the need to distinguish between official policies and guidelines.

Promote Awareness



"Users are much more likely to support and comply with policies if they clearly understand the purpose for the policies and their responsibilities in regard to the policies."

-- Information security manager for a state agency

User awareness is essential to successfully implementing information security policies and ensuring that related controls are working properly. Computer users, and others with access to information resources, cannot be expected to comply with policies that they are not aware of or do not understand. Similarly, if they are not aware of the risks associated with their organization's information resources, they may not understand the need for and support compliance with policies designed to reduce risk. For this reason, the organizations considered promoting awareness as an essential element of the risk management cycle.

Practice 12: Continually Educate Users and Others on Risks and Related Policies

The central groups had implemented ongoing awareness strategies to educate all individuals who might affect the organization's information security. These individuals were primarily computer users, who might be employees; contractors; clients; or commercial partners, such as suppliers. One organization took an even broader view, targeting awareness efforts also at custodians and security guards, after a night security guard accidentally destroyed some important data while playing games on a computer after hours.

The groups focused their efforts on increasing everyone's understanding of the risks associated with the organization's information and the related policies and controls in place to mitigate those risks. Although these efforts were generally aimed at encouraging policy compliance, the senior security official at the retailing company emphasized the importance of improving users' understanding of risks. She said that her central security group had recognized that policies, no matter how detailed, could never address every scenario that might lead to a security incident. As a result, her overarching philosophy regarding awareness efforts was that users who thoroughly understood the risks were better equipped to use good judgment when faced with a potential security breach. For example, such employees were less likely to be tricked into disclosing sensitive information or passwords.

This last point highlights one of the most important reasons for sensitizing computer users and other employees to the importance of information security. Users disclosing sensitive information or passwords in response to seemingly innocent requests from strangers either over the phone or in person can provide intruders easy access to an organization's information and systems. Such techniques, often referred to as "social engineering," exploit users' tendencies to be cooperative and helpful, instead of guarded, careful, and suspicious, when information is requested. Without adequate awareness about the risks involved in disclosing sensitive information, users may volunteer information which can allow an intruder to circumvent otherwise well-designed access controls.

Practice 13: Use Attention-Getting and User-Friendly Techniques

To get their message across, the central security groups used a variety of training and promotional techniques to make organizational policies readily accessible, educate users on these policies, and keep security concerns in the forefront of users' minds. Techniques used included

- intranet websites that communicated and explained information security-related policies, standards, procedures, alerts, and special notes;
- awareness videos with enthusiastic endorsements from top management for the security program to supplement basic guidance, such as the importance of backing up files and protecting passwords;
- interactive presentations by security staff to various user groups to market the services provided by the central information security group and answer user questions; and
- security awareness day and products with security-related slogans.

The organizations avoided having once-a-year, one-size-fits-all security briefings like those seen at many federal agencies. The security managers said that it was important to relate security concerns to the specific risks faced by users in individual business groups and ensure that security was an everyday consideration.

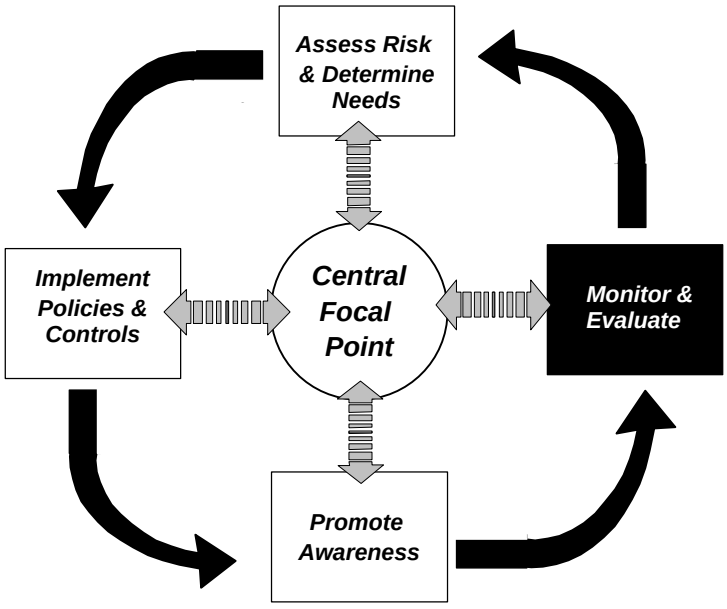
Case Example - Coordinating Policy Development and Awareness Activities

After experiencing a significant virus infection in 1989, a retailing company assigned one of its managers to step up efforts to promote employee awareness of information security risks and related organizational policies. Since then, this individual's responsibilities for information security policy development and awareness, which had previously been handled on a part-time basis, have evolved into a full-time "awareness manager position" in the organization's central security group. The company's response to a minor incident involving the unintentional release of company financial data illustrates the compatibility of these roles. To reduce the chances of a similar incident, the awareness manager concurrently (1) coordinated the development of a policy describing organizational data classification standards and (2) developed a brochure and guidelines to publicize the new standards and educate employees on their implementation. By coordinating policy development and awareness activities in this manner, she helps ensure that new risks and policies are communicated promptly and that employees are periodically reminded of existing policies through means such as monthly bulletins, an intranet web site, and presentations to new employees.

Getting Started--Promoting Awareness

Senior Program Officials	Demonstrate support by participating in efforts to promote information security awareness.
CIOs	Provide adequate funding and support to adequately promote awareness throughout the agency.
Senior Security Officers	Implement ongoing awareness strategies to educate all individuals who might affect the organization's information security.

Monitor and Evaluate Policy and Control Effectiveness



As with any type of business activity, information security should be monitored and periodically reassessed to ensure that policies continue to be appropriate and that controls are accomplishing their intended purpose. Over time, policies and procedures may become inadequate because of changes in threats, changes in operations, or deterioration in the degree of compliance. Periodic assessments or reports on activities can be a valuable means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security program.

The organizations we studied had recognized that monitoring control effectiveness and compliance with policies is a key step in the cycle of managing information security. Accordingly, they monitored numerous factors associated with their security programs, and they used the results to identify needed improvements. They used various techniques to do this, and several mentioned their efforts to identify, evaluate, and implement new, more effective tools as they become available. Such tools include software that can be used to automatically monitor control effectiveness and information systems activity. In addition, several of the security managers expressed interest in improving their ability to more precisely measure the costs and benefits of security-related activities so that their organizations could better determine which controls and activities were the most cost effective.

Practice 14: Monitor Factors that Affect Risk and Indicate Security Effectiveness

The organizations focused their monitoring efforts primarily on (1) determining if controls were in place and operating as intended to reduce risk and (2) evaluating the effectiveness of the security program in communicating policies, raising awareness levels, and reducing incidents. As discussed below, these efforts included testing controls, monitoring compliance with policies, analyzing security incidents, and accounting for procedural accomplishments and other indicators that efforts to promote awareness were effective.

Testing the Effectiveness of Controls

Directly testing control effectiveness was cited most often as an effective way to determine if the risk reduction techniques that had been agreed to were, in fact, operating effectively. In keeping with their role as advisors and facilitators, most of the security managers said that they relied significantly on auditors to test controls. In these cases, the central security management groups kept track of audit findings related to information security and the organization's progress in implementing corrective actions.

However, several of the central security groups also performed their own tests. For example, the central security group at the university periodically ran a computer program designed to detect network vulnerabilities at various individual academic departments and reported weaknesses to department heads. A subsequent review was performed a few months later to determine if weaknesses had been reduced. The central security manager told us that she considered the tests, which could be performed inexpensively by her staff, a cost-effective way to evaluate this important aspect of security and provide a service to the academic departments, which were ultimately responsible for the security of their departments' information and operations.

Several organizations periodically tested system and network access controls by allowing designated individuals to try to "break into" their systems using the latest hacking techniques. This type of testing is often referred to as penetration testing. The individuals performing the tests, which at various organizations were internal auditors, contractors, student interns, or central security staff, were encouraged to research and use hacking instructions and tools available on the Internet or from other sources in order to simulate attacks from real hackers. By allowing such tests, the organizations could readily identify previously unknown vulnerabilities and either eliminate them or make adjustments in computer and network use to lessen the risks.

One organization had performed annual tests of its disaster recovery plan to identify and correct plan weaknesses. A recent test was particularly effective because it involved a comprehensive simulation of a real disaster. The test involved staging a surprise "bomb scare" to get employees, who were unaware that the threat was a pretense, to evacuate the building. After the employees had evacuated, they were told that they were participating in a test, that they were to assume that a bomb had actually destroyed their workplace, and to proceed with emergency recovery plans. The test, which was organized by the agency's contingency planning group, proved extremely successful in identifying plan weaknesses and in dramatically sensitizing employees to the value of anticipating and being prepared for such events.

Monitoring Compliance With Policies and Guidelines

All of the organizations monitored compliance with organizational policies to some extent. Much of this monitoring was achieved through informal feedback to the central security group from system administrators and others in other organizational units. However, a few organizations had developed more structured mechanisms for such monitoring. For example, the utility company developed quarterly reports on compliance with organizational policies, such as the number of organizational units that had tailored their own information protection policies as required by corporate-level policy. Also, several organizations said that they had employed self-assessment tools, such as the Computer Security Institute's "Computer Security Compliance Test," to compare their organization's programs to preestablished criteria.

Accounting For and Analyzing Security Incidents

Keeping summary records of actual security incidents is one way that an organization can measure the frequency of various types of violations as well as the damage suffered from these incidents. Such records can provide valuable input for risk assessments and budgetary decisions.

Although all of the organizations kept at least informal records on incidents, those that had formalized the process found such information to be a valuable resource. For example, at the nonbank financial institution, the central security manager kept records on viruses detected and eradicated, including estimates of the cost of potential damage to computer files that was averted by the use of virus detection software. This information was then used to justify annual budget requests when additional virus detection software was needed. However, as discussed in the following case example, the university had

developed the most comprehensive procedures for accounting for and analyzing security incidents.

Case Example: Developing an Incident Database

A university's central security group had developed a database that served as a valuable management tool in monitoring problems, reassessing risks, and determining how to best use limited resources to address the most significant information security problems. The database accounted for the number of information security incidents that had been reported, the types of incidents, and actions taken to resolve each incident, including disciplinary actions. At the time of our visit, in February 1997, incidents were categorized into 13 types, which generally pertained to the negative effects of the violations. Examples included denial of service, unauthorized access, data compromise, system damage, copyright infringement, and unauthorized commercial activity.

By keeping such records, the central group could develop monthly reports that showed increases and decreases in incident frequency, trends, and the status of resolution efforts. This, in turn, provided the central security group a means of (1) identifying emerging problems, (2) assessing the effectiveness of current policies and awareness efforts, (3) determining the need for stepped up education or new controls to address problem areas, and (4) monitoring the status of investigative and disciplinary actions to help ensure that no individual violation was inadvertently forgotten and that violations were handled consistently.

The means of maintaining the database and the details that it contained had changed as the number of reported incidents at the university had grown--from 3 or 4 a month in 1993 to between 50 and 60 a month in early 1997--and as the database's value as a management tool became more apparent. Records originally maintained in a paper logbook had been transferred to a personal computer, and information on follow-up actions had recently been expanded.

The university's senior security officer noted that the database could be augmented to provide an even broader range of security management information. For example, while the university did not develop data on the actual cost of incidents, such as the cost of recovering from virus infections, the database could be used to compile such information, which would be useful in measuring the cost of security lapses and in determining how much to spend on controls to reduce such lapses.

Monitoring the Effectiveness of the Central Security Management Group

Several of the central security groups had developed measures of their own activities, outputs, and expertise as an indication of their effectiveness. Examples of these items included

- the number of calls from users, indicating knowledge of and respect for security specialists;
- the number of security-related briefings and training sessions presented;
- the number of risk assessments performed;
- the number of security managers and systems administrators who were Certified Information System Security Professionals; and
- the number of courses and conferences held or attended.

Emerging Interest in More Precisely Measuring Cost and Benefits

Several of the security managers expressed an interest in developing better measurement capabilities so that they could more precisely measure the ultimate benefits and drawbacks of security-related policies and controls--that is, the positive and negative affects of information security on business operations. However, they said that such measurements would be difficult because it is costly to do the research and recordkeeping necessary to develop information on (1) the full cost of controls--both the initial cost and operational inefficiencies associated with the controls--and (2) the full cost of incidents or problems resulting from inadequate controls. Further, as discussed previously regarding risk assessment, actual reductions in risk cannot be precisely quantified because sufficient data on risk factors are not available.

In an effort to more thoroughly explore this topic, we expanded our discussions beyond the eight organizations that were the primary subjects of our study by requesting the Computer Security Institute to informally poll its most active members on this subject. We also discussed assessment techniques with experts at NIST. Although we identified no organizations that had made significant progress in applying such measures, we found that more precisely measuring the positive and negative effects of security on business operations is an area of developing interest among many information security experts. For this reason, improved data and measurement techniques may be available in the future.

Practice 15: Use Results to Direct Future Efforts and Hold Managers Accountable

Although monitoring, in itself, may encourage compliance with information security policies, the full benefits of monitoring are not achieved unless results are used to improve the security program. Analyzing the results of monitoring efforts provides security specialists and business managers a means of (1) reassessing previously identified risks, (2) identifying new problem areas, (3) reassessing the appropriateness of existing controls and security-related activities, (4) identifying the need for new controls, and (5) redirecting subsequent monitoring efforts. For example, the central security group at the utility redirected its training programs in response to information security weaknesses reported by its internal auditors. Similarly, security specialists at the manufacturing company recently visited one of the company's overseas units to assist in resolving security weaknesses identified by internal auditors. The previously cited example of using records on virus incidents to determine the need for virus-detection software also illustrates this point.

Results can also be used to hold managers accountable for their information security responsibilities. Several organizations had developed quarterly reporting mechanisms to summarize the status of security-related efforts. However, the financial services corporation provided the best example of how periodic reports of results can be used to hold managers accountable for understanding, as well as reducing, the information security risks to their business units. A description of this process is provided in the following case example.

Case Example: Measuring Control Effectiveness and Management Awareness

At a major financial services corporation, managers are expected to know what their security problems are and to have plans in place to resolve them. To help ensure that managers fulfill this responsibility, they are provided self-assessment tools that they can use to evaluate the information security aspects of their operations. When weaknesses are discovered, the business managers are expected to either improve compliance with existing policies or consult with the corporation's security experts regarding the feasibility of implementing new policies or control techniques.

Ratings based on audit findings serve as an independent measure of control effectiveness and management awareness. At the start of every audit, the auditors ask the pertinent business managers what weaknesses exist in their operations and what corrective actions they have deemed necessary and have planned. After audit work is complete, the auditors compare their findings with management's original assertions to see if management was generally aware of all of the weaknesses prior to the audit. The auditors then develop two ratings on a scale of 1 to 5: One rating to indicate the effectiveness of information security controls and a second rating to indicate the level of management awareness. If the auditors discover serious, but previously unrecognized weaknesses, the management awareness rating will be lowered. However, if the auditor finds no additional weaknesses, management will receive a good awareness rating, even if controls need to be strengthened.

These ratings are forwarded to the CEO and to the board of directors, where they can be used as performance measures. According to the bank's central security manager, the bank chairman's goal is for all business units to have favorable ratings (4 or 5) in both categories. Such a rating system provides not only a measure of performance and awareness, but it also places primary responsibility for information security with the managers whose operations depend on it. Further, it recognizes the importance of identifying weaknesses and the risk they present, even when they cannot be completely eliminated.

Practice 16: Be Alert to New Monitoring Tools and Techniques

The security specialists said that they were constantly looking for new tools to test the security of their computerized operations. Two security managers noted that their organizations had implemented new, more sophisticated, software tools for monitoring network vulnerabilities. However, several security managers said that the development of automated monitoring tools is lagging behind the introduction of new computer and network technologies and that this has impaired their efforts to detect incidents, especially unauthorized intrusions. Similarly, as discussed previously, managers are looking for practical techniques for more precisely measuring the value of security controls and obtaining better data on risk factors. In such an environment, it is essential that (1) security specialists keep abreast of developing techniques and tools and the latest information about system vulnerabilities and (2) senior executives ensure they have the resources to do this.

Several security managers told us that, in addition to reading current professional literature, their involvement with professional organizations was a valuable means of learning about the latest monitoring tools and research efforts. Examples of such organizations included the Computer Security Institute, Information Systems Security Association, the Forum of Incident Response and Security Teams, and less formal discussion groups of security professionals associated with individual industry segments. Several security managers said that by participating in our study, they hoped to gain insights on how to improve their information security programs.

Getting Started--Monitoring and Evaluating Policy and Control Effectiveness	
Senior Program Officials	Determine what aspects of information security are important to mission-related operations and identify key indicators to monitor the effectiveness of related controls.
CIOs	Include security-related performance measures when developing information technology performance measures.
Senior Security Officers	Establish a reporting system to account for the number and type of incidents and related costs. Establish a program for testing and evaluating key areas and indicators of security effectiveness. Develop a mechanism for reporting evaluation results to key business managers and others who can act to address problems. Become an active participant in professional associations and industry discussion groups in order to keep abreast of the latest monitoring tools and techniques.

Conclusion

"We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress."

Vice President Albert Gore, Jr., in the Administration's July 1997 report, A Framework For Global Electronic Commerce

To achieve the benefits offered by the new era of computer interconnectivity, the federal government, like other organizational entities and individuals, must find ways to address the associated security implications. Individual security controls and monitoring tools will change as technology advances, and new risks are likely to emerge. For this reason, it is essential that organizations such as federal agencies establish management frameworks for dealing with these changes on an ongoing basis.

Developing an information security program that adheres to the basic principles outlined in this guide is the first and most basic step that an agency can take to build an effective security program. In this regard, agencies must continually (1) explore and assess information security risks to business operations, (2) determine what policies, standards, and controls are worth implementing to reduce these risks, (3) promote awareness and understanding among program managers, computer users, and systems development staff, and (4) assess compliance and control effectiveness. As with other types of internal controls, this is a cycle of activity, not an exercise with a defined beginning and end.

By instituting such a management framework, agencies can strengthen their current security posture, facilitate future system and process improvement efforts, and more confidently take advantage of technology advances.

Appendix I

GAO Guides on Information Technology Management

Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments (GAO/AIMD-98-89, March 1998)

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (Exposure Draft, GAO/AIMD-10.1.19, February 1998)

Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997)

Business Process Reengineering Assessment Guide (GAO/AIMD-10.1.15, April 1997, Version 3)

Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making (GAO/AIMD-10.1.13, February 1997, Version 1)

Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994)

Appendix II

NIST's Generally Accepted Principles and Practices for Securing Information Technology Systems

To provide a common understanding of what is needed and expected in information technology security programs, NIST developed and published Generally Accepted Principles and Practices for Securing Information Technology Systems (Special Pub 800-14) in September 1996.[6] Its eight principles are listed below.

1. Computer Security Supports the Mission of the Organization
2. Computer Security Is an Integral Element of Sound Management
3. Computer Security Should Be Cost-Effective
4. Systems Owners Have Security Responsibilities Outside Their Own Organizations
5. Computer Security Responsibilities and Accountability Should Be Made Explicit
6. Computer Security Requires a Comprehensive and Integrated Approach
7. Computer Security Should Be Periodically Reassessed
8. Computer Security Is Constrained by Societal Factors

[6]At the time of publication, this document, along with other publications pertaining to information security, was available on NIST's Computer Security Resource Clearinghouse internet page at http://csrc.nist.gov/publications.html. The listed documents are also available through either the Government Printing Office or the National Technical Information Service, for more information call (202) 783-3238 or (703) 487-4650, respectively.

Appendix III

Major Contributors to This Executive Guide

Accounting and Information Management Division Washington, D.C.

Jean Boltz, Assistant Director, (202) 512-5247
Michael W. Gilmore, Information Systems Analyst
Ernest A. Döring, Senior Evaluator

GAO Reports and Testimonies on Information Security Issued Since September 1993

U.S. Government Financial Statements: Results of GAO's Fiscal Year 1997 Audit (GAO/T-AIMD-98-128, April 1, 1998)

Financial Audit: 1997 Consolidated Financial Statements of the United States Government (GAO/AIMD-98-127, March 31, 1998)

Financial Audit: Examination of IRS' Fiscal Year 1996 Custodial Financial Statements (GAO/AIMD-98-18, December 24, 1997)

Financial Management: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls (GAO/AIMD-97-128, September 9, 1997)

Financial Audit: Examination of IRS' Fiscal Year 1996 Administrative Financial Statements (GAO/AIMD-97-89, August 29, 1997)

Social Security Administration: Internet Access to Personal Earnings and Benefits Information (GAO/T-AIMD/HEHS-97-123, May 6, 1997)

IRS Systems Security and Funding: Employee Browsing Not Being Addressed Effectively and Budget Requests for New Systems Development Not Justified (GAO/T-AIMD-97-82, April 15, 1997)

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/T-AIMD-97-76, April 10, 1997)

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997)

High Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997)

Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996)

Financial Audit: Examination of IRS' Fiscal Year 1995 Financial Statements (GAO/AIMD-96-101, July 11, 1996)

Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses (GAO/AIMD-96-106, June 7, 1996)

Information Security: Computer Hacker Information Available on the Internet (GAO/T-AIMD-96-108, June 5, 1996)

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996)

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/T-AIMD-96-92, May 22, 1996)

Security Weaknesses at IRS' Cyberfile Data Center (GAO/AIMD-96-85R, May 9, 1996)

Tax Systems Modernization: Management and Technical Weaknesses Must Be Overcome To Achieve Success (GAO/T-AIMD-96-75, March 26, 1996)

Financial Management: Challenges Facing DOD in Meeting the Goals of the Chief Financial Officers Act (GAO/T-AIMD-96-1, November 14, 1995)

Financial Audit: Examination of IRS' Fiscal Year 1994 Financial Statements (GAO/ AIMD-95-141, August 4, 1995)

Federal Family Education Loan Information System: Weak Computer Controls Increase Risk of Unauthorized Access to Sensitive Data (GAO/AIMD-95-117, June 12, 1995)

Department of Energy: Procedures Lacking to Protect Computerized Data (GAO/AIMD-95-118, June 5, 1995)

Financial Management: Control Weaknesses Increase Risk of Improper Navy Civilian Payroll Payments (GAO/AIMD-95-73, May 8, 1995)

Information Superhighway: An Overview of Technology Challenges (GAO/AIMD-95-23, January 23, 1995)

Information Superhighway: Issues Affecting Development (GAO/RCED-94-285, September 30, 1994)

IRS Automation: Controlling Electronic Filing Fraud and Improper Access to Taxpayer Data (GAO/T-AIMD/GGD-94-183, July 19, 1994)

Financial Audit: Federal Family Education Loan Program's Financial Statements for Fiscal Years 1993 and 1992 (GAO/AIMD-94-131, June 30, 1994)

Financial Audit: Examination of Customs' Fiscal Year 1993 Financial Statements (GAO/AIMD-94-119, June 15, 1994)

Financial Audit: Examination of IRS' Fiscal Year 1993 Financial Statements (GAO/AIMD-94-120, June 15, 1994)

HUD Information Resources: Strategic Focus and Improved Management Controls Needed (GAO/AIMD-94-34, April 14, 1994)

Financial Audit: Federal Deposit Insurance Corporation's Internal Controls as of December 31, 1992 (GAO/AIMD-94-35, February 4, 1994)

Financial Management: Strong Leadership Needed to Improve Army's Financial Accountability (GAO/AIMD-94-12, December 22, 1993)

Communications Privacy: Federal Policy and Actions (GAO/OSI-94-2, November 4, 1993)

IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information (GAO/AIMD-93-34, September 22, 1993)

Document Security: Justice Can Improve Its Controls Over Classified and Sensitive Documents (GAO/GGD-93-134, September 7, 1993)